

II. The government’s use of non-governmental entities to censor Americans by proxy

The Select Subcommittee’s oversight revealed how the federal government also worked with third parties to target and censor Americans’ speech, including (1) how the Cybersecurity and Infrastructure Security Agency (CISA) used proxies and partners to target and censor Americans’ election-related speech;³⁵ and (2) how the National Science Foundation (NSF) has funded and supported the development of AI-powered tools that would supercharge the government’s ability to censor disfavored speech.³⁶

On November 6, 2023, the Select Subcommittee issued a report, [“The Weaponization of ‘Disinformation’ Pseudo-Experts and Bureaucrats: How the Federal Government Partnered with Universities to Censor Americans’ Political Speech,”](#) detailing how Stanford University and other partners created the Election Integrity Partnership (EIP), a consortium of “disinformation” academics led by the Stanford Internet Observatory (SIO), that worked directly with the Department of Homeland Security (DHS) and the State Department’s Global Engagement Center (GEC) to monitor and censor Americans’ online speech in advance of the 2020 presidential election.³⁷ Created in the summer of 2020 “at the request of DHS/CISA,” the EIP provided a way for the federal government to launder its censorship activities in an effort to bypass both the First Amendment and public scrutiny.³⁸ The Select Subcommittee uncovered how the EIP sent thousands of Americans’ social media posts directly to Big Tech, often with specific recommendations on how Big Tech should censor the posts.³⁹ The flagged posts included true information, jokes, and political opinions.⁴⁰

The Select Subcommittee has shown that CISA’s unconstitutional censorship efforts have continued well beyond the 2020 election. In particular, the Select Subcommittee’s June 26, 2023 report, [“The Weaponization of CISA: How a ‘Cybersecurity’ Agency Colluded with Big Tech and ‘Disinformation’ Partners to Censor Americans,”](#) revealed that, instead of focusing on legitimate cybersecurity threats, CISA turned its focus to alleged domestic misinformation, disinformation, and malinformation (MDM) and metastasized into the nerve center of the federal

³⁵ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023); STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

³⁶ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION: HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO CENSOR ONLINE SPEECH “AT SCALE” AND TRYING TO COVER UP ITS ACTIONS (Comm. Print Feb. 5, 2024).

³⁷ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

government’s domestic surveillance and censorship operations on social media.⁴¹ The report detailed how under Director Jen Easterly’s tenure: (1) CISA has “work[ed] with federal partners to mature a whole-of-government approach” to curbing alleged misinformation and disinformation; (2) CISA considered the creation of an anti-misinformation “rapid response team” capable of physically deploying across the country; (3) CISA moved its censorship operation to a CISA-funded non-profit after the states of Missouri and Louisiana, along with several other plaintiffs, sued CISA and the Biden-Harris Administration in federal court; (4) CISA wanted to use the same CISA-funded non-profit as its mouthpiece to “avoid the appearance of government propaganda”; and (5) members of CISA’s advisory committee internally worried that it was “only a matter of time before someone realizes we exist and starts asking about our work.”⁴²

The Select Subcommittee also documented how the federal government has poured millions of taxpayer dollars into automating censorship and propaganda technologies.⁴³ The Select Subcommittee’s February 5, 2024 report, “[The Weaponization of the National Science Foundation: How NSF is Funding the Development of Automated Tools to Censor Online Speech “At Scale” and Trying to Cover Up Its Actions,](#)” detailed the NSF’s funding of AI-powered censorship and propaganda tools, and its repeated efforts to hide its actions to avoid political and media scrutiny.⁴⁴ In the name of combatting alleged misinformation regarding COVID-19 and the 2020 presidential election, the NSF issued multi-million-dollar grants to university and non-profit research teams to develop AI-powered censorship and propaganda tools that can be used by governments and Big Tech to shape public opinion by restricting certain viewpoints and promoting others.⁴⁵ Non-public documents obtained by the Select Subcommittee demonstrate that these federal bureaucrats, “disinformation” researchers, and non-profit groups understood that their actions—“content moderation” and combatting so-called misinformation—amounted to “censorship.”⁴⁶ Yet, the NSF forged ahead, supporting new technologies that would essentially enable the censorship of online speech at scale.⁴⁷ These documents also revealed a years-long, intentional effort by the NSF to hide its role in funding these censorship and propaganda tools from media and political scrutiny.⁴⁸

From working with third parties to set up a consortium of “disinformation” pseudo-scientists to flag Americans’ social media posts for censorship, to relocating its censorship activities to a government-funded non-profit, to funding university and non-profit research teams to build censorship and propaganda tools, the Select Subcommittee has shown how the federal

⁴¹ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

⁴² *Id.*

⁴³ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION: HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO CENSOR ONLINE SPEECH “AT SCALE” AND TRYING TO COVER UP ITS ACTIONS (Comm. Print Feb. 5, 2024).

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

government has consistently attempted to bypass the First Amendment and public scrutiny by laundering its censorship activities through third parties.



**THE WEAPONIZATION OF “DISINFORMATION” PSEUDO-EXPERTS AND
BUREAUCRATS:
HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO
CENSOR AMERICANS’ POLITICAL SPEECH**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



November 6, 2023

EXECUTIVE SUMMARY

Following the 2016 presidential election, a sensationalized narrative emerged that foreign “disinformation” affected the integrity of the election. These claims, fueled by left-wing election denialism about the legitimacy of President Trump’s victory, sparked a new focus on the role of social media platforms in spreading such information.¹ “Disinformation” think tanks and “experts,” government task forces, and university centers were formed, all to study and combat the alleged rise in alleged mis- and disinformation. As the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have shown previously, these efforts to combat so-called foreign influence and misinformation quickly mutated to include domestic—that is, American—speech.²

The First Amendment to the Constitution rightly limits the government’s role in monitoring and censoring Americans’ speech, but these disinformation researchers (often funded, at least in part, by taxpayer dollars) were not strictly bound by these constitutional guardrails. What the federal government could not do directly, it effectively outsourced to the newly emerging censorship-industrial complex.

Enter the Election Integrity Partnership (EIP), a consortium of “disinformation” academics led by Stanford University’s Stanford Internet Observatory (SIO) that worked directly with the Department of Homeland Security and the Global Engagement Center, a multi-agency entity housed within the State Department, to monitor and censor Americans’ online speech in advance of the 2020 presidential election. Created in the summer of 2020 “at the request” of the Cybersecurity and Infrastructure Security Agency (CISA),³ the EIP provided a way for the federal government to launder its censorship activities in hopes of bypassing both the First Amendment and public scrutiny.

In the lead-up to the 2020 election, amid the COVID-19 pandemic, the American public and lawmakers debated the merits of unprecedented, mid-election-cycle changes to election procedures.⁴ These issues, like all contemporary discourse about questions of political import, were extensively discussed on the world’s largest social media platforms—the modern town square. But as American citizens, including candidates in these elections, attempted to exercise their First Amendment rights on these platforms, their constitutionally protected speech was intentionally suppressed as a consequence of the federal government’s direct coordination with

¹ See, e.g., Tim Starks, *Russian trolls on Twitter had little influence on 2016 voters*, WASH. POST (Jan. 9, 2023) (“The study, which the New York University Center for Social Media and Politics helmed, explores the limits of what Russian disinformation and misinformation was able to achieve on one major social media platform in the 2016 elections.”); *id.* (“There was no measurable impact on ‘political attitudes, polarization, and vote preferences and behavior’ from the Russian accounts and posts.”).

² See STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023).

³ Email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.).

⁴ See, e.g., REPUBLICAN STAFF OF THE H. COMM. ON THE JUDICIARY AND THE COMM. ON OVERSIGHT AND REFORM, 116TH CONG., *HOW DEMOCRATS ARE ATTEMPTING TO SOW UNCERTAINTY, INACCURACY, AND DELAY IN THE 2020 ELECTION* (Sept. 23, 2020); see also *Changes to election dates, procedures, and administration in response to the coronavirus (COVID-19) pandemic, 2020*, BALLOTPEDIA (last visited Nov. 3, 2023).

third-party organizations, particularly universities, and social media platforms.⁵ Speech concerning elections—the process by which Americans select their representatives—is of course entitled to robust First Amendment protections.⁶ This bedrock principle is even more critical as it relates to speech by political candidates.⁷ But as disinformation “experts” acknowledge, the labeling of any kind of speech is “inherently political”⁸ and itself a form of “censorship.”⁹

This interim staff report details the federal government’s heavy-handed involvement in the creation and operation of the EIP, which facilitated the censorship of Americans’ political speech in the weeks and months leading up to the 2020 election. This report also publicly reveals for the first time secret “misinformation” reports from the EIP’s centralized reporting system, previously accessible only to select parties, including federal agencies, universities, and Big Tech. The Committee and Select Subcommittee obtained these nonpublic reports from Stanford University only under the threat of contempt of Congress. These reports of alleged mis- and disinformation were used to censor Americans engaged in core political speech in the lead up to the 2020 election.

As this new information reveals, and this report outlines, the federal government and universities pressured social media companies to censor true information, jokes, and political opinions. This pressure was largely directed in a way that benefitted one side of the political aisle: true information posted by Republicans and conservatives was labeled as “misinformation” while false information posted by Democrats and liberals was largely unreported and untouched by the censors. The pseudoscience of disinformation is now—and has always been—nothing more than a political ruse most frequently targeted at communities and individuals holding views contrary to the prevailing narratives.

The EIP’s operation was straightforward: “external stakeholders,” including federal agencies and organizations funded by the federal government, submitted misinformation reports

⁵ See *Missouri v. Biden*, No. 23-30445, (5th Cir. Oct. 3, 2023), ECF No. 268-1 (affirming preliminary injunction in part); *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. Jul. 4, 2023), ECF No. 293 (memorandum ruling granting preliminary injunction).

⁶ See, e.g., *Snyder v. Phelps*, 562 U.S. 443, 452 (2011) (“[S]peech on public issues occupies the highest rung of the hierarchy of First Amendment values”) (quoting *Connick v. Myers*, 461 U.S. 138, 145 (1983)); *Ariz. Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721, 755 (2011) (internal quotation marks and citation omitted) (The First Amendment protects the “profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open.”); see also *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 346 (1995) (cleaned up) (“There is practically universal agreement that a major purpose of the Amendment was to protect the free discussion of governmental affairs, of course including discussions of candidates.”).

⁷ “The First Amendment ‘has its fullest and most urgent application precisely to the conduct of campaigns for political office,’” *FEC v. Cruz*, 142 S. Ct. 1638, 1650 (2022) (quoting *Monitor Patriot Co. v. Roy*, 401 U.S. 265, 272 (1971)); see also *Buckley v. Valeo*, 424 U.S. 1, 52 (1976) (A candidate “has a First Amendment right to engage in the discussion of public issues and vigorously and tirelessly to advocate his own election.”).

⁸ Email from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.); see also Kate Starbird et al., Proposal to the National Science Foundation for “Collaborative Research: SaTC: Core: Large: Building Rapid-Response Frameworks to Support Multi-Stakeholder Collaborations for Mitigating Online Disinformation” (Jan. 29, 2021) (unpublished proposal) (on file with the Comm.) (“The study of disinformation today invariably includes elements of politics.”).

⁹ Team F-469 First Pitch to NSF Convergence Accelerator, UNIV. OF MICH., at 1 (presentation notes) (Oct. 27, 2021) (on file with the Comm.).

directly to the EIP. The EIP’s misinformation “analysts” next scoured the internet for additional examples for censorship. If the submitted report flagged a Facebook post, for example, the EIP analysts searched for similar content on Twitter, YouTube, TikTok, Reddit, and other major social media platforms. Once all of the offending links were compiled, the EIP sent the most significant ones directly to Big Tech with *specific* recommendations on how the social media platforms should censor the posts, such as reducing the posts’ “discoverability,” “suspending [an account’s] ability to continue tweeting for 12 hours,” “monitoring if any of the tagged influencer accounts retweet” a particular user, and, of course, removing thousands of Americans’ posts.¹⁰



Government agencies and disinformation “experts” are quick to cite the need to combat foreign actors attempting to undermine American elections as a justification for this censorship regime. While foreign states do attempt to conduct influence operations, the Committee’s and Select Subcommittee’s investigation has revealed that the true focus and purpose of the censors’ “election integrity” work was to target the very Americans they claim to protect. Instead of targeting foreign or inauthentic accounts, the EIP targeted Americans, disproportionately candidates and commentators with conservative viewpoints. And despite its stated purpose to combat “disinformation,” the EIP worked with social media companies to censor true information, jokes and satire, and political opinions.

¹⁰ See, e.g., EIP-581, submitted by [REDACTED], ticket created (Nov. 2, 2020, 2:36 PM) (archived Jira ticket data produced to the Comm.); EIP-673, submitted by [REDACTED], ticket created (Nov. 3, 2020, 11:51 AM) (archived Jira ticket data produced to the Comm.) (citing Mike Coudrey, TWITTER (Nov. 3, 2020, 10:13 AM), <https://twitter.com/MichaelCoudrey/status/1323644406998597633>); EIP-638, submitted by [REDACTED], ticket created (Nov. 3, 2020, 9:23 AM) (archived Jira ticket data produced to the Comm.).

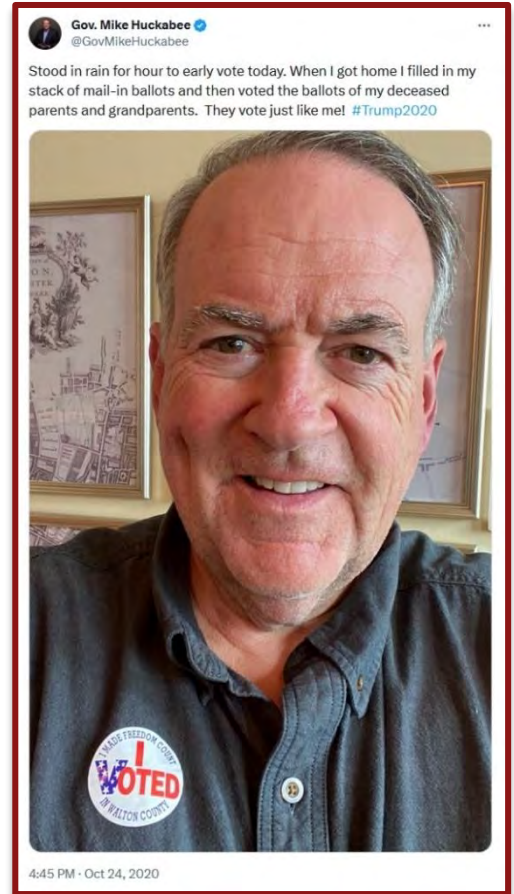
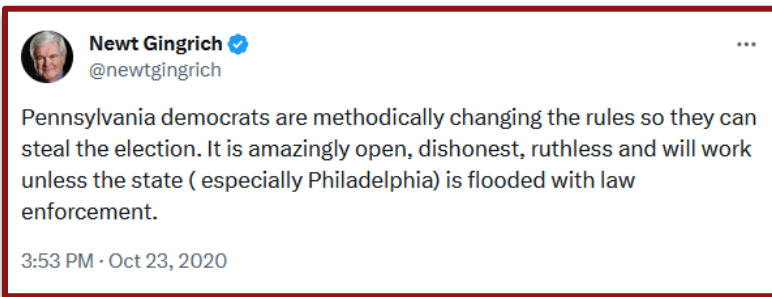
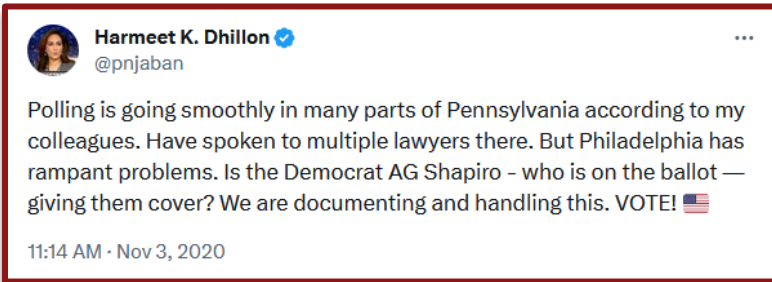
Who was being censored?

- President Donald J. Trump
- Senator Thom Tillis
- Speaker Newt Gingrich
- Governor Mike Huckabee
- Congressman Thomas Massie
- Congresswoman Marjorie Taylor Greene
- Newsmax
- The Babylon Bee
- Sean Hannity
- Mollie Hemingway
- Harmeet Dhillon
- Charlie Kirk
- Candace Owens
- Jack Posobiec
- Tom Fitton
- James O’Keefe
- Benny Johnson
- Michelle Malkin
- Sean Davis
- Dave Rubin
- Paul Sperry
- Tracy Beanz
- Chanel Rion
- An untold number of everyday Americans of all political affiliations



What was being censored?

- True information
- Jokes and satire
- Political opinions



As part of this report, the Committee and Select Subcommittee are releasing all of the previously secret, archived data the Committee has obtained pursuant to a subpoena issued to Stanford University, which Stanford produced only after the threat of contempt.¹¹ In the lead-up to the 2020 election, the Department of Homeland Security (DHS) had the ability to see what American speech was being censored. Today, as a result of the Committee’s and Select Subcommittee’s investigation, political candidates, journalists, and all Americans have the opportunity to see if they were targeted by their government and what viewpoints DHS, Stanford, and others worked to censor. While the EIP disproportionately targeted conservatives, Americans of all political affiliations were victims of censorship.

The First Amendment prohibits the government from “abridging the freedom of speech” and protects “the right of the people . . . to petition the Government.”¹² The ability of Americans to criticize the government and its policies is a fundamental and sacrosanct principle of our constitutional republic. The Supreme Court has long recognized that for “core political speech” “the importance of First Amendment protections is at its zenith.”¹³ Moreover, as constitutional scholars have explained: “Because the First Amendment bars ‘abridging’ the freedom of speech,

¹¹ See App’x II.

¹² U.S. Const. amend. I.

¹³ Meyer v. Grant, 486 U.S. 414, 420, 425 (1988) (internal quotation marks omitted).

any law or government policy that reduces that freedom on the [social media] platforms . . . violates the First Amendment.”¹⁴

The government may not dictate the type or terms of the criticism to which it is subject, even when—especially when—the government disagrees with the merits of that criticism. To inform potential legislation, the Committee and the Select Subcommittee have been investigating the Executive Branch’s collusion with third-party intermediaries, including universities, to censor protected speech on social media.

The Committee and the Select Subcommittee are responsible for investigating “violation[s] of the civil liberties of citizens of the United States.”¹⁵ In accordance with this mandate, this interim staff report on CISA’s violations of the First Amendment and other unconstitutional activities fulfills the obligation to identify and report on the weaponization of the federal government against American citizens. The Committee’s and Select Subcommittee’s investigation remains ongoing. CISA still has not adequately complied with a subpoena for relevant documents, and more fact-finding is necessary. In order to better inform the Committee’s legislative efforts, the Committee and Select Subcommittee will continue to investigate how the Executive Branch worked with social media platforms and other intermediaries to censor disfavored viewpoints in violation of the U.S. Constitution.

¹⁴ Philip Hamburger, *How the Government Justifies Its Social-Media Censorship*, WALL ST. J. (June 9, 2023).

¹⁵ H. Res. 12 § 1(b)(E).

TABLE OF CONTENTS

Executive Summary	1
Table of Contents	7
Glossary of Key Terms & Names	8
I. CISA’s Role in the Creation of the EIP	11
A. CISA’s Precursor Censorship Efforts	11
1. Switchboarding, Disclaimers, and the Threat of Government Retaliation	12
2. EI-ISAC	21
3. Misinformation Reporting Portal.....	23
4. CISA Did Not Distinguish Foreign and Domestic Actors on Social Media	31
B. Creation of the EIP	35
C. The EIP’s Purpose: Using Proxies to Circumvent the First Amendment	41
II. CISA’s Complete Intertwinement with the EIP.....	44
A. CISA’s Collusion with the EIP	44
B. Jira Tickets: The Main Weapon in the EIP’s Censorship Arsenal	54
C. The Collusion in Practice: The Coordinated Flagging of Posts	55
D. The State Department’s Direct Participation in the EIP’s Censorship Operation.....	61
E. Other Federal Agencies’ Involvement with the EIP: the FBI and the NSA	64
III. The EIP’s Jira Tickets: An Encyclopedia of Conservative Censorship.....	66
A. Dropping the Pretense of “Mis- and Disinformation”: The EIP’s Absurd Approach to Classification.....	67
B. Efforts to Censor the Truth.....	68
C. Efforts to Censor President Trump and His Family	69
D. Efforts to Censor Political Candidates and Legislators.....	74
E. Efforts to Censor Humor and Satire	77
F. Efforts to Censor Other Influential Conservative Accounts	80
IV. The EIP’s Coercive Tactics	81
V. Stanford’s Efforts to Obstruct the Committee’s Investigation	84
A. Stanford’s Deceitful Public Statements about the EIP’s Flagging of Posts	84
B. Stanford’s Initial Efforts to Unlawfully Misrepresent and Withhold Jira Data	86
C. Numerous Documents Contradict Witness Testimony Regarding CISA’s Involvement with the EIP	87
D. Stanford’s Continued Misrepresentations Regarding CISA, the EIP, and Jira.....	88
Epilogue	93
Appendix I	97
Appendix II.....	103

GLOSSARY OF KEY TERMS & NAMES

Term/Name	Organization	Description/Definition
CFITF	CISA’s Countering Foreign Influence Task Force (CFITF)	Department of Homeland Security (DHS) Task Force under the Cybersecurity & Infrastructure Security Agency (CISA) which brought together DHS components, including DHS Intelligence and Analysis and others to look at the broader foreign influence and disinformation challenge based on the U.S. intelligence community’s 2017 assessment of foreign influence. In 2021, the CFITF name was changed to Mis-, Dis-, and Malinformation Team (“MDM Team”).
CIP	Center for an Informed Public	University of Washington’s Center for an Informed Public’s mission is to resist strategic misinformation, promote an informed society and strengthen democratic discourse. One of the four founding members of the EIP.
CIS	Center for Internet Security (CIS)	CIS is a CISA-funded, nonprofit that channeled reports of mis- and disinformation from state and local government officials to social media platforms.
CISA	The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency	The Cybersecurity & Infrastructure Security Agency (CISA), a component of the Department of Homeland Security, has stated that one of its goals is to build “resiliency to foreign influence operations and disinformation . . . in close partnership with the interagency, private sector, academia, and international stakeholders.”
DFRLab	The Atlantic Council’s Digital Forensic Research Lab	The Atlantic Council’s DFRLab is dedicated to operationalizing the study of disinformation, tracking information campaigns, exposing attempts to pollute the information space, and building digital resilience. One of the four founding members of the EIP.
DHS I&A	DHS Intelligence and Analysis	DHS I&A specializes in sharing unique intelligence and analysis with operators and decision-makers to identify and mitigate threats to the homeland.
Disinformation		CISA defines disinformation as “deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.”

EI-ISAC	Elections Infrastructure Information Sharing & Analysis Center	The EI-ISAC operated as an intermediary between state and local election officials and the social media platforms, offering a centralized reporting mechanism.
EIP	Election Integrity Partnership (“EIP”)	Originally named the “Election Disinformation Partnership,” the EIP was a collaborative project to develop real-time misinformation response capabilities. The EIP worked with a number of “external stakeholders,” including the federal government. The four original members at the EIP were: <ul style="list-style-type: none"> • Stanford Internet Observatory; • the University of Washington, Center for an Informed Public; • Graphika; and • The Atlantic Council’s Digital Forensic Research Lab (DFRLab).
FITF	The FBI’s Foreign Influence Task Force (FITF)	In 2017, the Federal Bureau of Investigation (FBI) established the Foreign Influence Task Force (FITF) to identify and counteract malign foreign influence operations targeting the United States.
GEC	Department of State, Global Engagement Center	The GEC is a multi-agency organization housed within the State Department tasked with identifying and combating foreign propaganda and disinformation.
Graphika	Graphika, digital intelligence company	Graphika is a social media analytics platform that specializes in monitoring online networks as well as content to provide insights on the spread of information.
Hale, Geoff	Senior CISA official	
Jira	Jira Software system	Jira is a software system used to create tickets to assist with project management. The EIP used JIRA tickets to track and share misinformation reports with large social media companies, the government, and other parties.
Krebs, Chris	Former CISA Director	
Malinformation		CISA defines malinformation as “based on fact, but used out of context to mislead, harm, or manipulate.”
MDM		Misinformation, Disinformation, and Malinformation

MDM Subcommittee	CISA Cybersecurity Advisory Committee's (CSAC) Subcommittee on "Protecting Critical Infrastructure from Misinformation & Disinformation"	The MDM Subcommittee, which has since disbanded, played an advisory role, and consisted of Big Tech executives, former federal government officials, and academic misinformation "experts." The MDM Subcommittee meetings featured CISA participants.
MDM Team (CISA)	CISA's Mis-, Dis, and Malinformation Team (formerly CISA's Countering Foreign Influence Task Force (CFITF))	In January 2021, CISA transitioned its Countering Foreign Influence Task Force to promote more flexibility to focus on general MDM, or so-called "Mis-, Dis-, and Malinformation." According to CISA's website in February 2023, the MDM team was "charged with building national resilience to MDM and foreign influence activities." CISA publicly posted that "[f]oreign and domestic threat actors use MDM campaigns to cause chaos, confusion, and division."
Misinformation		CISA defines misinformation as "false, but not created or shared with the intention of causing harm."
MS-ISAC	Multi-State Information Sharing & Analysis Center	MS-ISAC is a joint-CISA supported collaboration with the Center for Internet Security (CIS) designed to serve as the central cybersecurity resource for the nation's state, local, territorial, and tribal (SLTT) governments.
Scully, Brian	Former Head of CISA's CFITF (later MDM team)	
SIO	Stanford Internet Observatory	SIO is a cross-disciplinary laboratory, within Stanford University's Cyber Policy Center, for the study of abuse in information technologies, with a focus on the misuse of social media.
Stamos, Alex	SIO Director; former Chief Security Officer at Facebook	

I. CISA’S ROLE IN THE CREATION OF THE EIP

The Election Integrity Partnership (EIP) was established in July 2020, and consisted of the nation’s self-described “leading institutions focused on understanding misinformation and disinformation in the social media landscape: the Stanford Internet Observatory, the University of Washington’s Center for an Informed Public (CIP), Graphika, and the Atlantic Council’s Digital Forensic Research Lab.”¹⁶ According to the EIP’s postmortem report about its censorship activities during the 2020 election cycle, the EIP’s goals included “[i]dentify[ing] misinformation before it goes viral,” and “flag[g]ing policy violations to [social media] platforms.”¹⁷

Led by Stanford, the EIP was devised and founded in close coordination with CISA, a little-known agency within the Department of Homeland Security (DHS), created less than two years earlier.¹⁸ Stanford and others, in collaboration with the federal government, established the EIP for the express purpose of violating Americans’ civil liberties: because no federal agency “has a focus on, or authority regarding, election misinformation originating from domestic sources within the United States,” there is “a critical gap for non-governmental entities to fill.”¹⁹ CISA and Stanford created the EIP to bridge this “critical gap”—an unconstitutional workaround for unconstitutional censorship.

A. CISA’s Precursor Censorship Efforts

The creation of EIP did not occur in a vacuum. Before EIP’s origination in the summer of 2020, CISA was directly or indirectly involved with the operation or consideration of at least three other “misinformation” reporting channels: (1) switchboarding; (2) the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC); and (3) a “Misinformation Reporting Portal” to be operated by the Center for Internet Security (CIS), a non-profit funded in part by CISA.²⁰

The constitutional defects with these reporting channels notwithstanding, CISA and “disinformation” experts recognized that they needed another avenue to monitor and remove Americans’ speech in the lead-up to the 2020 election. The EIP served that role, functioning in the words of the head of EIP (and former Chief Security Office at Facebook) Alex Stamos as the “one-stop shop for local election officials, *DHS*, and voter protection organizations” to work

¹⁶ ELECTION INTEGRITY P’SHP, *THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION*, at 2 (Eden Beck, ed., 2021).

¹⁷ *Id.* at 6.

¹⁸ *Id.* at 2; *see also* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023).

¹⁹ ELECTION INTEGRITY P’SHP, *supra* note 16, at v.

²⁰ *See generally* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023).

directly with social media platforms to censor the speech of American political candidates and commentators.²¹

1. Switchboarding, Disclaimers, and the Threat of Government Retaliation

“Switchboarding” describes the federal government’s practice of referring requests for the removal of content on social media from state and local election officials to the relevant platforms.²² CISA personnel involved in the agency’s switchboarding operation have described it as a “resource intensive” process.²³ Documents and information obtained by the Committee and the Select Subcommittee reveal that CISA knew serious legal and constitutional concerns were implicated by switchboarding (a process DHS Secretary Mayorkas testified that CISA no longer participates in).²⁴ CISA’s inclusion of a lengthy—and ever-changing—legal disclaimer betrays that internally the agency understood that there were serious legal questions with the federal government’s engaging in this type of direct communication with social media platforms regarding Americans’ posts and content. Though the disclaimer ostensibly served as a written commitment against government retaliation, ironically, CISA’s disclaimer actually spelled out how the federal government’s multi-agency approach to censorship provided a number of avenues for government retaliation if the companies did not comply.

DHS’s efforts to assist with the reporting of “mis- and disinformation” on social media platforms pre-date the creation of CISA. Former CISA Director Christopher Krebs testified in a transcribed interview with the Committee and Select Subcommittee that CISA’s predecessor, the National Protection and Programs Directorate (NPPD), engaged in switchboarding prior to the creation of CISA.²⁵ After CISA’s creation, switchboarding continued throughout the 2020 election cycle, but was discontinued for the 2022 election.²⁶

DHS—in litigation and before the Committee—has insisted that CISA’s “switchboarding” role was only that of an intermediary facilitating the sharing of reports, but not playing a substantive role in the “misinformation” reporting process. For example, DHS Secretary Mayorkas testified to the Committee in July 2023 that “what it amounted to was serving as an intermediary between election officials and social media companies; *we were not making a judgment.*”²⁷ Head of CISA’s Countering Foreign Influence Task Force, Brian Scully, testified during his deposition in *Missouri v. Biden* that switchboarding was “CISA’s role in forwarding reporting received from election officials . . . to social media platforms.”²⁸ But documents obtained by the Committee and Select Subcommittee reveal that “switchboarding”

²¹ Email from Alex Stamos to Nextdoor employee (Aug. 4, 2020, 4:33 PM) (on file with the Comm.).

²² *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 209 (Deposition of Brian Scully) (hereinafter “Scully Dep.”) at 17:1–8.

²³ *Id.* at 62:15–22.

²⁴ *Hearing on the Oversight of the U.S. Department of Homeland Security Before the H. Comm. on the Judiciary*, 118th Cong. (July 26, 2023).

²⁵ House Judiciary Committee’s Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 7–8 (on file with the Comm.).

²⁶ Scully Dep., *supra* note 22, at 21:19–22:14.

²⁷ *Hearing on the Oversight of the U.S. Department of Homeland Security Before the H. Comm. on the Judiciary*, 118th Cong. (July 26, 2023) (emphasis added).

²⁸ Scully Dep., *supra* note 22, at 23:24–24:2.

From: Scully, Brian [redacted]@cisa.dhs.gov
Sent: 11/3/2020 4:22:20 PM
To: [redacted]@fb.com
CC: Masterson, Matthew [redacted]@cisa.dhs.gov; [redacted]@fb.com
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Both a and b are correct. Not a poll worker and no ballots destroyed.

Brian

Brian Scully
 DHS Countering Foreign Interference Task Force
 National Risk Management Center
 [redacted]
 [redacted]@cisa.dhs.gov

From: [redacted]@fb.com>
Sent: Tuesday, November 3, 2020 4:18:42 PM
To: Scully, Brian [redacted]@cisa.dhs.gov>
Cc: Masterson, Matthew [redacted]@cisa.dhs.gov>; [redacted]@fb.com>
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hello again, wanted to follow up on a few points just to be crystal clear -- could you please confirm that (a) the worker in question is not a pollworker, or (b) that he did not, in fact, destroy ballots (or at least that there is no evidence that he destroyed ballots).

Would appreciate this clarity tremendously. Thank you so much.

From: [redacted]@fb.com>
Sent: Tuesday, November 3, 2020 3:57:18 PM
To: Scully, Brian [redacted]@cisa.dhs.gov>
Cc: Masterson, Matthew [redacted]@cisa.dhs.gov>
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Appreciate the swift response!!

From: Scully, Brian [redacted]@cisa.dhs.gov>
Sent: Tuesday, November 3, 2020 3:52:45 PM
To: [redacted]@fb.com>
Cc: Masterson, Matthew [redacted]@cisa.dhs.gov>
Subject: Fwd: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Statement from PA. Confirms person was not poll worker.

Brian

Tranche 2

CISA to HJC 3/22/23 Letter & 4/28/23 Subpoena
Page 000470

Brian Scully
 DHS Countering Foreign Interference Task Force
 National Risk Management Center
 [redacted]
 [redacted]@cisa.dhs.gov

From: CFITF [redacted]@hq.dhs.gov
Sent: Tuesday, November 3, 2020 3:43:52 PM
To: CFITF All [redacted]@hq.dhs.gov
Subject: FW: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

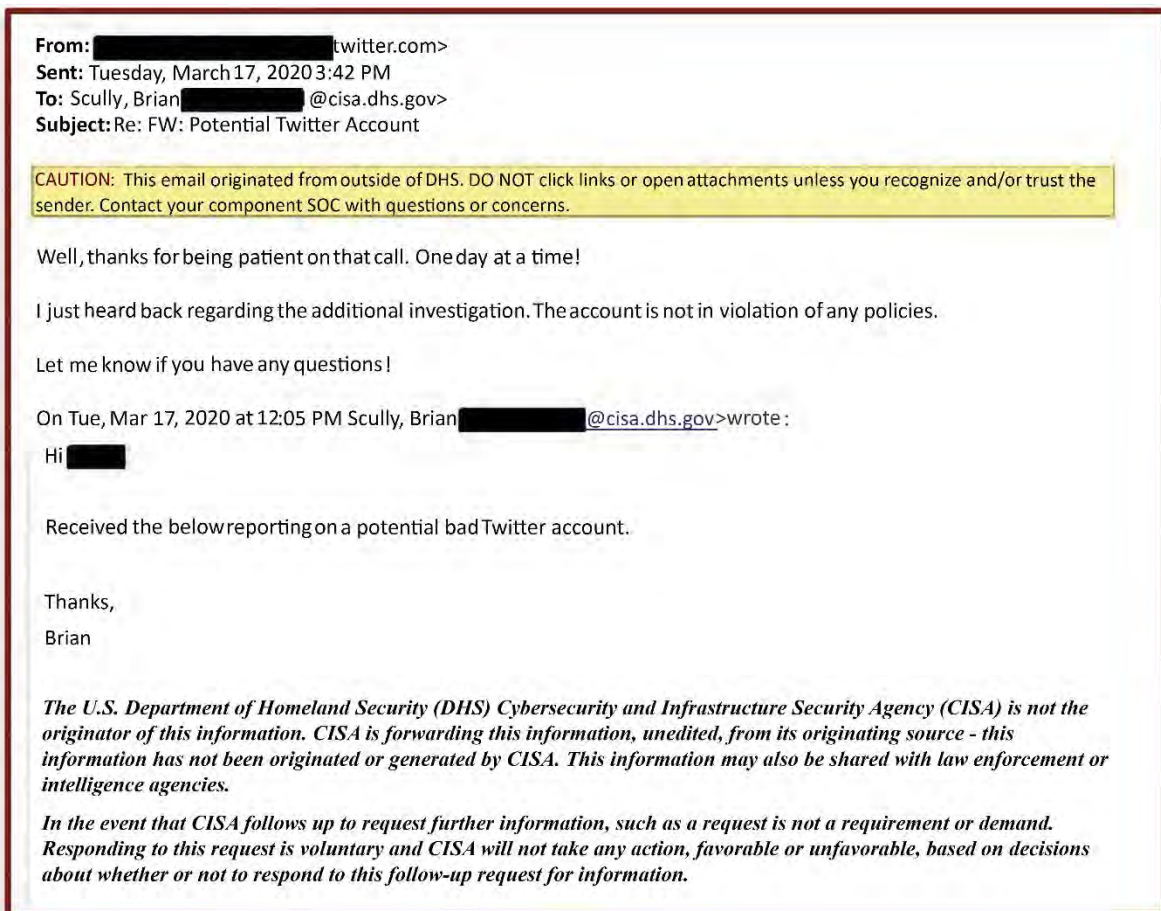
From: [redacted]@cisecurity.org
Sent: Tuesday, November 3, 2020 8:43:42 PM (UTC+00:00) Monrovia, Reykjavik
To: CFITF
Subject: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Reply above this line

[redacted]@cisecurity.org commented:
 The county has issued an official statement on the matter:

In addition to CISA substantively weighing in or commenting on the misinformation reports being shared with the social media companies, CISA could also attempt to influence the social media companies' decisions by deciding whether—and how many times—to follow up. Based on documents obtained by the Committee pursuant to a subpoena to CISA, starting in or around March 2020, used a disclaimer that stated that DHS and CISA were not the “originating source” of the misinformation report, but that the report “may also be shared with law enforcement or intelligence agencies.”³¹ The disclaimer continued: “In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.”³²

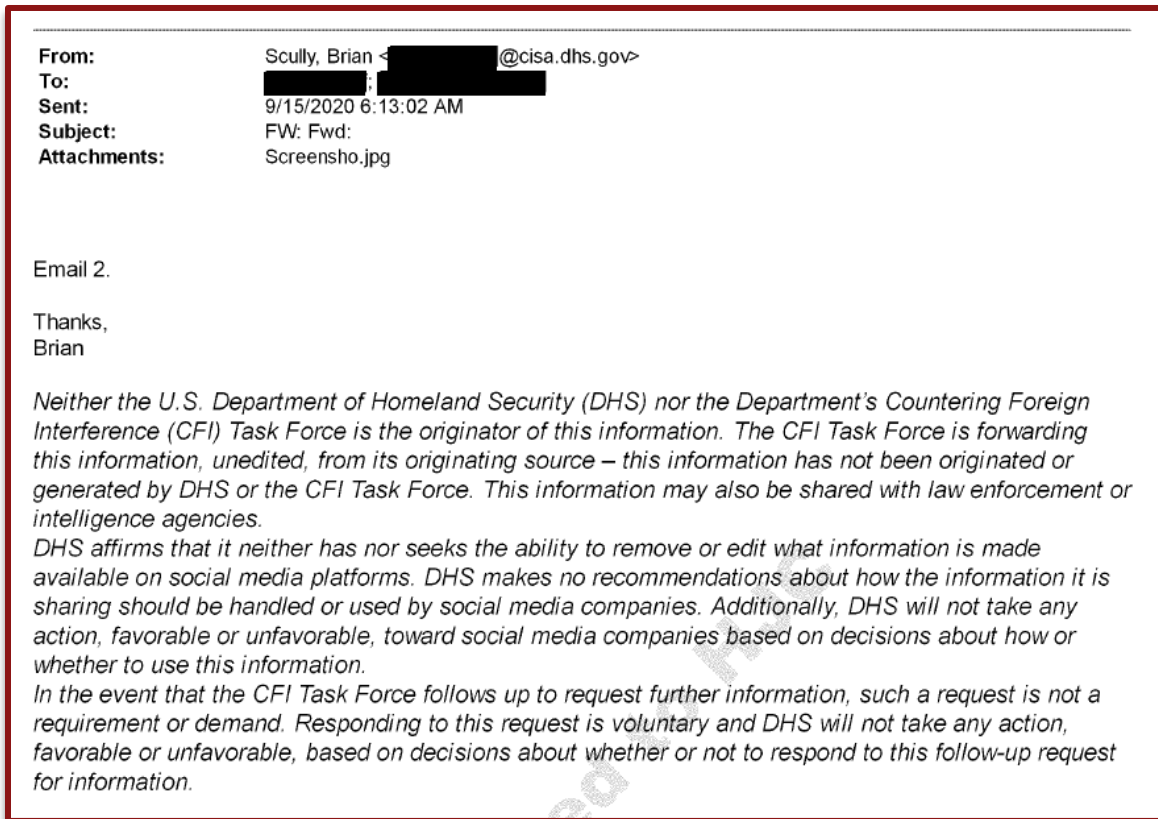


By September 2020, CISA’s switchboarding emails began to include an extra paragraph declaring that “DHS affirms that it neither has nor seeks the ability to remove what information is made available on social media platforms,” but it notably continued to leave open the possibility that the “information may also be shared with law enforcement or intelligence

³¹ Email from Brian Scully to Twitter employee (Mar. 17, 2020, 12:05 PM) (on file with the Comm.).

³² *Id.*

agencies.”³³ Put plainly, a lawyer for one of the social media companies would see that DHS *and* law enforcement agencies (such as the FBI) may know the company received the misinformation report, but only DHS committed to not take any unfavorable action against the company based on the company’s “decisions about how or whether to use this information”—i.e., the FBI or other law enforcement agencies may take action if the social media company did not censor appropriately.



The following month, CISA appeared to narrow the language of the disclaimer to state that CISA (rather than all of DHS) would not “take any action favorable or unfavorable, based on decisions about how or whether to use this information.”³⁴ The more limited disclaimer now stated only that: “*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies.*”³⁵ CISA also removed an entire paragraph of its disclaimer referencing follow-up communications.³⁶ In the ongoing federal litigation *Missouri v. Biden*, the Biden Administration cited the inclusion of this disclaimer as evidence that CIS and the EIP were not “‘censorship partners’ with CISA” and that the disclaimer supported companies to apply their policies

³³ Email from Brian Scully to Facebook employees (Sept. 15, 2020, 6:13 AM) (on file with the Comm.).

³⁴ *Cf. id.*; email from Brian Scully to Facebook employees (Oct. 1, 2020, 2:23 PM) (on file with the Comm.).

³⁵ *See, e.g.*, Brian Scully to Facebook employees (Oct. 1, 2020, 2:23 PM) (on file with the Comm.) (emphases added).

³⁶ *Id.*

“independently.”³⁷ But as described above, rather than ensure that companies did not feel pressure, the revised disclaimer emphasized that CISA would involve law enforcement agencies and that CISA would not (or could not) commit that law enforcement agencies would not take an unfavorable action based on how the social media platforms decided to respond to the misinformation report.

On Tue, Oct 27, 2020 at 4:09 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Please see below report from Washington.

Thanks,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

On or around October 28, 2020, CISA reinstated the paragraph in its disclaimer concerning follow-up communications.³⁸ To date, CISA has produced to the Committee and Select Subcommittee over twenty email threads dated between October 1, and October 27, in which the disclaimer does not include the paragraph regarding follow-up communications.³⁹

³⁷ See, e.g., Defs.’ Resp. to Pls.’ Proposed Findings of Fact in Supp. of Their Mot. for Prelim. Inj. at 547–548, Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 264-9.

³⁸ Cf. email from Brian Scully to Twitter employee (Oct. 27, 2020, 4:09 PM) (on file with the Comm.); email from Brian Scully to Twitter employee (Oct. 28, 2020, 6:29 PM) (on file with the Comm.).

³⁹ See, e.g., email from Brian Scully to Facebook employees (Oct. 2, 2020, 7:29 PM) (on file with the Comm.); email from CFITF to Facebook employees (Oct. 20, 2020, 2:11 PM) (on file with the Comm.).

On Wed, Oct 28, 2020 at 6:29 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:
Please see below report from Washington.

Regards,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source -- this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

Unsurprisingly, around this time, CISA began to follow-up with social media platforms about posts the agency had flagged, as seen in the example below.⁴⁰

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7F0C5C3963484338B25437EAAE765D72; [REDACTED]]
Sent: 10/19/2020 6:34:53 PM
To: [REDACTED]@twitter.com]
CC: [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@hq.dhs.gov]
Subject: RE: FW: Case #CIS-MIS000041: Twitter misinformation regarding ballots dumped on highway in CT

Checking in to see if there is anything that can be shared in regards to this reported incident.
[REDACTED]

From: [REDACTED]@twitter.com>
Sent: Thursday, October 15, 2020 11:42 AM
To: [REDACTED]@cisa.dhs.gov>
Cc: [REDACTED]@twitter.com>; [REDACTED]@twitter.com>; [REDACTED]@twitter.com>; [REDACTED]@hq.dhs.gov>
Subject: Re: FW: Case #CIS-MIS000041: Twitter misinformation regarding ballots dumped on highway in CT

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi [REDACTED]
We will ask the team to review.

Best,
[REDACTED]

⁴⁰ Email from DHS official to Twitter employee (Oct. 19, 2020, 6:34 PM) (on file with the Comm.).

During his transcribed interview with the Committee, Matt Masterson, a former senior cybersecurity advisor at CISA, testified that there had been internal deliberations with CISA’s lawyers regarding the disclaimer and whether constitutional rights and civil liberties were implicated:

- Q. Do you recall any discussions during your tenure at CISA regarding if there are any constitutional implications if CISA’s work engaged with, we’ll say, misinformation, disinformation, malinformation, coming from domestic actors?
- A. I don’t recall a specific conversation around that. I recall that – obviously that CISA lawyers were involved, as I previously indicated, for instance, around the disclaimer conversation, including lawyers around constitutional and civil liberties. But I don’t know or recall the specifics of any given conversation around that.⁴¹

CISA’s inclusion of a disclaimer discussing whether CISA’s frequent emails should be interpreted as a request or whether the refusal to respond could result in “unfavorable” action is evidence that, at a minimum, the lawyers within DHS felt compelled to consider whether the practice of switchboarding was legally and constitutionally sound. But rather than end the practice (as CISA apparently did by the 2022 election), in the fall of 2020, CISA decided to push forward with its censorship efforts, appending a meaningless email disclaimer as a weak and transparent attempt to satisfy the glaring First Amendment concerns.

Crucially, CISA’s disclaimer included the ominous line: “This information may also be shared with law enforcement or intelligence agencies.”⁴² Whereas the disclaimer stated that “CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information,” the disclaimer makes no such guarantee about retaliation from the “law enforcement or intelligence agencies” with whom CISA may share the relevant social media content.⁴³

The threat of law-enforcement reprisal is amplified by the fact that the FBI would inform social media companies when CISA provided the FBI a “misinformation” report. The Committee and Select Subcommittee have obtained multiple documents that show that social media companies were aware that CISA was sharing information with federal intelligence and law enforcement agencies, including the FBI.⁴⁴

From: Elvis Chan
Date: Sunday, October 4, 2020 at 2:31 PM
To: [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]
Subject: Tipper & Next FITF Meeting
 Facebook folks,
 First, I got a tip from CISA that there is a Facebook page that is misleading voters about time, place, and manner of voting, as well as trying to elicit Facebook user information. Please review and take whatever steps you deem appropriate. We would appreciate it if you let us know whether you take any actions based on this referral.

⁴¹ House Judiciary Committee’s Transcribed Interview of Matthew Masterson (Sept. 26, 2023), at 81.

⁴² See, e.g., email from Brian Scully to Facebook employees (Oct 2, 2020, 7:29 PM) (on file with the Comm.).

⁴³ *Id.* (emphasis added).

⁴⁴ See, e.g., email from Elvis Chan to Facebook employees (Oct. 4, 2020, 2:31 PM) (on file with the Comm.).

In other words, CISA’s disclaimer indicated to the social media companies that CISA, law enforcement, and intelligence agencies may receive the misinformation report, but the disclaimer stated only that *CISA* would not retaliate against the social media companies if they failed to censor the flagged content. CISA made no promises with respect to what the FBI or one of the intelligence agencies may do. And the social media companies were well aware that CISA was forwarding some subset of the reports to the FBI (if not other federal law enforcement or intelligence agencies).

In his interview before the Committee and Select Subcommittee, former Facebook executive Alex Stamos testified that involvement with a law enforcement agency such as the FBI was necessarily more worrisome for companies than CISA, explaining that “you can’t have a casual chat with an FBI agent when you’re an executive at a company. It’s not safe. You end up with a \$3,000-an-hour row of people sitting next to you.”⁴⁵ Mr. Stamos continued:

Q. And what do you mean you can’t have a casual conversation with the FBI? Why is that?

A. I think defense attorneys would tell you that FBI agents are always looking out – you might feel like you’re having a friendly conversation with them, but you never know if you’re actually the target. And I think there has been a number of situations which companies have tried to engage the FBI because they were victims of, say, a cybercrime, and then they end up getting punished or their executives getting punished And so, you know, dealing with a law enforcement agency that has coercive powers is just a risky thing to do if you’re part of some big organization and some other – there might be some investigation involving the organization that you don’t even know about.

Q. That perspective you just shared with respect to the FBI, do you think it was widely shared by the executives at Facebook when you were at the company?

A. Certainly, the policy of the company was that an executive could not talk to the FBI without attorneys present

Q. . . . Even if the government represents that the interests are aligned, it could be the case that, later on, the government changes its mind. Is that right?

A. Yes.

Q. Okay. And this fact is well known by tech executives?

⁴⁵ House Judiciary Committee’s Transcribed Interview of Alex Stamos (June 23, 2023), at 188 (on file with the Comm.).

- A. Yes. And I think all executives of all public companies understand that *there's lots of parts of the government that can punish you for activity that you thought was appropriate.*⁴⁶

So why did CISA engage in this “resource intensive” process of switchboarding, go through the trouble of writing and rewriting a disclaimer in hopes of sidestepping serious constitutional concerns, and directly involve federal law enforcement and intelligence agencies? Because CISA wanted flagged content removed, and switchboarding provided an effective means to do so. During his deposition in *Missouri v. Biden*, senior CISA official Brian Scully admitted that CISA did, in fact, have an understanding that its reporting would lead to removal by the platforms.⁴⁷

2. EI-ISAC

The Center for Internet Security (CIS) is a non-profit organization based in New York, which was established “in partnership with the U.S. Cybersecurity and Infrastructure Security Agency (CISA).”⁴⁸ CIS operates the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which is funded alongside the Multi-State Information Sharing and Analysis Center (MS-ISAC) to the tune of \$27 million for FY 2024 for the two ISACs.⁴⁹ The EI-ISAC is an information-sharing channel used by state and local election officials to report alleged “mis- and disinformation” to social media platforms.⁵⁰ During the 2018 midterm election cycle, all fifty states were participating in the EI-ISAC.⁵¹ Moreover, according to witness testimony to the Committee and Select Subcommittee, EI-ISAC employees are considered CIS employees.⁵²



According to the EIP’s report, in the 2020 election cycle, “the EI-ISAC served as a singular conduit for election officials to report false or misleading information to platforms.”⁵³ The report also explained EI-ISAC’s function in relation to CIS: “By serving as a one-stop

⁴⁶ *Id.* at 188–190 (emphasis added).

⁴⁷ Scully Dep., *supra* note 22, at 17:15–21.

⁴⁸ *EI-ISAC Charter*, CENTER FOR INTERNET SEC., <https://www.cisecurity.org/ei-isac/ei-isac-charter> (last visited Nov. 3, 2023).

⁴⁹ DEP’T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY BUDGET OVERVIEW FISCAL YEAR 2024 CONGRESSIONAL JUSTIFICATION, at 37 (2023).

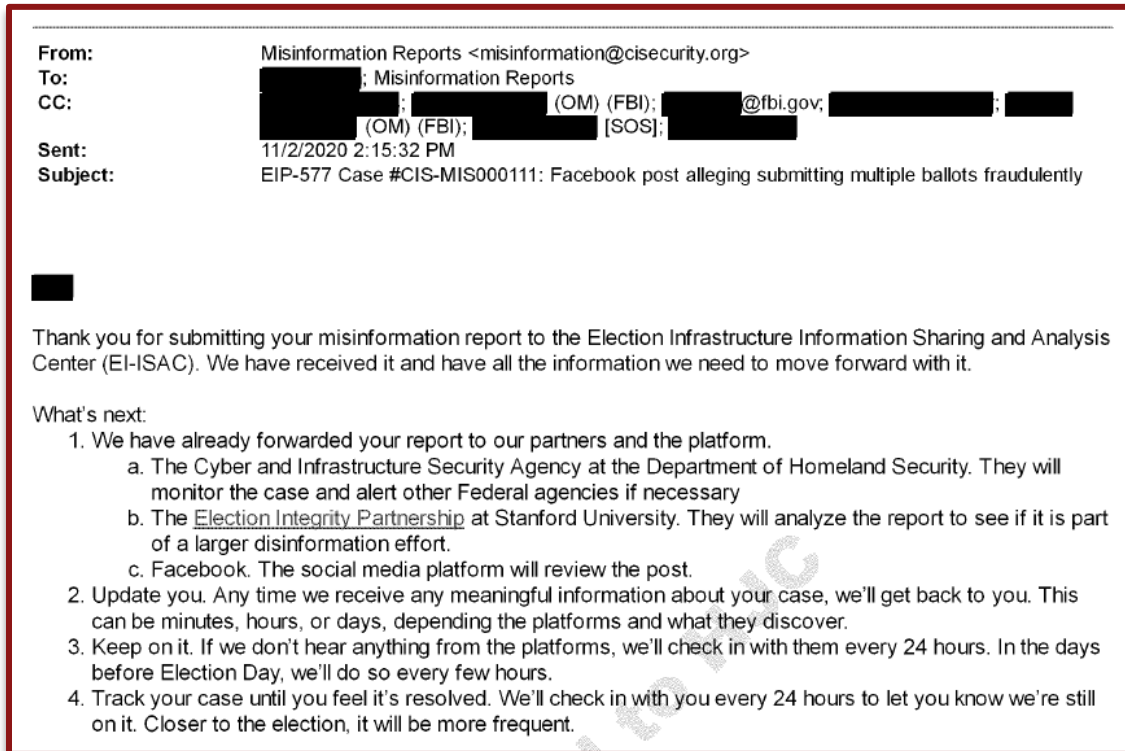
⁵⁰ ELECTION INTEGRITY P’SHP, *supra* note at 16, at 13.

⁵¹ House Judiciary Committee’s Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 34.

⁵² House Judiciary Committee’s Transcribed Interview of Matthew Masterson (Sept. 26, 2023), at 184.

⁵³ ELECTION INTEGRITY P’SHP, *supra* note at 16, at 13.

reporting interface, the EI-ISAC allowed election officials to focus on detecting and countering election misinformation while CIS and its partners reported content to the proper social media platforms.”⁵⁴ And the report described CISA’s role, noting that “the Countering Foreign Influence Task Force (CFITF), a subcomponent of CISA, aided in the reporting process and in implementing resilience efforts to counter election misinformation.”⁵⁵ The misinformation reports submitted to the EI-ISAC in the lead-up to the 2020 election were “also routed to the EIP ticketing system.”⁵⁶



Like switchboarding, the EI-ISAC operated as an intermediary between state and local election officials and the social media platforms, offering a centralized reporting mechanism in an effort to remove content from social media.⁵⁷ For example, on November 2, 2020, a state election official submitted a report of alleged misinformation to the EI-ISAC, which, in turn, forwarded the report to the relevant platform.⁵⁸ According to the EI-ISAC’s response to the state official, the EI-ISAC also shared the report with both CISA and the EIP.⁵⁹

⁵⁴ *Id.*

⁵⁵ *Id.* In January 2021, CISA transitioned its Countering Foreign Influence Task Force to promote more flexibility to focus on general MDM, or so-called “Mis-, Dis-, and Malinformation.” According to CISA’s website in February 2023, the MDM team was “charged with building national resilience to MDM and foreign influence activities,” and its efforts applied to “foreign and domestic” actors.

⁵⁶ *Id.*

⁵⁷ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS, at 22 (Comm. Print June 26, 2023).

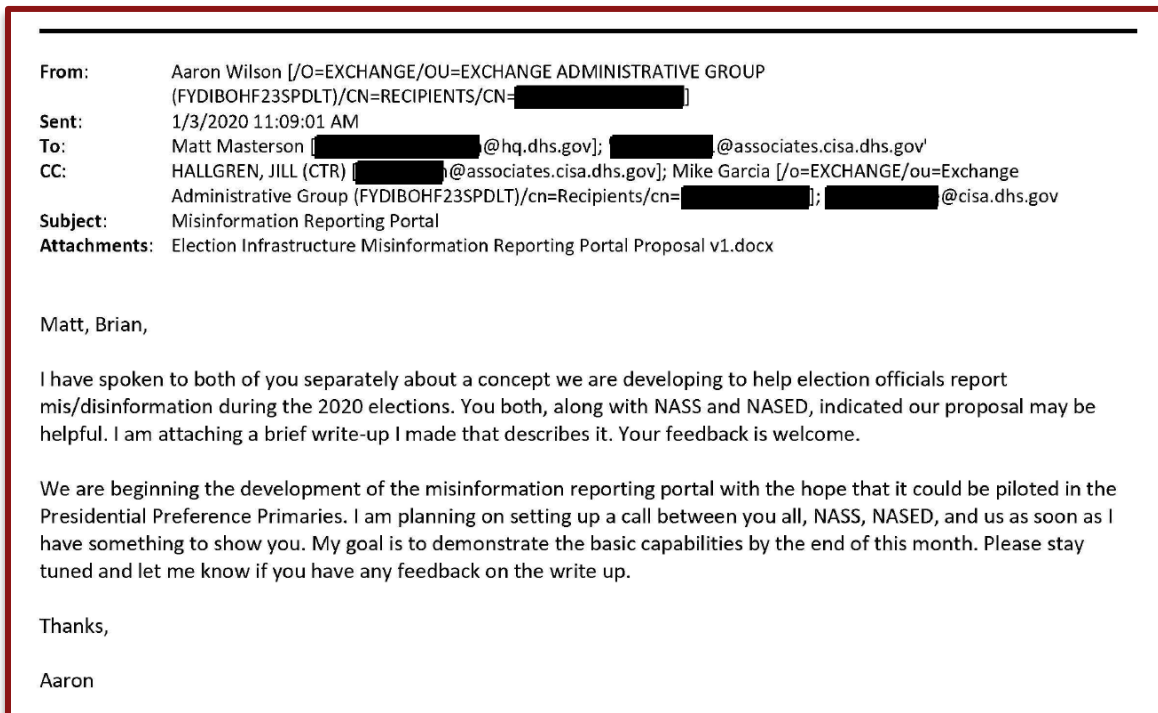
⁵⁸ Email from misinformation@cisecurity.org to Iowa state government official (Nov. 2, 2020, 2:15 PM) (on file with the Comm.).

⁵⁹ *Id.*

3. Misinformation Reporting Portal

Even with switchboarding and the EI-ISAC, CISA and CIS had discussions internally and with social media companies throughout the first half of 2020 on whether to create a “misinformation reporting portal.” Pursuant to multiple subpoenas, the Committee and Select Subcommittee have obtained documents revealing CISA’s and CIS’s efforts to pursue a third avenue of “misinformation reporting.”

As early as January 2020, CISA officials were in discussions with CIS to establish a “misinformation reporting portal.”⁶⁰ On January 3, Aaron Wilson, the Senior Director of Election Security at CIS, sent an email to senior CISA officials Matt Masterson and Brian Scully, among others, writing: “I have spoken to both of you separately about a concept we are developing to help election officials report mis/disinformation during the 2020 elections. You both . . . indicated our proposal may be helpful.”⁶¹ Mr. Wilson indicated that his goal was “to demonstrate the basic capabilities [of the misinformation reporting portal] by the end of this month.”⁶²



⁶⁰ Email from Aaron Wilson to Matt Masterson, Jill Hallgren, and Mike Garcia (Jan. 3, 2020, 11:09 AM) (on file with the Comm.).

⁶¹ *Id.*

⁶² *Id.*

CIS and CISA’s joint efforts were even briefed to law enforcement in January 2020 with CIS reaching out to the FBI, stating that “CIS is *working with DHS* on a misinformation reporting portal. The intent is to build a web portal to manage the reporting of election infrastructure misinformation from local and state election officials to the social media platforms. We are working with our partners at the National Association of Secretaries of States (NASS), National Association of State Election Directors (NASED), *and DHS* to vet this idea. We are currently building a prototype and will have something to show by the first week of February.”⁶³

From: Aaron Wilson [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=██████████]
Sent: 1/20/2020 2:09:04 PM
To: ██████████@fbi.gov
CC: Wedekind, Kirby (██████████@hq.dhs.gov); HALLGREN, JILL (CTR) (██████████@associates.cisa.dhs.gov); Scully, Brian (██████████@cisa.dhs.gov); Josiah, Chad (██████████@cisa.dhs.gov); Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=██████████]
Subject: Misinformation Reporting Portal FBI Briefing

JC,

It was great to meet you last week. As I mentioned, CIS is working with DHS on a misinformation reporting portal. The intent is to build a web portal to manage the reporting of election infrastructure misinformation from local and state election officials to the social media platforms. We are working with our partners at the National Association of Secretaries of States (NASS), National Association of State Election Directors (NASED), and DHS to vet this idea. We are currently building a prototype and will have something to show by the first week of February.

Given the FBI’s role, I’d like to bring you up to speed on our efforts and get your feedback on this effort, and hopefully your engagement. Our primary goals are to:

- Provide election officials a single place/POC to report misinformation
- Ease the burden on election officials when they go to report the misinformation
- Collect the information necessary for the FBI, DHS, and social media platforms to do their jobs
- Expedite and enhance the process by which social media companies are made aware of the misinformation
- Provide visibility about what election officials are reporting to: other election officials, DHS, NASS, NASED, FBI, etc.
- Facilitate information sharing between election officials about what they are seeing, what to look out for, etc.
- Provide meaningful feedback to election officials on the status of their misinformation reports

Are you available for a call this week to discuss more?

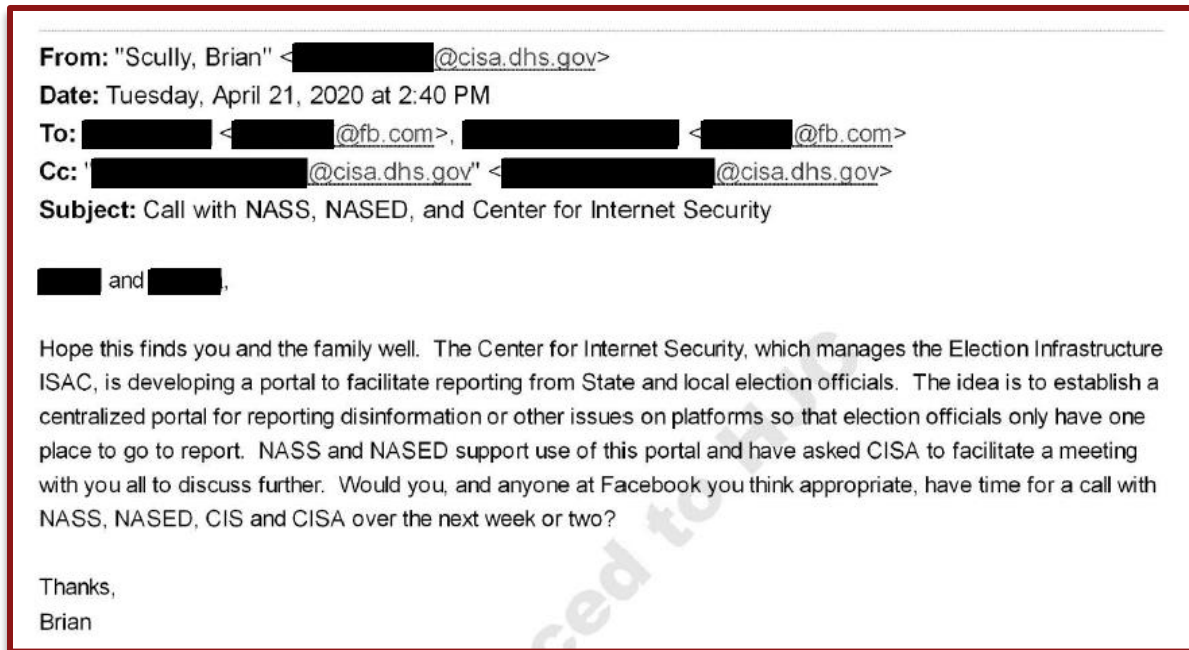
Thanks,

Aaron

CISA assumed an active role in promoting CIS’s proposal for a misinformation reporting portal, facilitating meetings between the relevant third-party non-profits and social media platforms. On April 21, 2020, for example, Brian Scully sent an email to two Facebook employees, in which Scully wrote: “The idea is to establish a centralized portal for reporting dis-

⁶³ Email from Aaron Wilson to Kirby Wedekind, Jill Hallgren, Brian Scully, Chad Josiah, and Mike Garcia (Jan. 20, 2020, 2:09 PM) (on file with the Comm.) (emphases added).

information or other issues on platforms so that election officials only have one place to go to report.”⁶⁴



But planning for a CIS-CISA misinformation reporting portal had hit a roadblock by May 2020. According to the internal notes of a call between Facebook employees and DHS personnel regarding a “Misinformation Reporting Portal,” “*DHS cannot openly endorse the portal*, but has behind-the-scenes signaled that [the National Association of Secretaries of State]/[the National Association of State Election Directors] has told them it would be easier for many states to have ‘one reporting channel’ and CISA and its ISAC would like to have incoming the same time that the platforms do.”⁶⁵ Less than two months later, the EIP would be established to serve that very purpose.

⁶⁴ Email from Brian Scully to Facebook employees (Apr. 21, 2020, 2:40 PM) (on file with the Comm.).

⁶⁵ Email from Facebook employee to Facebook employees (May 31, 2020, 10:44 AM) (on file with the Comm.) (emphasis added)

From: [REDACTED] <[REDACTED]@fb.com>
 Sent: Sunday, May 31, 2020 10:44 AM
 To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
 Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
 Subject: CIS & NASS/NA SED & DHS Call

Team,

Wanted to share a read-out from our call late Friday with DHS, NASS & NASED. Great job by [REDACTED] & [REDACTED]

No action for us now, however, we will reconvene after a Beta test of their proposed reporting portal in the next few weeks.

Best,
 [REDACTED]

TL;DR: On May 29, U.S. Public Policy ([REDACTED]), P&G Outreach ([REDACTED]), and Security Policy ([REDACTED]) met with DHS, the Center for Internet Security, and NASS/NA SED about a **"Misinformation Reporting Portal"** that CIS is developing for state and local-level elections officials to report mis/disinformation and IO-type activity concerning election interference to the platforms, with a focus on Facebook, Twitter, and Google. Following a beta test CIS will do in Florida, Colorado, North Carolina, and Rhode Island in early June, they would like to do a demo for Facebook. Internally, Facebook would prefer our independent reporting channel which makes us an industry leader, and was reported as successful by all parties on this call and is monitored 24/7, but we are aware that if the majority group moves towards a centralized channel, there are PR challenges for not participating.

o **Highlights:**

- **DHS cannot openly endorse the portal** but has behind-the-scenes signaled that NASS/NA SED has told them it would be easier for many states to have "one reporting channel" and CISA and its ISAC would like to have incoming the same time that the platforms do.
- CIS is in discussions with **Twitter** to gauge their interest, and it was unclear what engagement has been with **Google**
- CIS is talking with **Graphika**, which has said it is interested in nationwide trends that the reporting portal may reveal.
- CIS is talking with the **Belfer Center**, which is developing an "IO Playbook & Training" that may be released in the coming months before November 2020.
- NASS/NA SED is supportive, but **not all the states are onboard** – CIS said they would like to launch with platforms supportive and engaged and bring states incrementally along.
- **CIS would like some sort of API with Facebook** – such a set up may be impossible, and CrowdTangle, if this progresses, may be the way to go.

CONFIDENTIAL TREATMENT REQUESTED -
NOT FOR DISTRIBUTION - MEMBERS & STAFF ONLY

META-118HJC-0026420

3. To what extent can the U.S. government, other platforms, and others view back and forth with platforms and also cross-platform content or escalations, and how will this be controlled? Are you open to a version of the portal that forwards intake to a platform email, with further back and forth being handled just between the platform and the reporter (but the initial report is available to other states/platforms/portal users).
4. How will portal access be determined?
5. What is the limit on the number of people and organizations who will have access to the portal?
6. What is the data retention period for the portal?
7. Is it the expectation that the portal will be a short-term or long-term project?
8. How will the portal sort information so that it is of importance and properly sorted by various terms of service depending on the platform, so that recipients of the information will be able to triage it quickly and deconflict?
9. What quality control measures will be in place to ensure that the escalations sent to the portal are not "noise" and will be properly described and not duplicative, and also not repeats of the same already-escalated content, to avoid burdening resource, operational, and engineering bandwidth during a very high-stakes election cycle where timely response and action will be critical?
10. Is the expectation that the portal will replace the dedicated 1:1 reporting channels maintained by the platforms, either in the short or long terms?
11. How will the portal advise whether or not a particular escalation has already been reported to the platforms and avoid sending an alert when such an escalation has already been made?
12. To what extent can the portal be used to surface trends and patterns across platforms that can be shared, if of value, while maintaining direct platform-level communication from the states?
13. Which states are not yet onboarded to the portal and what is the plan for those states?
14. How will the portal be made user-friendly for the wide range of users?
15. Who will train users on the portal, trouble shoot, and provide tech support for the portal?
16. What will turn around time, both before the election, and on election day, for portal support and login issues?
17. How long does it take to approve access to the portal? Will there be expedited review closer to the election?
18. How will the portal enable platform-specific back and forth?
19. Will the portal provide links and not just screenshots to enable swift actioning of context?
20. How does the portal plan to surface behavior-type or pattern-type signals, as opposed to discrete pieces of content?
21. How will the portal prevent the same escalation being reported multiple times by multiple sources?
22. Aside from receiving "intake," and evaluating that, if possible, pursuant to platform-specific terms of service, what are other expectations of engagement from the platforms?

Twitter was initially briefed on the portal in May 2020, according to a meeting agenda produced to the Committee.⁶⁷ Per the agenda, “DHS appreciates the efforts of Twitter to help improve the ability of elections officials to submit mis/disinformation.”⁶⁸ The agenda was also indicative of CISA’s and the broader federal government’s effort to enhance the censorship operation through the portal: “Hopefully, this effort will streamline and make more efficient the process that has been improving over the past several years, but is still far from efficient and effective from the perspective of the elections community and Federal government.”⁶⁹ As indicated in the excerpt below, top CISA officials were scheduled to open this discussion on CIS’s potential misinformation reporting portal.⁷⁰

Misinformation Reporting Portal Discussion with Twitter

May 11, 2020, 2pm to 3pm ET

VTC Dial in information: **TBD**

Agenda and Candidate Discussion Points

Welcome – Brian Scully, CISA or Matt Masterson, CISA

- DHS appreciates the efforts of Twitter to help improve the ability of elections officials to submit mis/disinformation (e.g., the recent addition of an electronic submission capability). Also, we appreciate the opportunity to have a discussion with Twitter about the use of a Portal to improve the ability of elections officials to report mis/disinformation and to provide elections officials with visibility of similar reports and across platforms. Hopefully, this effort will streamline and make more efficient the process that has been improving over the past several years, but is still far from efficient and effective from the perspective of the elections community and Federal government.

⁶⁷ Center for Internet Sec., Misinformation Reporting Portal Discussion with Twitter (May 11, 2020) (unpublished meeting agenda) (on file with the Comm.).

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ *Id.*

Like Facebook, Twitter also submitted a list of questions to CIS regarding the portal.⁷¹

From: [REDACTED] [REDACTED]@twitter.com
Sent: 6/16/2020 3:59:09 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Aaron Wilsonb0d]
CC: [REDACTED] [REDACTED]@twitter.com]; Scully, Brian [REDACTED]@cisa.dhs.gov]; Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]; Snell, Allison [REDACTED]@cisa.dhs.gov]; John Gilligan [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/[REDACTED]]; [REDACTED] [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Amanda Burkart66d]; Amy Cohen [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Maria Benson [REDACTED]@sso.org]; Leslie Reynolds [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; [REDACTED] [REDACTED]@twitter.com]; [REDACTED] [REDACTED]@twitter.com]; [REDACTED] [REDACTED]@twitter.com]
Subject: Re: Reporting Portal with CIS, NASS, NASED and Twitter

All,

Below are some of the questions we hope to discuss during our next call. Looking forward to it!

[REDACTED]

These documents demonstrate that CISA and CIS caused the social media companies to seriously question and entertain the proposal for a misinformation reporting portal, although the portal was not ultimately established.

- 1.
2. Will there be some sort of agreement or terms of reference that will align all participants (reporters, government entities, companies) on objectives and usage of the portal?
- 3.
- 4.
5. Who will have access to view/analyze reported information? Will there be any restrictions in place to dictate what can be done with this information?
- 6.
- 7.
8. Would other companies have access to see reports for other platforms? What if the report has content from multiple companies?
- 9.
- 10.
11. What is the criteria used to determine who has access to the portal? How many individuals do you anticipate having access?
- 12.
- 13.
14. How long will reported information be retained?
- 15.
- 16.
17. How long will the portal be in operation? Just through the 2020 presidential election?
- 18.
- 19.

CONFIDENTIAL-NON-PUBLIC INFORMATION-PROVIDED TO CONGRESS IN RESPONSE TO SUBPOENA CIS-JUDCOM0000070_Confidential

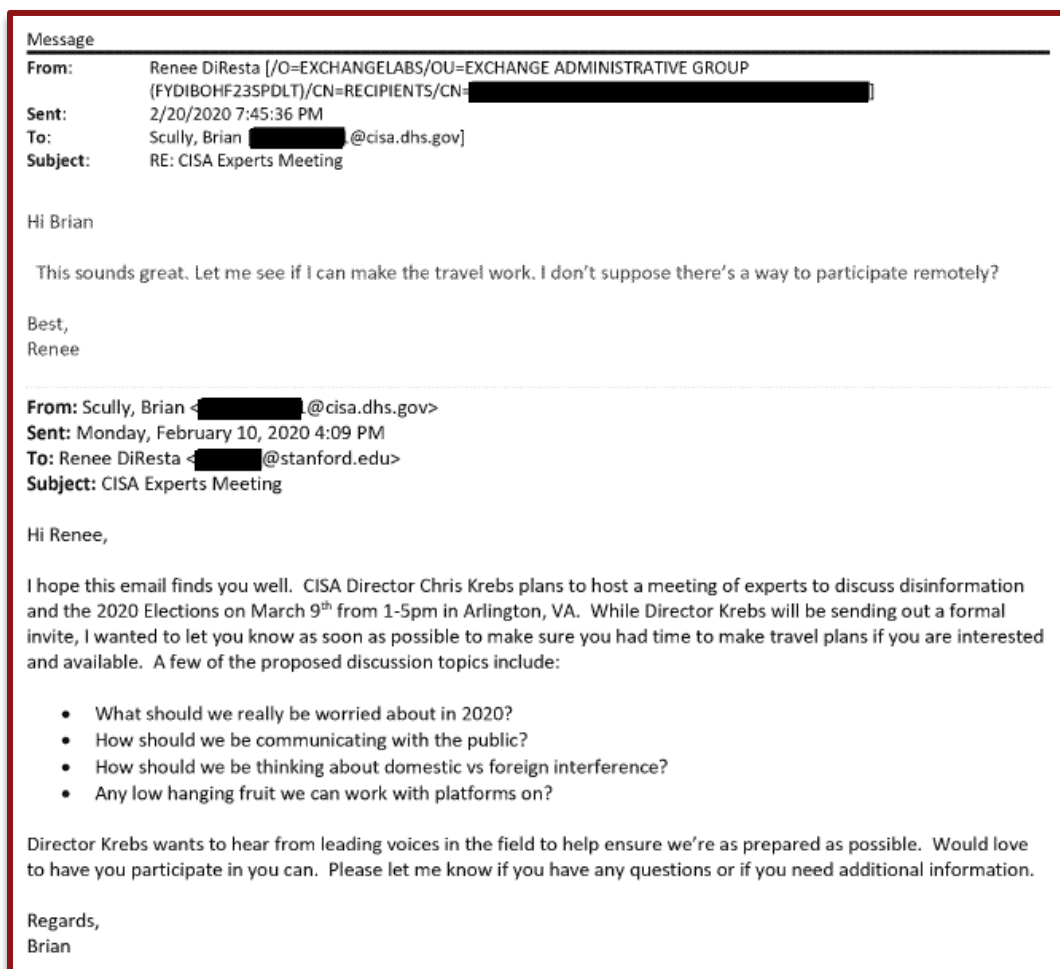
20. Companies' terms of service vary. How will individuals know what to report?
- 21.
- 22.
23. Will there be any quality checks in place? Will there be a review of reports before they are submitted to companies? Will all reports be treated with equal priority?
- 24.
- 25.
26. Will partners continue to use Partner Support Portal (PSP) or will everyone migrate to this reporting tool?

⁷¹ Email from Twitter employee to Aaron Wilson, Brian Scully, Matthew Masterson, and other personnel from CISA, CIS, and Twitter (June 16, 2020, 3:59 PM).

4. CISA Did Not Distinguish Foreign and Domestic Actors on Social Media

Finally, in the midst of operating or considering up to three different avenues of “misinformation reporting” (switchboarding, EI-ISAC, and the “misinformation reporting portal”), by early 2020, CISA had dropped any pretense of focusing only on foreign disinformation, openly discussing how to best monitor and censor the speech of Americans.

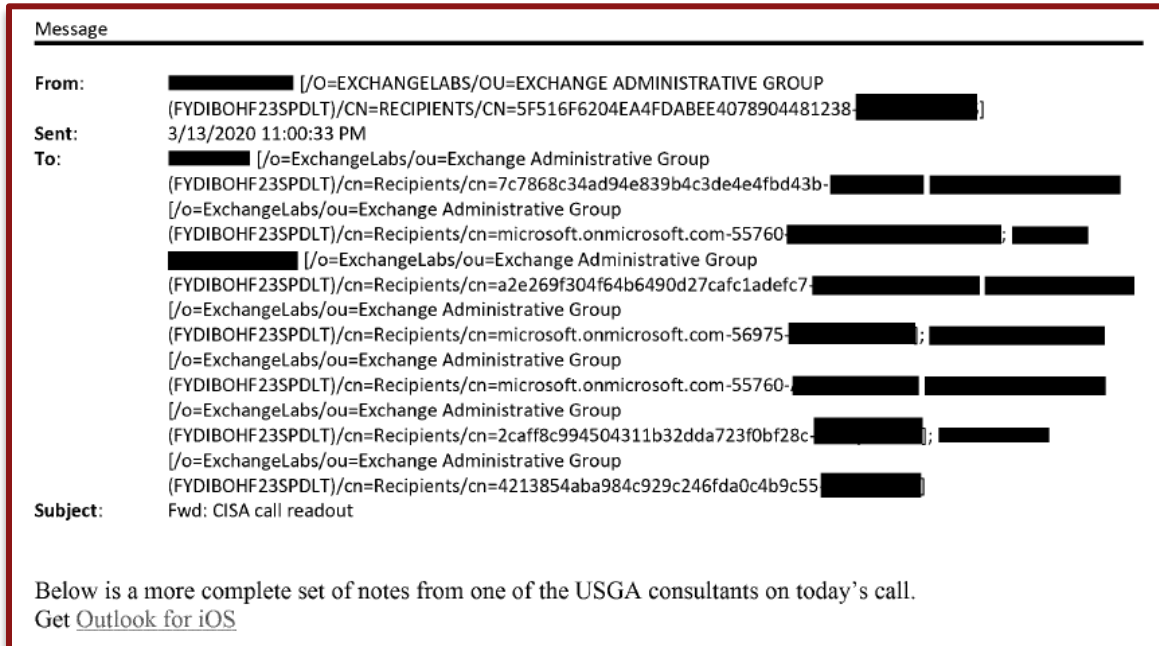
On February 20, 2020, Brian Scully, the head of CISA’s Countering Foreign Influence Task Force (CFITF), sent an email to the SIO’s Renée DiResta, inviting her to a meeting hosted by CISA Director Krebs, “to discuss disinformation and the 2020 Elections.”⁷² Scully provided a list of agenda items in the email, including: “How should we be thinking about domestic vs foreign interference?” and “Any low hanging fruit we can work with platforms on?”⁷³



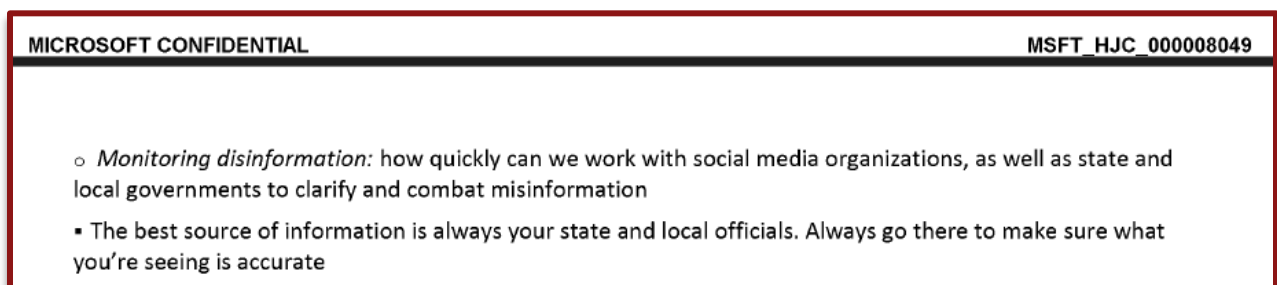
⁷² Email from Brian Scully to Renée DiResta (Feb. 20, 2020, 4:09 PM) (on file with the Comm.).

⁷³ *Id.*

The COVID-19 pandemic reinforced CISA’s desire to take a more active role in surveillance and censorship on social media. On March 13, 2020, Director Krebs participated in a “broad stakeholder conference call to provide an update regarding current activities related to” COVID-19.⁷⁴



According to internal Microsoft notes from the call obtained by the Committee pursuant to a subpoena to Microsoft, Krebs identified “Monitoring disinformation” as one of four “core lines of effort,” asking “how quickly can we work with social media organizations, as well as state and local governments to clarify and combat misinformation.”⁷⁵



⁷⁴ Email from Microsoft employee to Microsoft employees (Mar. 13, 2020, 11:00 PM) (on file with the Comm.).

⁷⁵ *Id.*

In his testimony before the Committee, Krebs stated unequivocally on multiple occasions that CISA did not treat content on social media differently based on its domestic or foreign origin.⁷⁶ At one point, Krebs even described the name of CISA’s Countering Foreign Influence Task Force as “a misnomer.”⁷⁷ Krebs further testified:

- Q. Was there an effort during this time to try to determine if the source was domestic or foreign?
- A. So, we certainly would look to the intelligence community if they made a determination on foreign threat actor intelligence. But, again, as these things pop up, things like “hammer and scorecard,” it doesn’t necessarily matter whether it’s foreign or domestic. Again, our authorities are rooted in the Homeland Security Act, which enables us to act on domestic or foreign threats. And, again, they don’t come waving a flag⁷⁸

Director Krebs reiterated CISA’s approach of treating foreign and domestic activity on social media in the same way in the context of CISA’s “Rumor Control” initiative.⁷⁹ For example, he testified:

- Q. When did these discussions regarding domestic influence first start?
- A. I don’t recall.
- Q. Okay. Were they ongoing by the beginning of 2020?
- A. Again, I don’t recall the moment in time or the periods of time within which we were thinking about the distinction between domestic and foreign interference. Again, I think this gets to, as we ultimately saw with rumor control, narratives are narratives, and we’re providing explanation on how the things actually work. So, again, it would not matter if it was foreign or domestic for the context, again, of rumor control.⁸⁰

⁷⁶ See e.g., House Judiciary Committee’s Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 153–154 (on file with the Comm.).

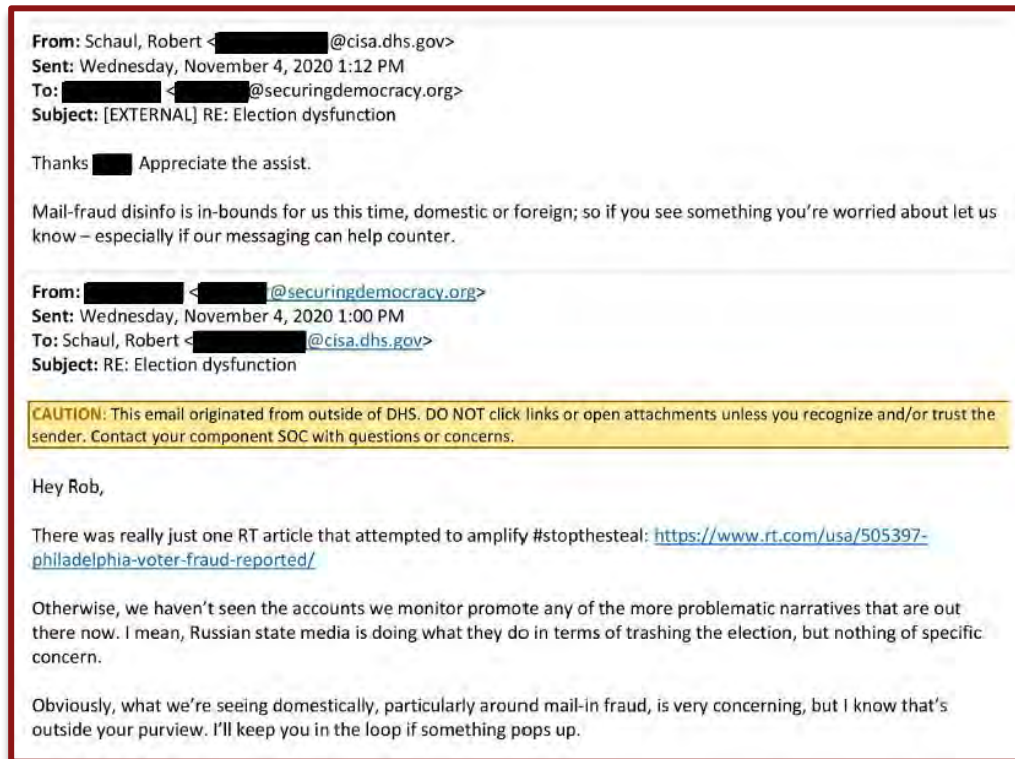
⁷⁷ *Id.* at 154.

⁷⁸ *Id.*

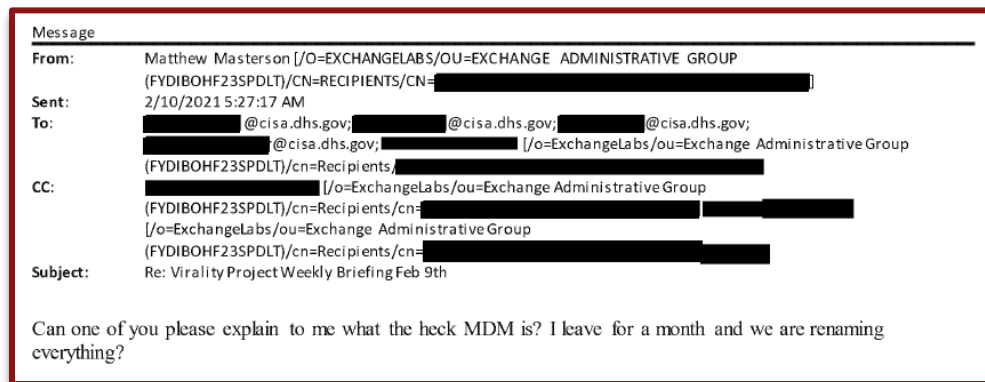
⁷⁹ One telling exchange between Mr. Krebs’s counsel and counsel for the Committee regarded whether any authorities limit CISA’s rights to combat so-called “misinformation.” Mr. Krebs’s counsel appeared to dismiss what role, if any, the First Amendment played with respect to restricting CISA’s ability to monitor and censor speech, demanding that the Committee cite a legal authority “other than the First Amendment” to justify its line of questioning. House Judiciary Committee’s Transcribed Interview of Chris Krebs (Oct. 11, 2023), at 162 (on file with the Comm.).

⁸⁰ *Id.* at 104.

Up to and through the 2020 election, CISA considered its authority as extending to domestic speech, not just foreign disinformation.⁸¹



In early 2021, CISA dropped the “misnomer” of the “Countering *Foreign* Influence Task Force” and became the “Mis-, Dis-, and Malinformation Team.”⁸² In spring 2023—following the *Missouri v. Biden* lawsuit, the Twitter Files reporting, and the Committee’s investigation—CISA removed all references on its website that its MDM team was censoring domestic speech too.⁸³



⁸¹ See, e.g., Email from Robert Schaul to Alliance for Securing Democracy Employee (Nov. 4, 2020 1:12 PM) (on file with the Comm.).

⁸² *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, Dep’t of Homeland Sec. Office of Inspector Gen., at 7 (Aug. 10, 2022), <https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf>.

⁸³ See STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS*, at 32–34 (Comm. Print June 26, 2023).

B. Creation of the EIP

Unable to proceed with its original plan, CISA enlisted Stanford to launder its censorship operation. On July 8, 2020, Stanford Internet Observatory (SIO) Director Alex Stamos sent an email to Dr. Kate Starbird at the University of Washington’s Center for an Informed Public (CIP), writing: “We are working on some election monitoring ideas with CISA and I would love your informal feedback before we go too far down this road . . . [T]hings that should have been assembled a year ago are coming together quickly this week.”⁸⁴

On Jul 8, 2020, at 9:41 AM, Alex Stamos <[REDACTED]@stanford.edu> wrote:

Hey, Kate-

Do you have any time this afternoon to chat? We are working on some election monitoring ideas with CISA and I would love your informal feedback before we go too far down this road.

Sorry for the last minute ask, but things that should have been assembled a year ago are coming together quickly this week.

Alex

The following day, on July 9, 2020, representatives from the SIO had a “[m]eeting with CISA to present [the] EIP concept.”⁸⁵ Among those in attendance were Brian Scully, the future head of CISA’s Mis-, Dis-, and Malinformation (MDM) team, Geoff Hale, the director of CISA’s Election Security Initiative, and Matt Masterson, then-Senior Cybersecurity Advisor at CISA.⁸⁶

Appointment

From: [REDACTED] [REDACTED]@cisa.dhs.gov

Sent: 7/8/2020 11:32:38 PM

To: [REDACTED]@cisa.dhs.gov; Snell, Allison [REDACTED]@cisa.dhs.gov; Scully, Brian [REDACTED]@cisa.dhs.gov; Masterson, Matthew [REDACTED]@cisa.dhs.gov; Hale, Geoffrey [REDACTED]@cisa.dhs.gov; Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]

Subject: CISA <> Stanford Internet Observatory, Election Misinformation Project Introduction

Location: Microsoft Teams Meeting

Start: 7/9/2020 4:00:00 PM

End: 7/9/2020 5:00:00 PM

Show Time As: Tentative

Recurrence: (none)

Good Afternoon All,

Thank you for taking the time to meet tomorrow for an introductory conversation on the Election Misinformation Project: a potential collaboration between ESI/CFI and the Stanford Internet Observatory. As we have discussed, this project aims to increase CFI’s real-time misinformation response capabilities by connecting SLTT and other CFI stakeholders to the third party misinformation research community.

The main topics we hope to cover this meeting are as follows:

- Overview of the Election Misinformation Project ([SLIDES](#))
- What are SIO’s core capabilities in this space?
- How would CISA and SIO’s misinformation response capabilities be augmented from such a partnership?
- Overview of open questions, concrete next steps.

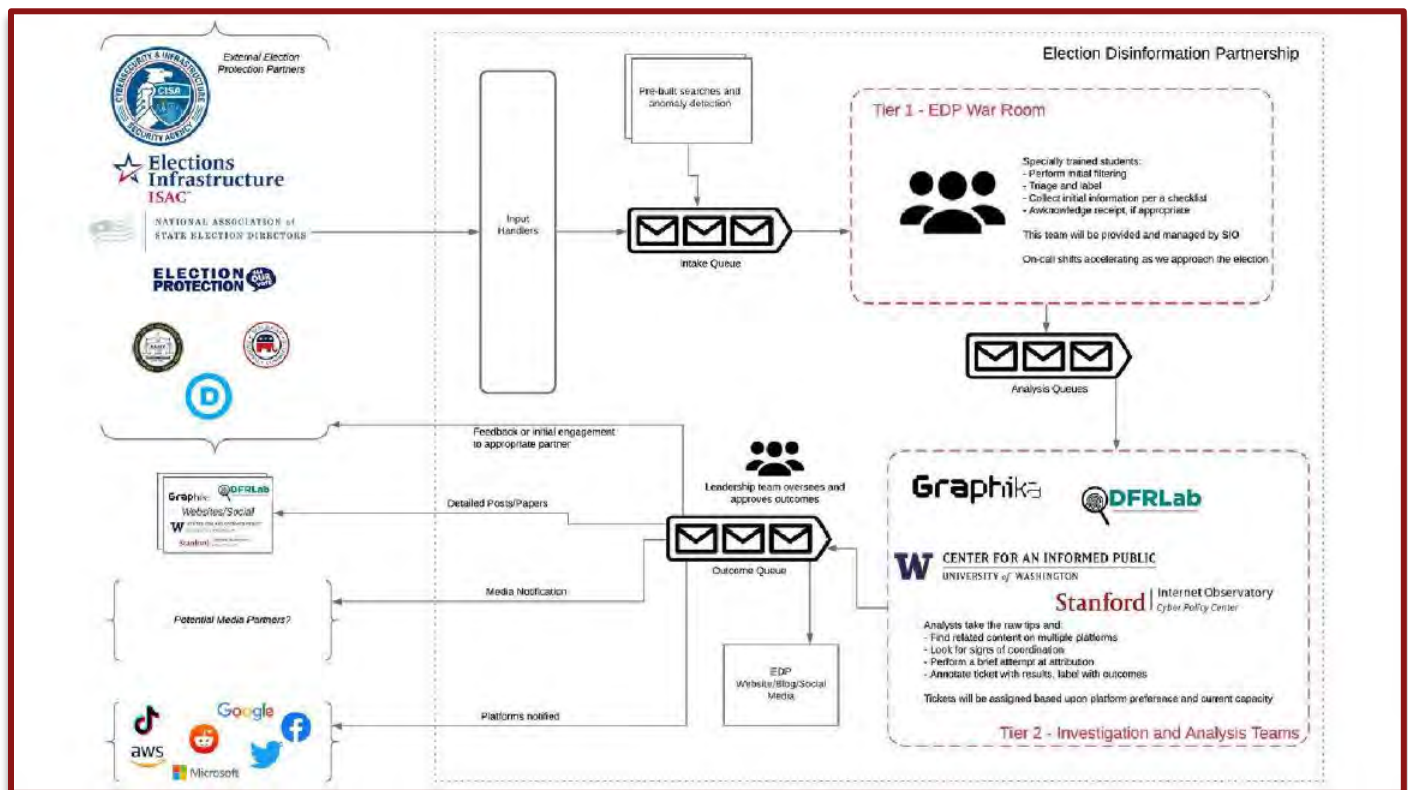
⁸⁴ Email from Alex Stamos to Kate Starbird (July 8, 2020, 9:41 AM) (on file with the Comm.).

⁸⁵ ELECTION INTEGRITY P’SHP, *supra* note at 16, at 3.

⁸⁶ Email from CISA official to CISA officials and SIO affiliates (July 8, 2020, 11:32 PM) (on file with the Comm.).

According to the email invitation for the meeting, the “Election Misinformation Project,” which would later be rebranded as the more euphemistic “Election Integrity Partnership,” “aim[ed] to increase . . . real-time misinformation response capabilities.” One of the agenda items was a discussion of how “CISA and SIO’s misinformation response capabilities [would] be augmented from such a partnership.”⁸⁷

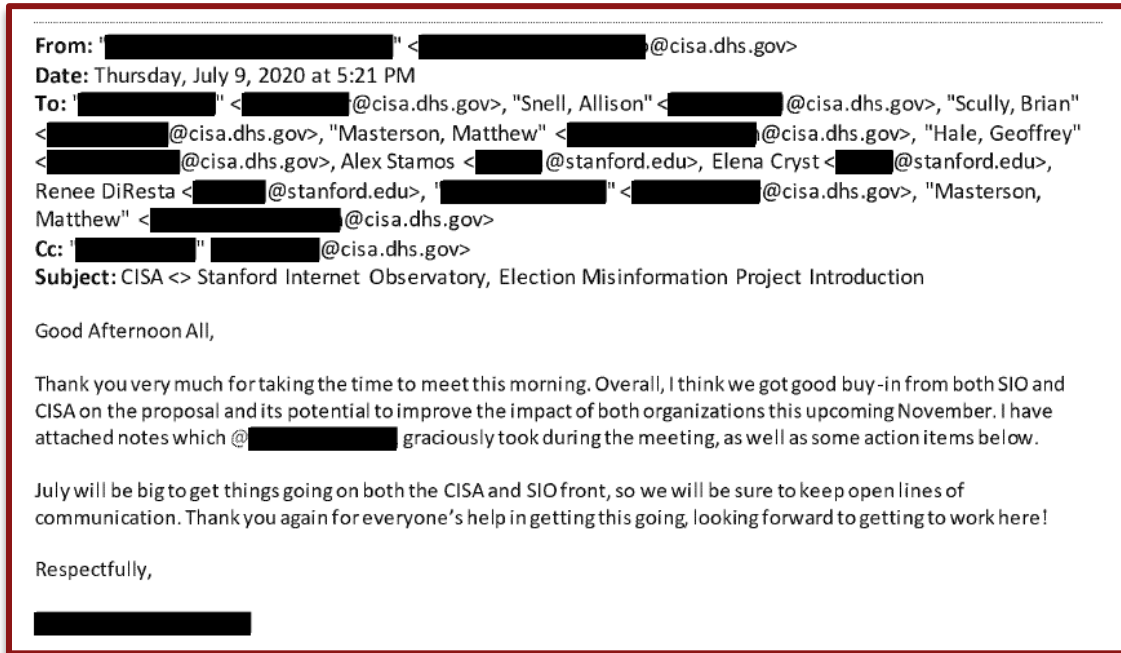
An early workflow diagram of the then-named “Election Disinformation Partnership” shows that from the beginning Stanford and CISA envisioned the partnership connecting federal agencies with social media platforms.⁸⁸



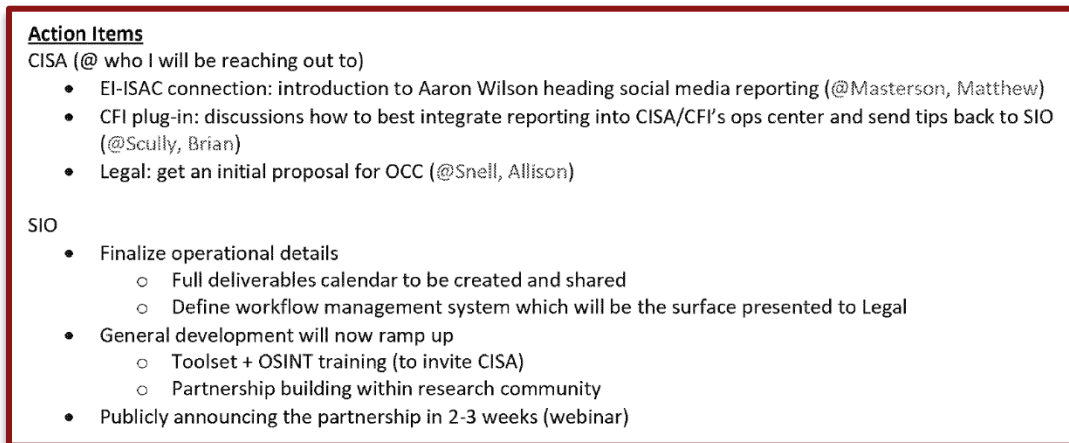
⁸⁷ *Id.*

⁸⁸ “CISA EIP Overview Deck.pptx” attach. to email from Emerson Brooking to Atlantic Council employees (Sept. 1, 2020, 11:12 AM) (on file with the Comm.). While the EIP invited both the DNC and RNC, the RNC declined to respond. House Judiciary Committee’s Transcribed Interview of Alex Stamos (June 23, 2023), at 8 (on file with the Comm.). The DNC not only accepted the invitation, but also submitted Jira tickets. ELECTION INTEGRITY P’SHIP, *supra* note 16, at 42.

A subsequent summary of the July 9 kick-off meeting from a CISA employee stated that “I think we got good buy-in from both SIO and CISA on the proposal and its potential to improve the impact of both organizations this upcoming November July will be big to get things going on both the CISA and SIO front, so we will be sure to keep open lines of communication.”⁸⁹



The summary also listed a number of action items for CISA and SIO, including “discussions [about] how to best integrate reporting into CISA/[Countering Foreign Influence]’s ops center and send tips back to SIO.”⁹⁰ Among the due-outs was a consultation with CISA’s Office of Chief Counsel (OCC), as seen in the action item “Legal: get an initial proposal for OCC.”⁹¹



⁸⁹ Email from CISA employee to CISA and SIO affiliates (July 9, 2020, 5:21 PM) (on file with the Comm.).

⁹⁰ *Id.*

⁹¹ *Id.*

Stamos also admitted during the interview that he had likely consulted with then-CISA Director Christopher Krebs during the summer of 2020 about the EIP. He testified:

Q. Did you consult with Chris Krebs in the summer of 2020?

A. I probably did, yes.⁹⁵

Documents produced to the Committee and Select Subcommittee likewise cast doubt on the notion that a handful of students were responsible for the EIP’s conception.⁹⁶ Regardless of what role, if any, students played in the “idea” of EIP, these documents show the direct role that high-ranking CISA, CIS, and SIO personnel played in forming an operation with nearly 100 people directly involved that worked with over a dozen partners to flag thousands of posts and narratives via hundreds of “misinformation” reports.⁹⁷

Finally, even the founding four partners of the EIP, such as the Atlantic Council’s DFRLab, understood in the summer of 2020 that the EIP was created at CISA’s request. As revealed in an internal Atlantic Council email obtained by the Committee pursuant to a subpoena, Graham Brookie, one of the central figures involved in the EIP, understood in July of 2020 that the EIP was “set up . . . at the request of DHS/CISA.”⁹⁸

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Friday, July 31, 2020 17:54
To: [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.ORG>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>
Cc: [REDACTED] <[REDACTED]@atlanticcouncil.org>; [REDACTED] <[REDACTED]@atlanticcouncil.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>
Subject: Re: Quick question -- Park Advisors

Thanks, [REDACTED]

And understood. Given the work DFRLab does on geopolitics, technology, and election interference with GEC, we were just caught off guard because they asked us about it.

I am not as concerned on the money or the project, but rather consolidating our approach to GEC as we go into the season for expanded renewals on two separate, multi-year agreements in the six figure range that cover a significant amount of our work on elections and all of our work in South Africa and Latin America.

On the DHS app, fake news, and any other US election-related work, it would be great to sync-up, as well. I know the Council has a number of efforts on broad policy issues around the elections, but we just set up an election integrity partnership at the request of DHS/CISA and are in weekly comms to debrief on disinfo, IO, etc..

Best,
 Graham

⁹⁵ *Id.* at 44. The Committee also interviewed former Director Krebs in October 2023, who claimed not to “recall any conversations with Alex [Stamos]” during the summer of 2020. House Judiciary Committee’s Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 164 (on file with the Comm.).

⁹⁶ *See, e.g.*, email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.).

⁹⁷ ELECTION INTEGRITY P’SHIP, *supra* note at 16, at xii, 12.

⁹⁸ Email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.) (emphasis added).

Internal Atlantic Council documents, obtained by the Committee and Select Subcommittee pursuant to a subpoena to the Atlantic Council, also reveal that while students were involved in the EIP, the critical work, including “attaching more contextual information,” preparing blog posts, and making recommendations to the social media platforms, was handled by the disinformation professionals.⁹⁹

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Wednesday, September 30, 2020 5:05 PM
To: Andy Carvin <[REDACTED]@ATLANTICCOUNCIL.org>; Emerson Brooking <[REDACTED]@ATLANTICCOUNCIL.org>
Subject: ANDY / EMERSON -- Coordination

COORDINATION ON US DOMESTIC PRIORITIES

Hi to both –

The struggle here is that Emerson is managing efforts and Andy is managing staff and outputs. The only way to be successful is to make sure that the three of us are explicitly on the same page about how we are allocating staff to efforts.

The below is intended to do that – and I will be adding Emerson to the DCHQ WhatsApp chain, where we will coordinate in general, as soon as we're on the same page as below. Our first obligation is always to our staff and not setting them up for failure. Our second obligation is to our core work, which every single one of us is managing key elements of. Thus the burden falls on the three of us to coordinate both.

Please reply in red or blue to the below. I also didn't have explicit names in the “staffing” section of each, so please fill out.

Thanks,
Graham

Election Integrity Partnership

Key questions: What is the schedule of shifts, noting that we just need to assign people to them? EIP, the voluntary shift system is a potential challenge because it requires a person to spend X amount of hours monitoring things, which either results in no outputs being produced, or a sudden need to complete an output that the person may or may not be suited to complete, especially if it's an international member of the team with limited knowledge of US politics, geography, culture, etc.

In scenarios where something potentially important surfaces within EIP, how do we go about prioritizing it? For example, when is it simply a matter of “this is a good story so please get me a draft in 72 hours” vs “all hands on deck, this is like a major takedown?” In either case, the three of us need to be locked up in order to not undermine our whole business operation through editorial capacity, who gets assigned, scheduling, etc.

One not ideal scenario is a situation where Jean or Ayush volunteer for a few hours, end up finding something important, and then having not having all three of our awareness and approval, which could lead to significant members of staff being taken away from their core responsibilities for extended periods of days/week. In other words, a shift is just the tip of the iceberg, commitment-wise.

Another question is what constitutes a contribution to EIP. While the focus has been on the partnership and the process (which makes sense) we're part of a team reviewing leads and deciding when to act on them. But we also continue to cover election-related stories that will originate from our original research, rather than the college students volunteering at EIP, especially now that Jared is coming on board and while looking into more conspiracy related content. Can we consider those contributions? I imagine for some researchers there's more incentive to contribute when they're able to generate research leads themselves rather than being responsive to tips, though I understand responding to tips is still core to the partnership.

Important to note: not college kids surfacing EIP leads. Krebs CISA is texting Stamos with some regularity. A few tickets have been flagged by the platforms. Starbird's UW team is surfacing a lot of stuff using advanced soc media listening methods. College kids (T-1) just doing the first round of analysis.

The job of DFRLab is to be T-2, doing a deep dive into tickets, attaching more contextual information, and writing up a twitter thread/blog post if that's the recommendation of the researcher (and the T-3 shift manager approves).

Analysts can step away and write a blog post on-shift. That's what Alyssa did [last week](#).

⁹⁹ Email exchange between Graham Brookie and Atlantic Council personnel (Sept. 30, 2020 5:05 PM) (on file with the Comm.).

C. The EIP’s Purpose: Using Proxies to Circumvent the First Amendment

By its own admission, the EIP was expressly created “in consultation with CISA”¹⁰⁰ to serve an unconstitutional purpose, as a mechanism for flaunting legal restrictions on illicit government activity. As stated in the EIP’s post-election report:

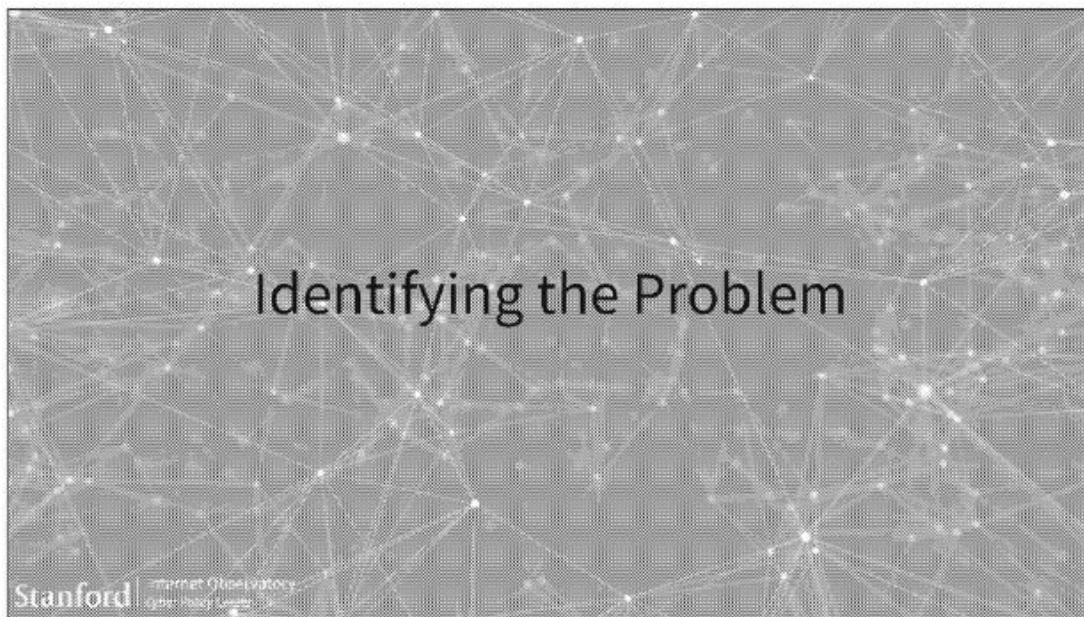
Yet, no government agency in the United States has the explicit mandate to monitor and correct election mis- and disinformation. This is especially true for election disinformation that originates from within the United States, which would likely be excluded from law enforcement action under the First Amendment and not appropriate for study by intelligence agencies restricted from operating inside the United States. As a result, during the 2020 election, local and state election officials, who had a strong partner on election-system and overall cybersecurity efforts in CISA, were without a clearinghouse for assessing mis- and disinformation targeting their voting operations . . . in consultation with CISA and other stakeholders, a coalition was assembled with like-minded partner institutions.¹⁰¹

In her notes for a fall 2021 presentation at the annual CISA Summit, Renée DiResta, the Research Manager at the SIO, wrote, as part of her presentation script, that the “gap” the EIP was intended to fill “had several components,” one of which was “[u]nclear legal authorities including *very real 1st amendment questions*.”¹⁰²

¹⁰⁰ ELECTION INTEGRITY P’SHIP, *supra* note at 16, at 2.

¹⁰¹ *Id.*

¹⁰² “CISA keynote.pptx” attach. to email from Renée DiResta to Kenneth Bradley and Amanda Glenn (Oct. 6, 2021, 3:58 PM) (on file with the Comm.); *see also* email from Renée DiResta to Kenneth Bradley and Amanda Glenn (Oct. 6, 2021, 3:58 PM) (on file with the Comm.) (DiResta writes, “I was just writing out the full script into the speaker notes in case the teleprompter was the best bet.”).



Our team and CISA's team have done some pioneering work in partnership thinking about how to respond to mis- and disinformation in areas in which it can have significant harm. One of those areas is elections, and I'm going to talk about some learnings from that work today.

In August 2020, students from the Stanford Internet Observatory (SIO) who were doing an internship with CISA identified a massive gap in the capability of federal, state and local governments to become aware of, analyze and rapidly respond to mis- and disinformation — both foreign and domestic — targeting the 2020 election.

That gap had several components:

- Federal gov't not prepared to identify and analyze election mis/disinfo:
 - There was no clear federal lead to coordinate this work. The IC, of course, is rightly limited to a foreign-focus. The FBI also has very specific designations and limitations, and CISA had created support but had no real capability.
 - Unclear legal authorities including very real 1st amendment questions
 - No expertise resident within federal gov't to analyze public content across platforms to identify trends & risks
- Lack of reporting mechanisms for state and local partners to surface activity that they saw building in their communities, to help them understand it.

The federal government was building relationships with platforms but there is a healthy distrust both ways for good reason

A trusted, nonpartisan partner(s) with expertise in the way that misinformation moved on public platforms, with analysts capable of understanding public conversations, and broad ability to explore publicly available data, was needed.

In order to circumvent these “very real 1st amendment questions,” organizations devoted to peddling the pseudoscience of “disinformation,” like the SIO and the University of Washington’s CIP, were selected to serve as part of a “central organization to support elections officials or CISA in identifying and responding to misinformation.”¹⁰³ According to an early EIP

¹⁰³ Election Disinformation Partnership: Overview for Partners (unpublished presentation notes) (on file with the Comm.).

presentation, “Academic/Research Institutions” were chosen to spearhead this effort specifically because they were considered to be the “‘easiest’ politically.”¹⁰⁴

Current Landscape

Who could potentially solve this problem? Why aren't they?

	CISA	Platforms	Academic/Research Institutions
Currently Offers	EHSAC collaboration to provide real-time monitoring tools such as the SOC as well as the classified and unclassified Situation Rooms	Direct contact with secretaries of state as well as some cross-platform communication on this front	Institutions have created their own independent groups, little coordination
Strengths	Direct communication with every election official, central node in the election infra ecosystem	Highest monitoring capacity into what is happening in the social landscape, lots of \$\$\$ and resources	'Easiest' politically, transparent, existing institutions (SIO). Agile, lightweight teams.
Weaknesses	All efforts focused on hardware, no misinformation workstream, govt entity, can't be seen as 'monitoring' the electorate, highly political.	Political, easily seen as partisan, don't have the direct communication/report with all election officials.	Don't have the direct communication or rapport with all election officials, need to raise \$\$\$

It is “axiomatic,” the Supreme Court has explained, that the government “may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish.”¹⁰⁵ CISA’s involvement in the creation of and collaboration with the EIP is the type of unconstitutional outsourcing against which the Supreme Court has long ruled.¹⁰⁶ Censorship-by-proxy is an especially nefarious form of state action, given that it is designed to evade detection, oversight efforts, and public records requests.¹⁰⁷

¹⁰⁴ *Id.*

¹⁰⁵ *Norwood v. Harrison*, 413 U.S. 455, 465 (1973).

¹⁰⁶ *See also Missouri v. Biden*, No. 23-30445, slip op. (5th Cir. Oct. 3, 2023), ECF No. 271. As the Committee’s investigation has revealed, CISA’s practice of exploiting third-party non-profits to sidestep legal prohibitions against censorship and surveillance also extended beyond the EIP. For example, on November 4, 2020, Robert Schaul, CISA’s Analysis and Resilience Policy Lead, sent an email to an individual affiliated with Alliance for Securing Democracy, a project of the German Marshall Fund and subject of several Twitter Files installments. In the email, Schaul writes that he is “checking in to see if you’re seeing anything of particular concern that might be worth elevating to Director Krebs. Are you still seeing #stopthesteal popping up? We’re still all hands on deck here.” Email from Robert Schaul to Alliance for Securing Democracy Employee (Nov. 4, 2020 12:02 PM) (on file with the Comm.). Notably, Schaul did not distinguish between organic, domestic discussion of #stopthesteal and foreign amplification of the hashtag.

¹⁰⁷ *See, e.g., Lee Fang, Biden Justice Dept. Intervened to Block Release of Social Media Censorship Docs*, SUBSTACK (June 6, 2023), <https://www.leefang.com/p/biden-justice-dept-intervened-to>; *see also* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS, at 34–35 (Comm. Print June 26, 2023).

II. CISA'S COMPLETE INTERTWINEMENT WITH THE EIP

“CISA and the EIP were completely intertwined.”

-Missouri v. Biden, Case No. 3:22-cv-1213,
ECF No. 293 (Injunction & Opinion) at 113 (July 4, 2023).

A. CISA's Collusion with the EIP

After CISA helped to create the EIP, the federal agency remained thoroughly intertwined with the EIP's operations in the months preceding the 2020 election. Throughout the fall of 2020, CISA officials coordinated extensively with the EIP and CIS.¹⁰⁸ Emails obtained by the Committee and Select Subcommittee pursuant to a subpoena show clearly that the EIP system was designed to operate as a unit, not as a separate entity from DHS. Moreover, while there were many students involved in the EIP (which had nearly 100 people working for it, not including external stakeholders such as the GEC and CISA), the EIP was led by well-known figures in the censorship-industrial complex, such as Stanford Internet Observatory (SIO) Director (and former Chief Security Officer at Facebook) Alex Stamos, SIO Research Manager Renee DiResta, and Vice President and Senior Director of the Atlantic Council's Digital Forensic Research Lab (DFRLab) Graham Brookie. The EIP also collaborated closely with senior CISA officials, including Brian Scully, the head of CISA's Countering Foreign Influence Task Force (CFITF).

Not only were there a number of university students involved with the EIP, at least four of the students were employed by CISA during the operation of EIP, using their government email accounts to communicate with CISA officials and other “external stakeholders” involved with the EIP. For example, by September 3, 2020, CISA had designated one of these DHS-SIO interns as the point of contact to be responsible for “taking point on a lot of the EIP <> CISA interface.”¹⁰⁹

¹⁰⁸ See, e.g., email from CISA staff to CISA officials, CIS employees, and SIO affiliates (Oct. 5, 2020, 12:52 PM) (on file with the Comm.).

¹⁰⁹ Email from CISA staff to Aaron Wilson, Ben Spear, and Mike Garcia (Sept. 3, 2020, 1:51 PM) (on file with the Comm.).

From: [REDACTED] [REDACTED]@cisa.dhs.gov
Sent: 9/3/2020 1:51:40 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlT)/cn=recipients/cn=[REDACTED]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED] [REDACTED]@cisa.dhs.gov
CC: Masterson, Matthew [REDACTED]@cisa.dhs.gov; Snell, Allison [REDACTED]@cisa.dhs.gov; Scully, Brian [REDACTED]@cisa.dhs.gov; Hale, Geoffrey [REDACTED]@cisa.dhs.gov
Subject: RE: CISA <> CSI Disinfo Reporting follow up

Hello Aaron:

Sorry for the delay here – for some reason, the @cisecurity alias keeps getting routed to my 'Other' folder, so I was about to follow up on this myself. I'll try and chat with our techdesk today about this.

On the EIP side, if you could please add tips@eipartnership.net, this alias will auto create Jira tickets for any incoming reports for visibility to the whole EIP team. I've also added [REDACTED] to this thread, [REDACTED]@cisa.dhs.gov, who will be taking point on a lot of the EIP <> CISA interface here, so he should also be added. I will let Brian and Matt note whether they also would like to be on the backend of this alias.

One note on the EIP side: we just finished getting our Jira system online to be ready for intake. For security purposes, the tips@eipartnership.net alias has a strict whitelist of emails which will be allowed through: any email not specifically designated into an organization will be silently dropped. I've created a new CIS organization on our system and added misinformation@cisecurity.org to it, as well as [REDACTED]'s CISA email. Any reports forwarded from these email addresses will make it into our system. However, if misinformation@cisecurity.org auto forwards anything in such a way that it is sent from a different alias (ex: bob@washington.gov), this will be dropped in our system.

There are ways around this, but I just wanted to flag this upfront and get a sense from you how this might be working on your end? I have a free calendar all day tomorrow basically, and could hop on a call with our tech lead to figure out the best way of doing this.

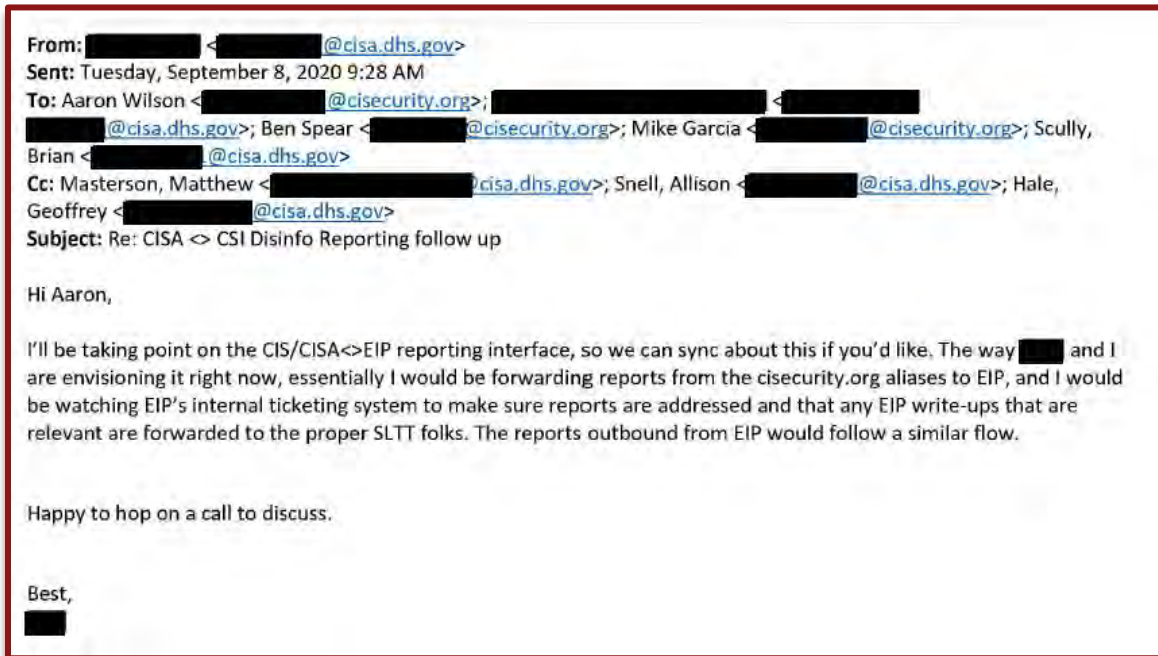
Best,

[REDACTED]

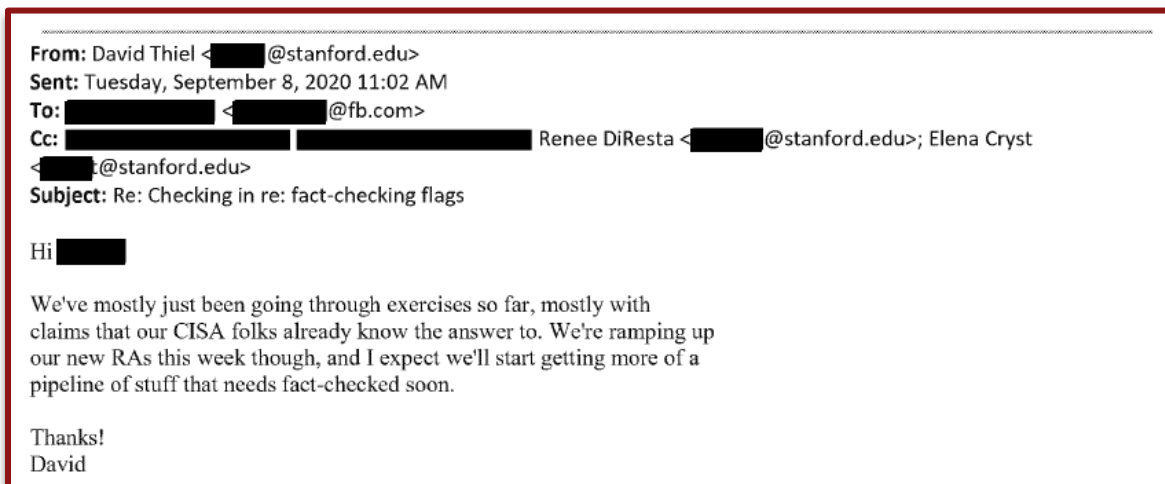
This Stanford student, working as a DHS intern, would be “inside the EIP network,” with the responsibility of “forwarding reports from the cisecurity.org aliases to EIP,” and “watching EIP’s internal ticketing system to make sure reports are addressed and that any EIP write-ups that are relevant are forwarded to the proper SLTT [state, local, tribal, and territorial] folks.”¹¹⁰

¹¹⁰ Email from CISA official to Aaron Wilson, Ben Spear, Mike Garcia, and Brian Scully (Sept. 8, 2020, 9:28 AM) (on file with the Comm.).

In other words, DHS had a point of contact with direct access to the EIP’s internal ticketing system who could (and did) share this information with the agency.¹¹¹



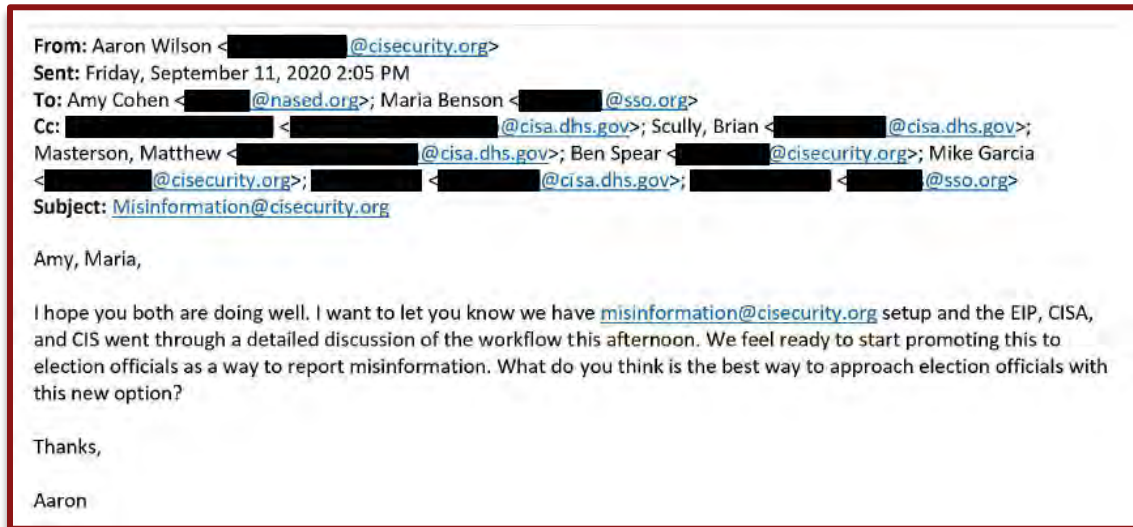
As the EIP geared up for the 2020 election, it appears that the EIP coordinated with CISA to conduct censorship “exercises.” A September 8, 2020, email to a Facebook employee from David Thiel, the SIO’s Chief Technologist, reads: “We’ve mostly just been going through exercises so far, mostly with claims that our CISA folks already know the answer to.”¹¹²



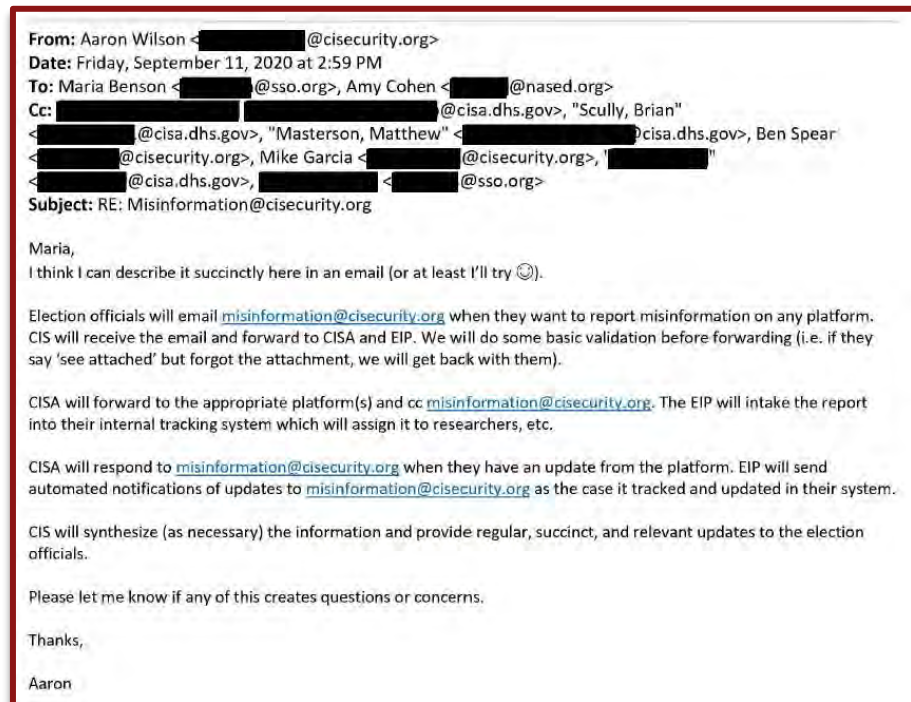
¹¹¹ Moreover, witnesses before the Committee have testified that they did not recall knowing that the individual using the “@cisa.dhs.gov” email domain was an intern. *See, e.g.*, House Judiciary Committee’s Transcribed Interview of Aaron Wilson (November 2, 2023), at 46 (on file with the Comm.).

¹¹² Email from David Thiel to Facebook employee (Sept. 8, 2020, 11:02 AM) (on file with the Comm.).

On September 11, Aaron Wilson, emailed that “the EIP, CISA, and CIS went through a detailed discussion of the workflow this afternoon. We feel ready to start promoting this to election officials as a way to report misinformation.”¹¹³

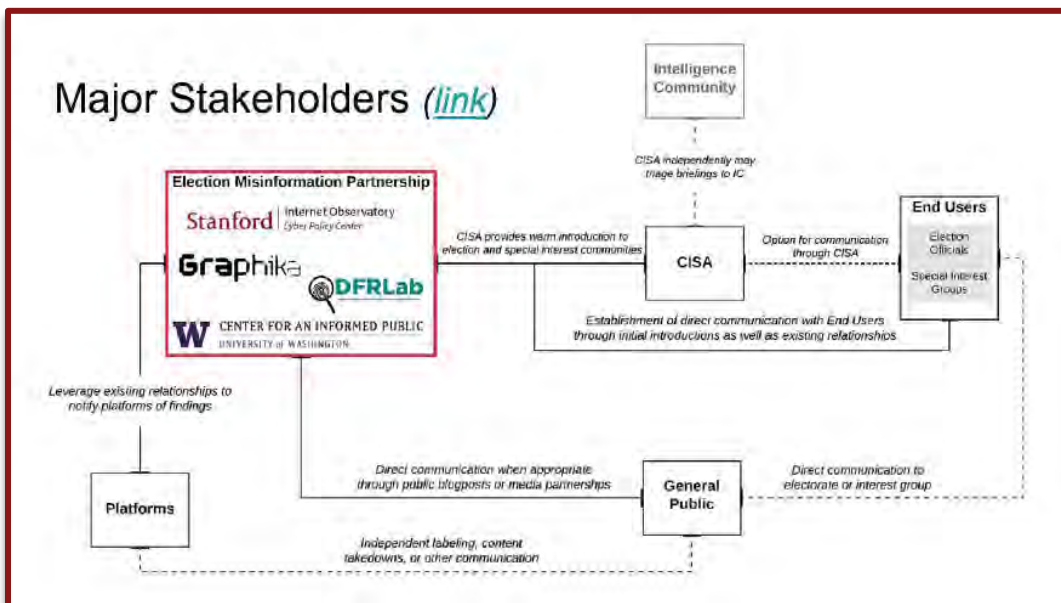
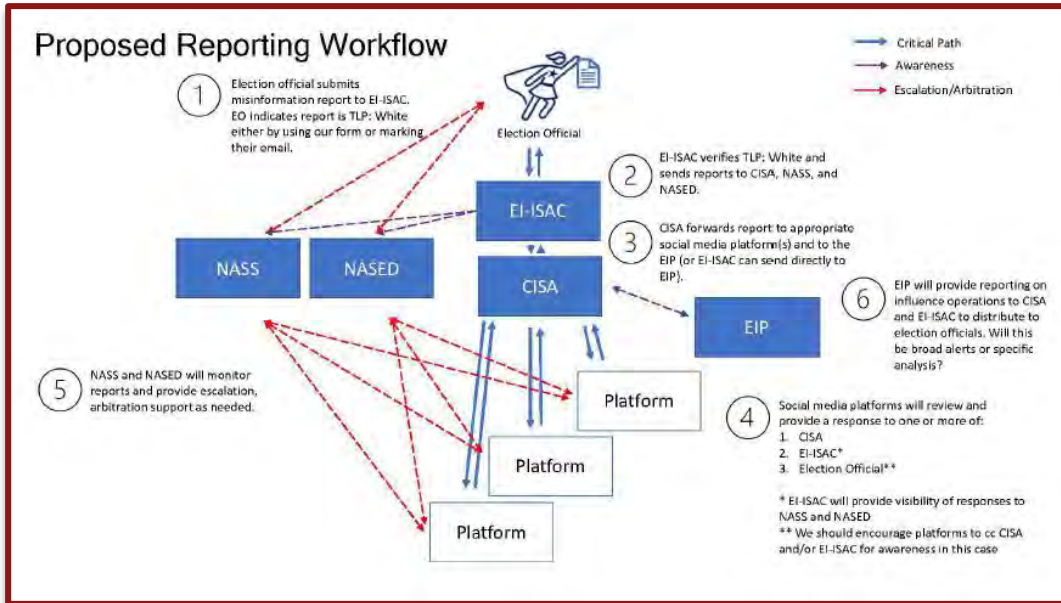


The proposed workflow makes clear that neither the EIP nor CIS were acting completely independently of CISA, but instead operated cooperatively and systematically within the same censorship organ CISA helped to create. As described in the same mid-September 2020 email thread below, election officials would submit misinformation reports to CIS; CIS would then (1) forward the email to CISA, with the agency then forwarding the report to the social media platforms (i.e., the CISA track); and (2) forward the email to EIP, who would search for other similar content to be flagged before sending reports to the social media platforms (i.e., the EIP track). As a consequence, CISA had visibility on what was being submitted to the EIP. And critically, social media platforms knew that CISA had knowledge of the EIP’s intake.



¹¹³ Email from Aaron Wilson to Amy Cohen and Maria Benson (Sept. 11, 2020, 2:05 PM) (on file with the Comm.).

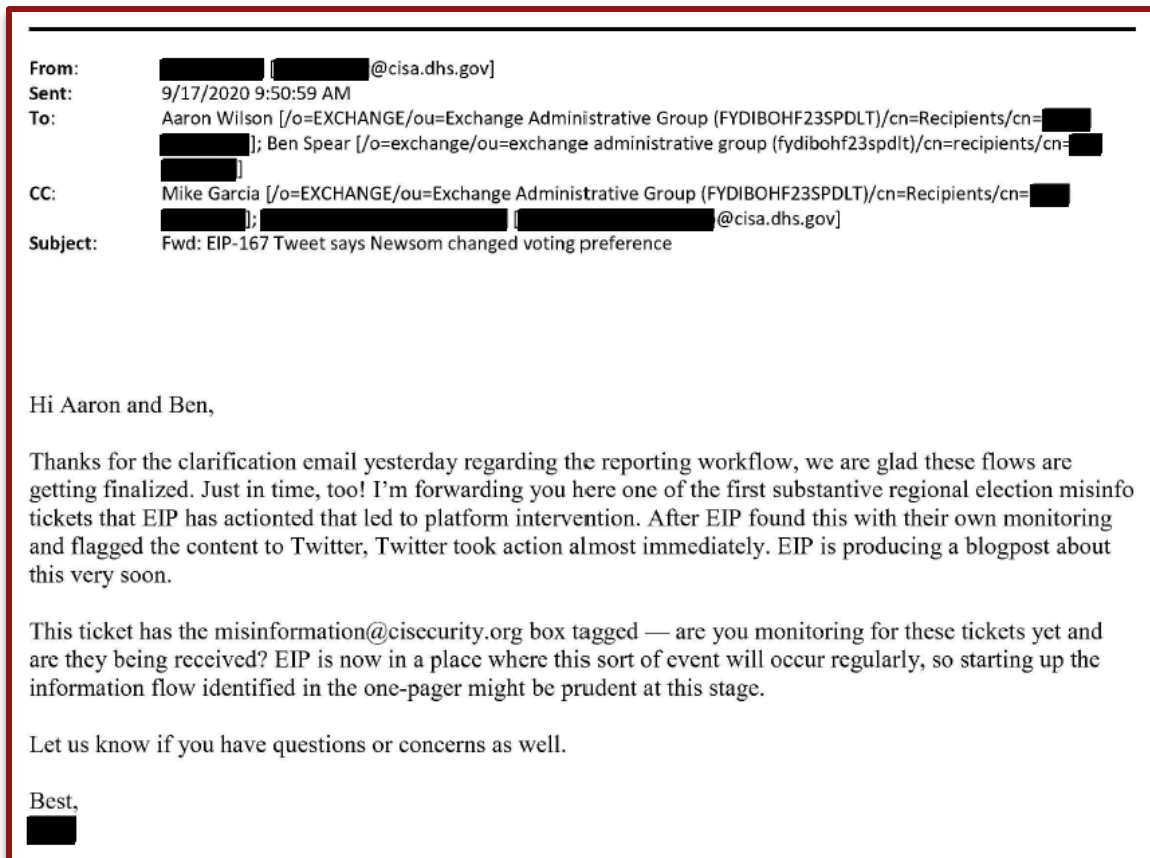
The close, direct coordination between CISA and the EIP was contemplated from the beginning, as seen in the below diagrams contained in what appear to be early EIP briefing materials. Multiple steps in the “Proposed Reporting Workflow,” explicitly link CISA and the EIP. For example, one step read: “CISA forwards report to appropriate social media platform(s) and to the EIP (or EI-ISAC can send directly to EIP).”¹¹⁴ Another diagram, titled “Major Stakeholders” drew a link between the EIP, CISA, and the Intelligence Community.¹¹⁵



¹¹⁴ Proposed Reporting Workflow (unpublished diagram) (on file with the Comm.).

¹¹⁵ Election Disinformation Partnership: Overview for Partners (unpublished presentation notes) (on file with the Comm.).

This arrangement quickly bore fruit for the federal government’s censorship-launders operation. On September 17, a CISA official emailed CIS’s Aaron Wilson and Ben Spear, writing: “I’m forwarding you here one of the first substantive regional election misinfo tickets that EIP has actioned that led to platform intervention. After EIP found this with their own monitoring and flagged the content to Twitter, Twitter took action almost immediately.”¹¹⁶ Put plainly, the EIP reported back to the federal government that it had successfully induced Big Tech to censor Americans’ political speech on behalf of CISA.



CISA knew that flagging individual posts for removal would not be sufficient to achieve its goal of categorically censoring disfavored viewpoints, primarily conservative political speech. Instead, entire “narratives” needed to be targeted for censorship. Pursuant to multiple subpoenas, the Committee and Select Subcommittee obtained communications between CISA, the EIP, and CIS demonstrating that the true objective in flagging content to social media platforms was to censor entire narratives not just specific, flagged posts. However, this did not stop the EIP from identifying massive amounts of social media posts allegedly spreading “misinformation,” with some misinformation reports containing over 500 individual links.¹¹⁷

¹¹⁶ Email from CISA official to Aaron Wilson and Ben Spear (Sept. 17, 2020, 9:50 AM) (on file with the Comm.).

¹¹⁷ EIP-915, submitted by [REDACTED], ticket created (Nov. 5, 2020, 9:07 PM) (archived Jira ticket data produced to the Comm.); see also James O’Keefe, TWITTER (Nov. 6, 2020, 5:44 PM), <https://twitter.com/JamesOKeefeIII/status/1324845160358940673>.

On September 24, one of the CISA-SIO interns wrote: “there is no way we found every piece of misinfo related to this incident, so we don’t give a ton of weight to how many of the links that we sent over got actioned (though we hope all would) Because of this, we see the narrative itself as the most important thing to communicate.”¹¹⁸

From: [REDACTED] [REDACTED]@cisa.dhs.gov]
Sent: 9/24/2020 5:21:14 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]; [REDACTED]; [REDACTED]@cisa.dhs.gov]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]
CC: Scully, Brian [REDACTED]@cisa.dhs.gov]; Snell, Allison [REDACTED]@cisa.dhs.gov]; Tipton, James [REDACTED]@cisa.dhs.gov]; Dragseth, John [REDACTED]@cisa.dhs.gov]; Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]
Subject: RE: EIP-167 Tweet says Newsom changed voting preference

Hello Aaron:

Jumping in to answer a couple of the technical questions! We just had an issue with Facebook’s reporting box which was configured oddly as a ‘bulk’ email inbox. Is your mail receiver for misinfo@cisecurity.org automatically dropping emails tagged as ‘bulk’? Because if so, the Jira alias where these tips are coming from (which I think is a bulk inbox) won’t work with it. I am relaying this from our technical team so can ask for more information as helpful.

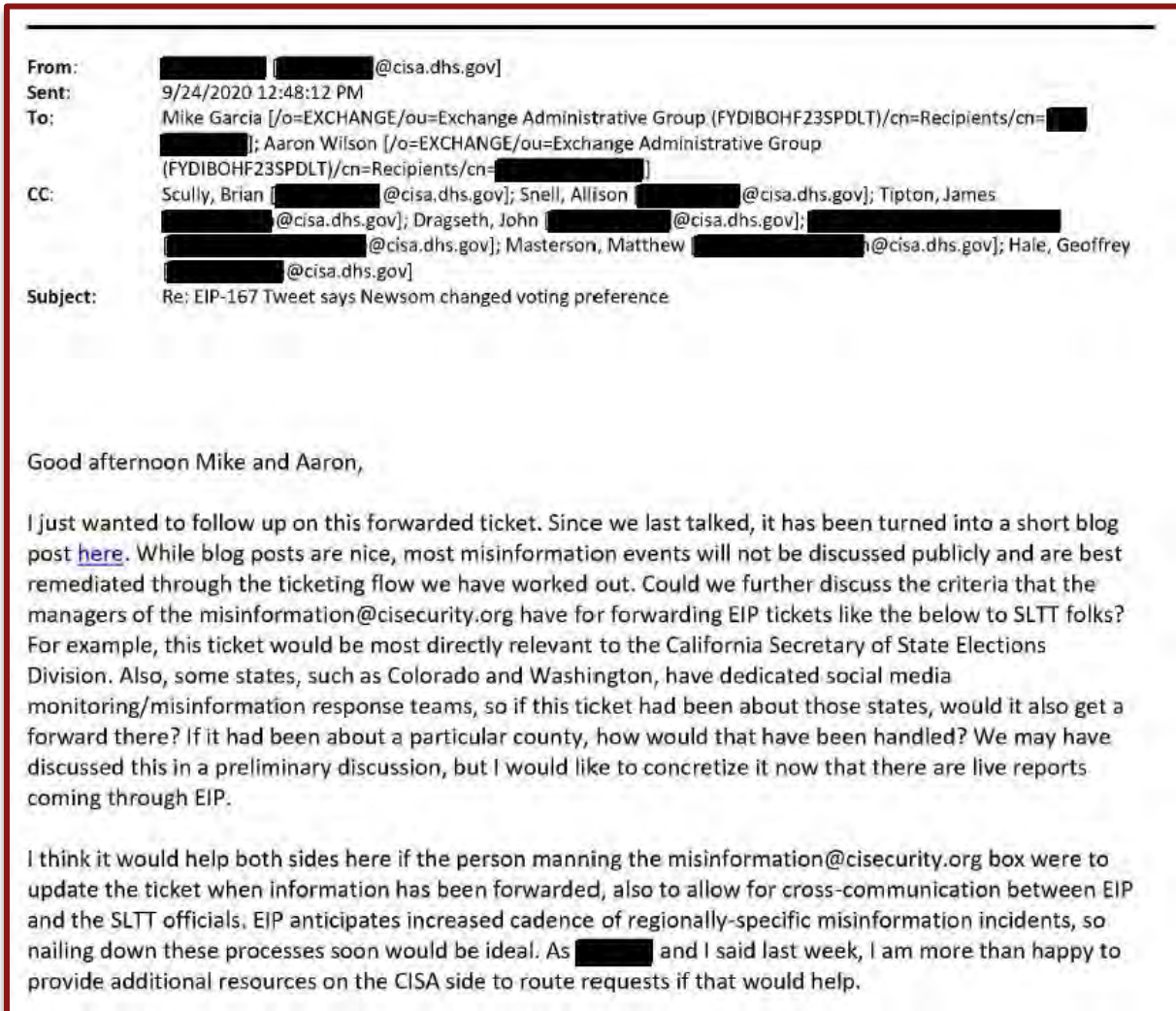
Regarding your second question on whether the ticket is closed: we closed the ticket as we had given the organizations tagged a reasonable amount of time to respond (~1 week in this case) and received no further commentary. We also wrote up our findings publicly. I don’t think the status of the ticket as Open or Closed means much for the election officials – we are sending this to you early in hopes of having it go straight to the impacted stakeholders as close to instantly as possible, so that if its of interest, they can ask further questions and we can be responsive to find more information. We just don’t know what is helpful to them yet.

As to the action on certain links: there is no way we found every piece of misinfo related to this incident, so we don’t give a ton of weight to how many of the links that we sent over got actioned (though we hope all would) because we know we didn’t find all the links anyways, and that the platforms are not going to communicate to us how many further leads they found and actioned as well (it could be none, it could be a network of 1000 users. Though they’d likely tell us about the latter). Because of this, we see the narrative itself as the most important thing to communicate, and the links as supplementary examples. We are always available to re-open a case to give further information on a narrative as helpful.

In another email sent on September 24, one of the CISA-SIO interns who was later hired to the full-time staff at CISA offered support for the joint censorship enterprise, writing, “EIP anticipates increased cadence of regionally-specific misinformation incidents, so nailing down

¹¹⁸ Email from CISA official to Aaron Wilson and Mike Garcia (Sept. 24, 2020, 5:21 PM) (on file with the Comm.).

these processes soon would be ideal I am more than happy to provide additional resources on the CISA side to route requests if that would help.”¹¹⁹



Furthermore, while the SIO has claimed that the “EIP’s goal was and continues to be to research and analyze attempts to prevent or deter people from voting,” the SIO-affiliated individual wrote in the same email that “[w]hile blog posts are nice, most misinformation events will not be discussed publicly and are best remediated through the ticketing flow we have worked out.”¹²⁰

Evidence obtained by the Committee and Select Subcommittee also makes clear that the highest levels of CISA leadership, including then-Director Krebs, had awareness of the CISA-

¹¹⁹ Email from CISA official to Mike Garcia and Aaron Wilson (Sept. 24, 2020, 12:48 PM) (on file with the Comm.).

¹²⁰ Cf. *id.*; *Background on the SIO’s Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), <https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media>.

EIP-CIS censorship campaign.¹²¹ On September 25, 2020, an email from CISA to CIS reveals that Twitter took “action on one of the tweets in [an EIP] ticket. Evidently Director Krebs personally reached out to [SIO head] Stamos asking what had happened around this event around the time the content was taken down.”¹²² In internal Atlantic Council email exchanges around this time, EIP members stated that “Krebs CISA is texting Stamos with some regularity.”¹²³

From: [REDACTED] [REDACTED]@cisa.dhs.gov
Sent: 9/25/2020 7:45:38 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Misinformation Reports [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=093d02c79b0f4dba805c5322cd750647-misinformation]
CC: Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=[REDACTED]]; [REDACTED] [REDACTED]@cisa.dhs.gov
Subject: Re: EIP-243 Claim the thousands of ballots found in dumpster in Sonoma

Hi all,

Just bumping this. Twitter has now taken action on one of the tweets in this ticket. Evidently Director Krebs personally reached out to Stamos asking what had happened around this event around the time the content was taken down, which was only an hour after this ticket was created. If this system is to work, we will need the turnaround time to be much faster for sending these tickets out to states.

Can anyone advise on next steps for actioning this event?

Thank you,
 [REDACTED]

Overt coordination between CISA, the EIP, and CIS continued well into the 2020 election cycle. On October 5, 2020, Masterson, Scully, Stamos, and Garcia, among others, were invited to a meeting titled “EIP-CIS Sync.”¹²⁴ According to the email invitation: “The misinformation@cisecurity.org reporting system is now up and running, as is EIP’s inbound and

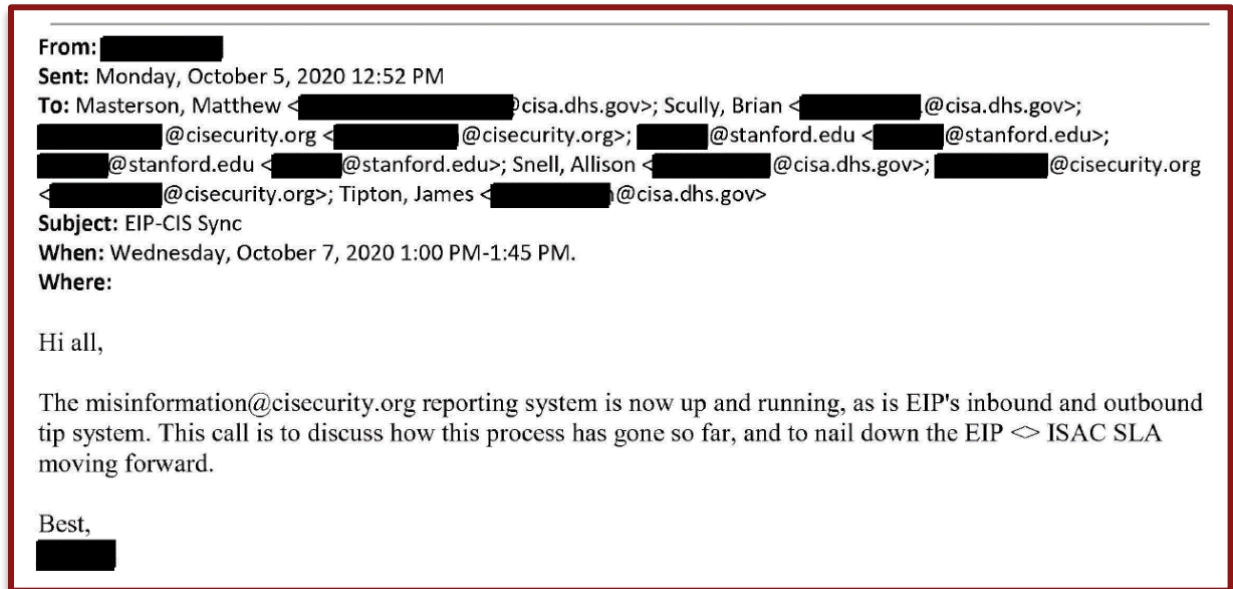
¹²¹ See e.g., email from CISA official to Aaron Wilson and Mike Garcia (Sept. 25, 2020, 7:45 PM) (on file with the Comm.).

¹²² *Id.*

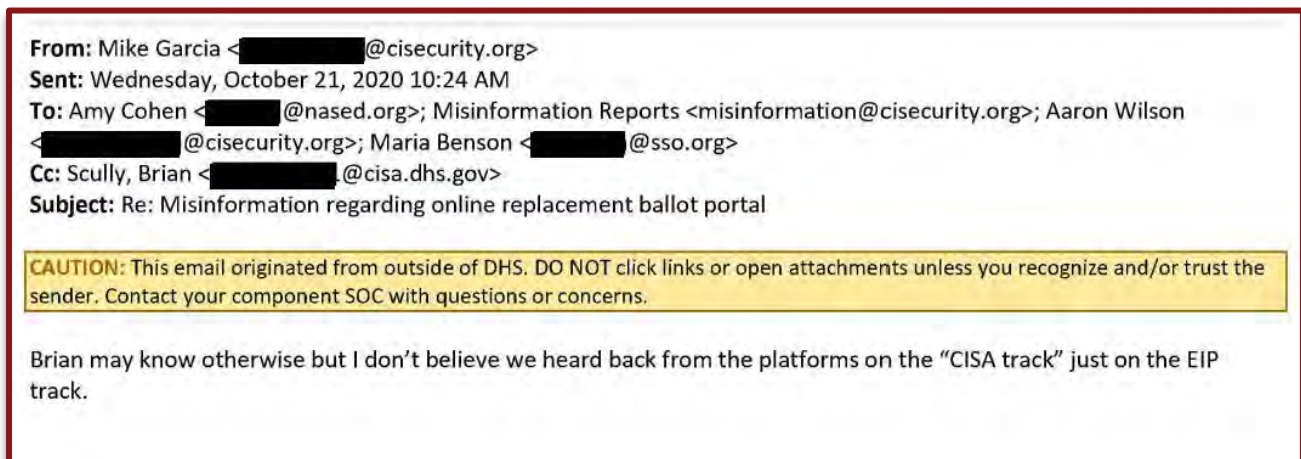
¹²³ Email exchange between Graham Brookie, Andy Carvin and Emerson Brooking (Sept. 30, 2020 5:05 PM) (on file with the Comm.).

¹²⁴ Email from CISA official to CISA officials, CIS employees, and SIO affiliates (Oct. 5, 2020, 12:52 PM) (on file with the Comm.).

outbound tip system. This call is to discuss how this process has gone so far, and to nail down the EIP \diamond ISAC SLA moving forward.”¹²⁵



An email from CIS, sent on October 21, 2020, demonstrates that CIS was keeping track of both the “CISA track” and the “EIP track” for flagging posts on social media platforms.¹²⁶

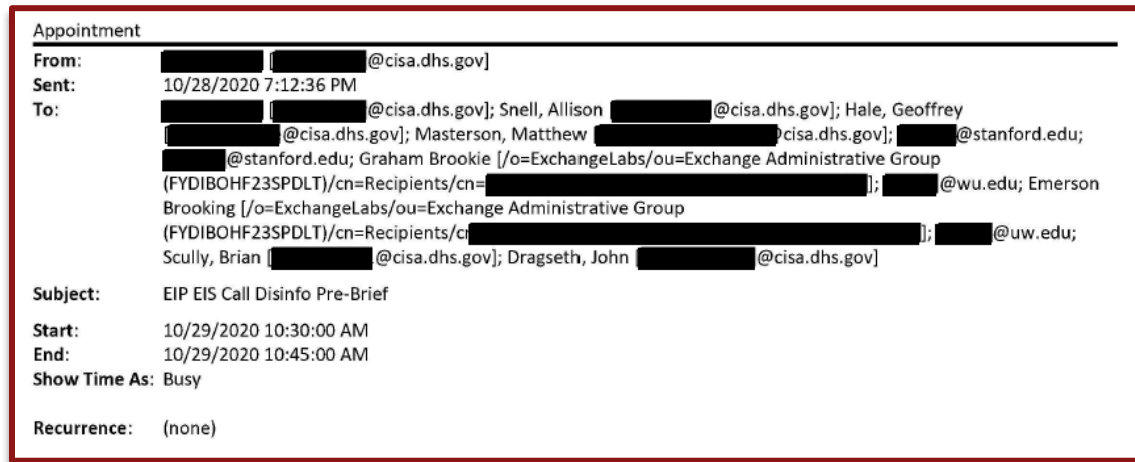


The EIP and CISA had another meeting to coordinate their censorship operation on October 29, 2020, as evidenced by a meeting invitation with the subject “EIP EIS [Election

¹²⁵ *Id.*

¹²⁶ Email from Mike Garcia to Amy Cohen, misinformation@cisecurity.org, Aaron Wilson, and Maria Benson (Oct. 21, 2020, 10:24 AM) (on file with the Comm.).

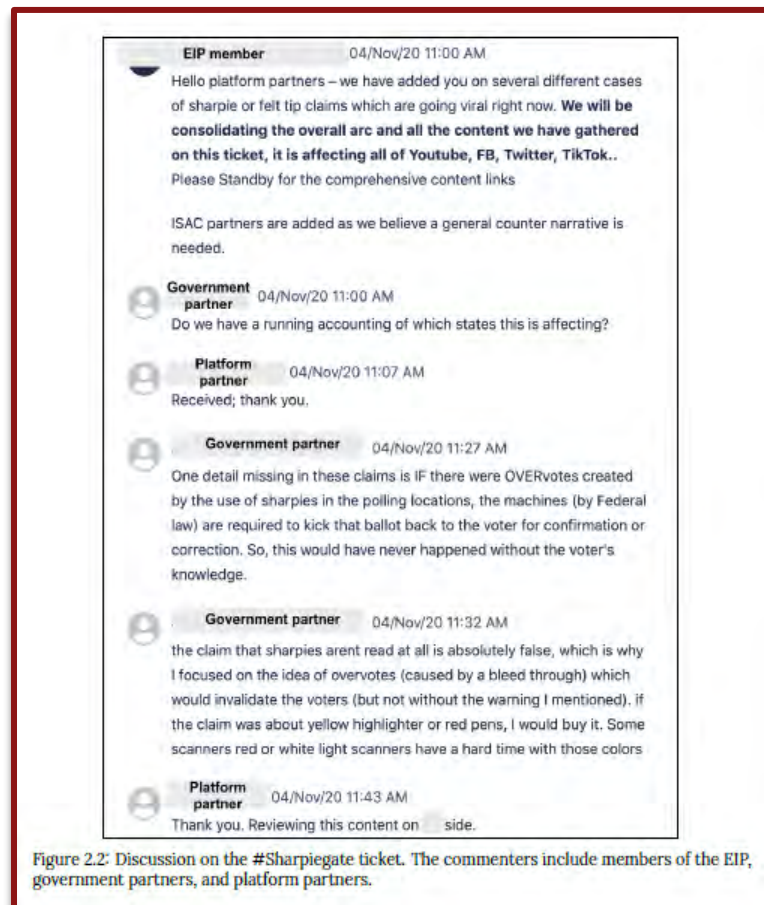
Security Initiative] Call Disinfo Pre-Brief.”¹²⁷ EIS appears to be in reference to CISA’s Election Security Initiative, which included Geoff Hale and Matt Masterson at the time.



B. Jira Tickets: The Main Weapon in the EIP’s Censorship Arsenal

Once the EIP had been formally organized on July 26, 2020, it quickly set about devising a method to mass-report content that it deemed undesirable to the relevant social media platforms. The EIP’s tipline of choice was Jira, an issue-tracking software developed by Atlassian, an Australian software company.¹²⁸ According to the EIP’s post-election report, the EIP “chose Jira because it supported a large team and allowed the addition of workflows that require both robust customer management capabilities and organizational features to reflect the numerous roles needed to respond to any inbound request.”¹²⁹

The EIP’s report including an example image of what a Jira



¹²⁷ Email from CISA official to CISA officials and EIP personnel (Oct. 28, 2020, 7:12 PM) (on file with the Comm.).

¹²⁸ See *Jira Software*, ATlassian, <https://www.atlassian.com/software/jira> (last visited Nov. 3, 2023).

¹²⁹ ELECTION INTEGRITY P’SHPHIP, *supra* note at 16, at 24.

ticket looked like, demonstrating how the Jira system allowed for real-time collaboration by “members of the EIP, government partners, and platform partners.”¹³⁰

C. The Collusion in Practice: The Coordinated Flagging of Posts

Pursuant to a subpoena, CISA has produced to the Committee and Select Subcommittee dozens of emails in which CIS sent reports of misinformation from state and local election officials to both the EIP and CISA. CISA then switchboarded the reports to the relevant social media platforms. CIS frequently included both CISA and the EIP on the same email chains, including CISA’s Brian Scully, CISA’s CFITF, and the EIP (as indicated by the EIP email domain “@2020partnership.atlassian.net”).¹³¹

Plainly put, the federal government, CIS, and the EIP were all on the same email chains discussing the censorship of Americans’ political speech. One of just many examples is shown below.¹³² While Stanford and SIO Director (and effectively the head of the EIP) Alex Stamos have given carefully crafted statements and testimony to the Committee and Select Subcommittee that CISA could not *directly* report misinformation content to the EIP, this email chain and others show that CISA routinely was copied on emails from CIS to the EIP reporting misinformation.¹³³ In other words, while CISA did not directly report content *to the EIP*, CISA had complete visibility on what was being reported to the EIP and at the same time was reporting the same content directly to the social media platforms. While CISA had “no official role,” CISA knew what reports were being submitted to the EIP, received Jira ticket reports and notifications via email, had personnel with direct access to the EIP ticketing system, and was in direct contact with the social media platforms.



In another characteristic example below, CIS’s “Misinformation Reports” email account sent an email to Brian Scully, CISA Central, CISA’s CFITF, and EIP, which read:

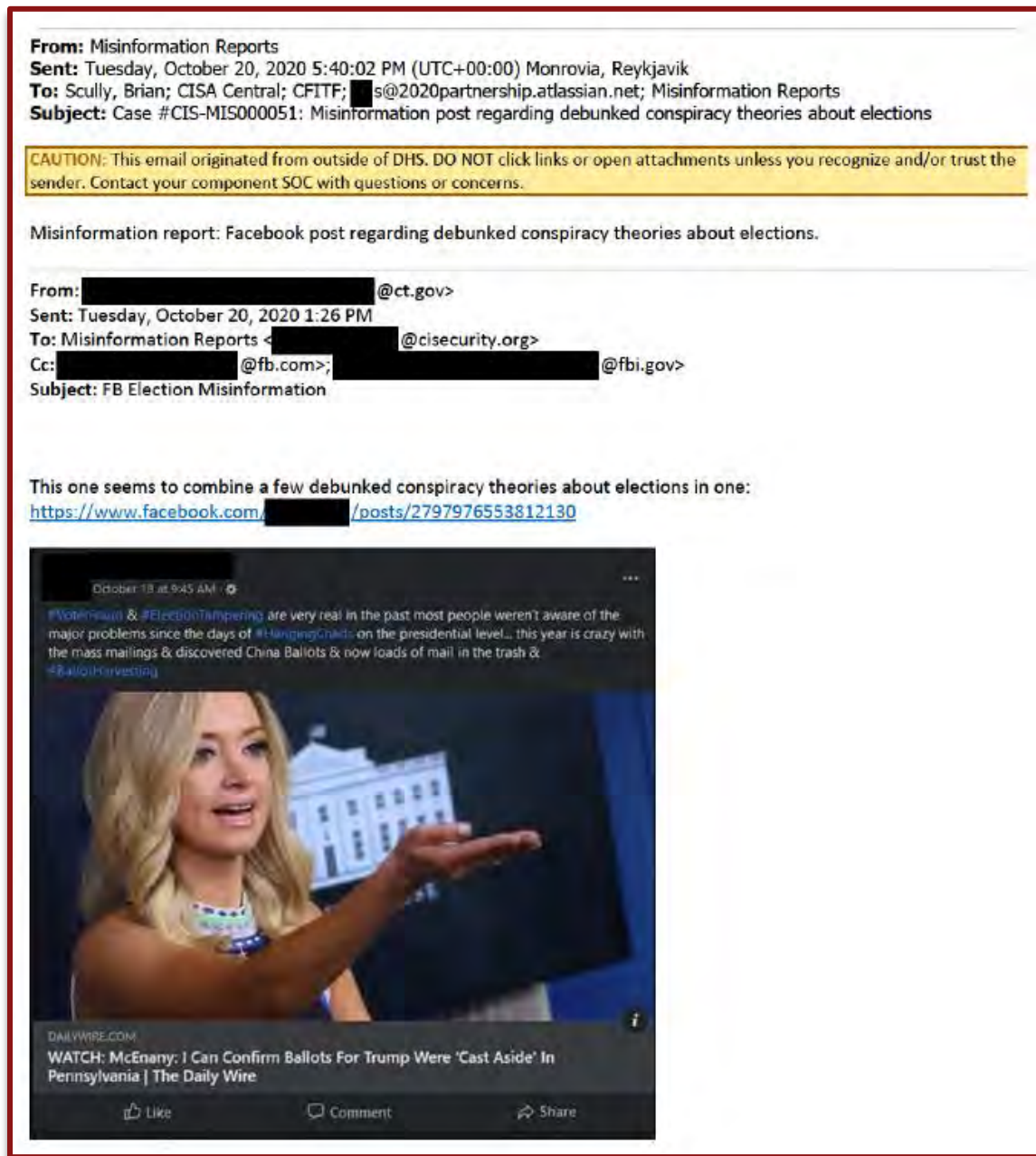
¹³⁰ *Id.* at 30.

¹³¹ *See, e.g.*, email from CIS to Brian Scully, CISA Central, CFITF, and EIP personnel (Nov. 11, 2020 4:49 PM) (on file with the Comm.).

¹³² Email from CIS to Brian Scully, CISA Central, CFITF, and EIP personnel (Nov. 11, 2020 4:49 PM) (on file with the Comm.).

¹³³ House Judiciary Committee’s Transcribed Interview of Alex Stamos (June 23, 2023), at 224 (on file with the Comm.) (“I still believe we did not receive any *direct* requests from CISA.”) (emphasis added); *Background on the SIO’s Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), <https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media> (“Did EIP receive *direct* requests from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) to eliminate or censor tweets? No.”) (emphasis added).

“Misinformation report: Facebook post regarding debunked conspiracy theories about elections.”¹³⁴ The Facebook post in question linked to an article from the Daily Wire, a prominent conservative publication.¹³⁵



Emails from CIS to CISA and EIP continued throughout the 2020 election cycle, including the months of October and November 2020, during which time many Americans relied

¹³⁴ Email from CIS to Brian Scully, CISA Central, CFITF, and EIP personnel (Oct. 20, 2020 5:40 PM) (on file with the Comm.).

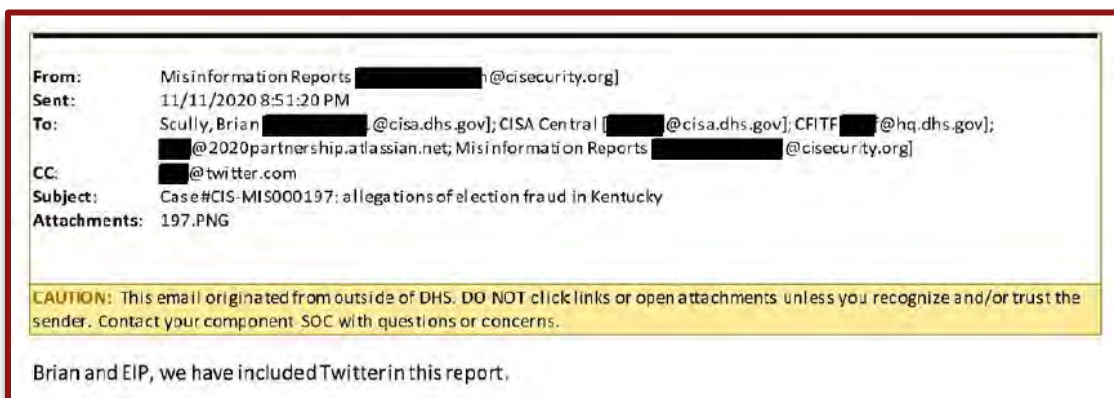
¹³⁵ See Hank Berrien, *WATCH: McEnany: I Can Confirm Ballots For Trump Were 'Cast Aside' In Pennsylvania*, THE DAILY WIRE (Sept. 24, 2020).

on information shared on social media platforms to inform their vote. Moreover, a significant number of emails from CIS were directly addressed specifically to CISA CFITF team lead “Brian [Scully] and EIP” and included employees of the social media platforms hosting the content of concern.

On November 5, for example, an email was sent from CIS’s Misinformation Reports email address to CISA, the EIP, and Facebook, which read “Brian and EIP – we have included Facebook in this report.”¹³⁶ The email copied two employees of Facebook directly on the report of “misinformation.”¹³⁷ Thus, the Facebook personnel on the receiving end of this email would understand that CISA and the EIP were receiving the same notifications at the same time. Emails such as this one revealed that the federal government had direct knowledge of what was being reported to the EIP.



On November 11, CIS sent an email to a Twitter employee, multiple CISA accounts, and the EIP, writing, “Brian and EIP, we have included Twitter in this report.”¹³⁸ The email copied an employee of Twitter on the alert about “misinformation.”¹³⁹



¹³⁶ Email from CIS to Brian Scully, CISA Central, CFITF, EIP, and Facebook employees (Nov. 5, 2020 5:18 PM) (on file with the Comm.).

¹³⁷ *Id.*

¹³⁸ Email from CIS to Brian Scully, CISA Central, CFITF, EIP, and Twitter employee (Nov. 11, 2020 8:51 PM) (on file with the Comm.).

¹³⁹ *Id.*

In one particularly alarming instance, CIS forwarded a report from the Arizona Secretary of State's Office—led at the time by Katie Hobbs, a Democrat—to CISA, the EIP, and Facebook: “Brian and EIP, I included Facebook in this report.”¹⁴⁰ In the original “misinformation” report to CIS, an Information Security Officer at the Arizona Secretary of State's Office flagged a Facebook URL, writing, “[t]his post was on a *private* [Facebook] page.”¹⁴¹

From: Misinformation Reports [REDACTED]@cisecurity.org]
Sent: 11/6/2020 10:08:42 AM
To: Scully, Brian ([REDACTED]@cisa.dhs.gov); CISA Central ([REDACTED]@cisa.dhs.gov); CFITF ([REDACTED]@hq.dhs.gov); [REDACTED]@2020partnership.allianian.net; Misinformation Reports [REDACTED]@cisecurity.org]
CC: [REDACTED]@fb.com; [REDACTED]@fb.com]
Subject: Case#CIS-MIS000182: Misinformation post that Trump already won AZ
Attachments: misinformation.jpg

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP, I included Facebook in this report.

Misinformation report: (private) Facebook post that Trump already won AZ

From: [REDACTED]@azsos.gov>
Sent: Friday, November 6, 2020 9:54 AM
To: Misinformation Reports <[REDACTED]@cisecurity.org>
Subject: Fake statement by Arizona Election Worker about fraud

Hi There,

[https://www.facebook.com/photo.php?fbid=\[REDACTED\]](https://www.facebook.com/photo.php?fbid=[REDACTED])

This post was on a private FB page, above. I've included a screenshot.

Thank you!



KATIE HOBBS
 SECRETARY OF STATE
 State of Arizona

[REDACTED]
 Information Security Officer
 Arizona Secretary of State's Office

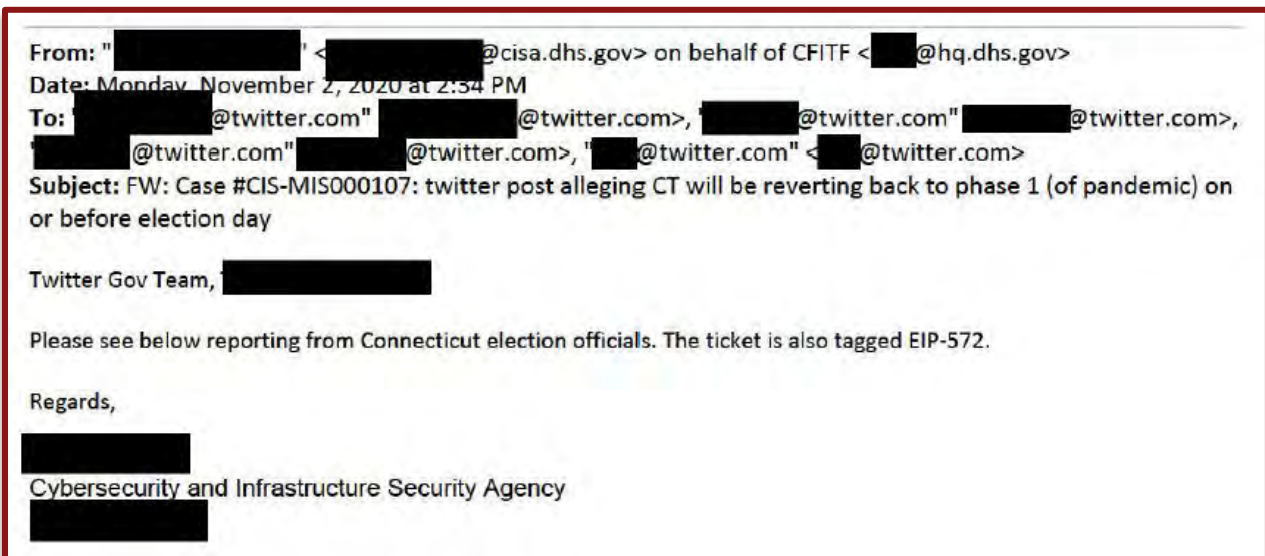
Email: [REDACTED]@azsos.gov
 Office: [REDACTED]
 Cell: [REDACTED]

¹⁴⁰ Email from CIS to Brian Scully, CISA Central, CFITF, EIP, and Facebook employees (Nov. 6, 2020 10:08 AM) (on file with the Comm.).

¹⁴¹ *Id.* (emphasis added).

While the First Amendment certainly applies to states and state officials, it is concerning that Secretary Hobbs expended her office’s limited resources to flag content on social media regarding a Republican candidate’s speech. But even more alarming, Hobbs’s staff was apparently trawling through *private* Facebook pages to identify dissent and “misinformation” for removal. According to public reporting, Hobbs’s office continued flagging social media posts well after the election, into January 2021.¹⁴² In some cases, Hobbs’s staff emailed the social media platforms directly, requesting that posts criticizing her be censored.¹⁴³

Even more damaging to the argument that CISA and EIP were independent of one another is the fact that CISA personnel, who supposedly had no access to the EIP’s Jira system, referenced the EIP-specific ticket codes when discussing “misinformation” reports. The email below, sent on November 2—the day before the 2020 election—is one such example, in which a CISA official informed Twitter: “Please see below reporting from Connecticut election officials. The ticket is *also tagged EIP-572*.”¹⁴⁴



At one point, it appears that Christopher Krebs, the then-Director of CISA, directed Robert Schaul, CISA’s Analysis and Resilience Policy Lead, to contact Graham Brookie, Senior Director of the Atlantic Council’s Digital Forensic Research Lab (DFRLab), to inquire about a particular election-related narrative spreading on social media. In the email, Schaul wrote: “We’re getting the EIP take as well but wanted to check in with you . . . [Director Krebs is] particularly interested in any analytics we can pull together on the narrative as well as where it’s coming from and who is amplifying it.”¹⁴⁵ Internal Atlantic Council documents show that

¹⁴² See Jeremy Duda, *Secretary of State Had Disinformation Pulled From Twitter*, AXIOS (Dec. 6, 2022).

¹⁴³ See Houston Keene, *Dem Gov Katie Hobbs Requested Twitter Censor Critics of Tweet Comparing Trump Supporters to Nazis*, FOX NEWS (Aug. 10, 2023).

¹⁴⁴ Email from CISA official to Twitter employees (Nov. 2, 2020 2:34 PM) (on file with the Comm.) (emphasis added).

¹⁴⁵ Email from Robert Schaul to Graham Brookie (Nov. 10, 2020 8:31 AM) (on file with the Comm.).

Brookie and others understood that Director Krebs and SIO Director Alex Stamos were texting “with some regularity.”¹⁴⁶

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Wednesday, September 30, 2020 5:05 PM
To: Andy Carvin <[REDACTED]@ATLANTICCOUNCIL.org>; Emerson Brooking <[REDACTED]@ATLANTICCOUNCIL.org>
Subject: ANDY / EMERSON -- Coordination

COORDINATION ON US DOMESTIC PRIORITIES

Hi to both –

The struggle here is that Emerson is managing efforts and Andy is managing staff and outputs. The only way to be successful is to make sure that the three of us are explicitly on the same page about how we are allocating staff to efforts.

The below is intended to do that – and I will be adding Emerson to the DCHQ WhatsApp chain, where we will coordinate in general, as soon as we're on the same page as below. Our first obligation is always to our staff and not setting them up for failure. Our second obligation is to our core work, which every single one of us is managing key elements of. Thus the burden falls on the three of us to coordinate both.

Please reply in red or blue to the below. I also didn't have explicit names in the “staffing” section of each, so please fill out.

Thanks,
Graham

Election Integrity Partnership

Key questions: What is the schedule of shifts, noting that we just need to assign people to them? EIP, the voluntary shift system is a potential challenge because it requires a person to spend X amount of hours monitoring things, which either results in no outputs being produced, or a sudden need to complete an output that the person may or may not be suited to complete, especially if it's an international member of the team with limited knowledge of US politics, geography, culture, etc.

In scenarios where something potentially important surfaces within EIP, how do we go about prioritizing it? For example, when is it simply a matter of “this is a good story so please get me a draft in 72 hours” vs “all hands on deck, this is like a major takedown?” In either case, the three of us need to be locked up in order to not undermine our whole business operation through editorial capacity, who gets assigned, scheduling, etc.

One not ideal scenario is a situation where Jean or Ayush volunteer for a few hours, end up finding something important, and then having not having all three of our awareness and approval, which could lead to significant members of staff being taken away from their core responsibilities for extended periods of days/week. In other words, a shift is just the tip of the iceberg, commitment-wise.

Another question is what constitutes a contribution to EIP. While the focus has been on the partnership and the process (which makes sense) we're part of a team reviewing leads and deciding when to act on them. But we also continue to cover election-related stories that will originate from our original research, rather than the college students volunteering at EIP, especially now that Jared is coming on board and while looking into more conspiracy related content. Can we consider those contributions? I imagine for some researchers there's more incentive to contribute when they're able to generate research leads themselves rather than being responsive to tips, though I understand responding to tips is still core to the partnership.

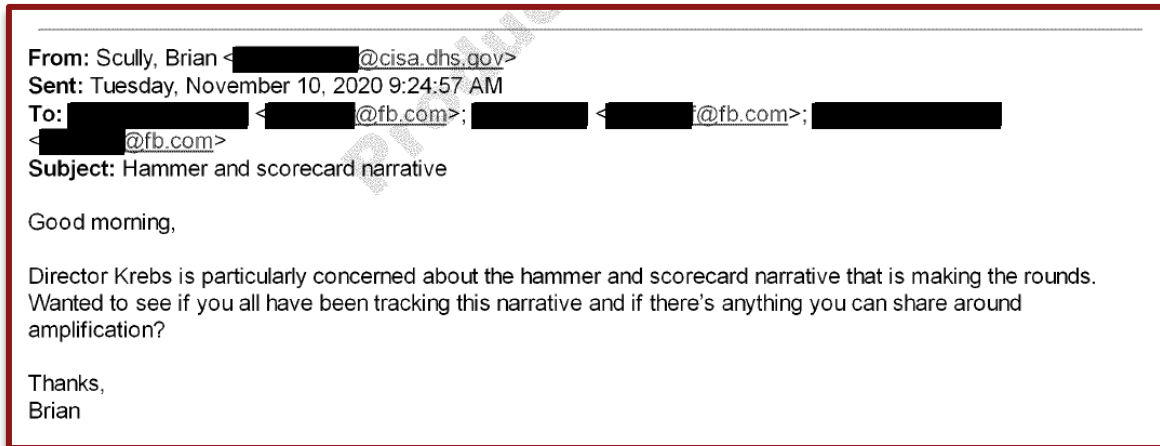
Important to note: not college kids surfacing EIP leads. Krebs CISA is texting Stamos with some regularity. A few tickets have been flagged by the platforms. Starbird's UW team is surfacing a lot of stuff using advanced soc media listening methods. College kids (T-1) just doing the first round of analysis.

The job of DFRLab is to be T-2, doing a deep dive into tickets, attaching more contextual information, and writing up a twitter thread/blog post if that's the recommendation of the researcher (and the T-3 shift manager approves).

Analysts can step away and write a blog post on-shift. That's what Alyssa did [last week](#).

¹⁴⁶ Email exchange between Graham Brookie and Atlantic Council personnel (Sept. 30, 2020 5:05 PM) (on file with the Comm.).

CISA personnel also solicited information about political speech on social media from employees of the platforms. On the same day, November 10, Scully sent an email to three Facebook employees, writing, “Director Krebs is particularly concerned about the hammer and scorecard narrative that is making the rounds. Wanted to see if you have been tracking this narrative and if there’s anything you can share around amplification?”¹⁴⁷



These emails directly contradict claims that CISA had only a “very little role, if none” in the EIP.¹⁴⁸ To the contrary, CISA had real-time awareness of what was being submitted to EIP, what steps EIP was conducting, and what actions the social media platforms were taking—and EIP and the social media platforms were aware of CISA’s significant role.

D. The State Department’s Direct Participation in the EIP’s Censorship Operation

The Global Engagement Center (GEC) is a multi-agency organization housed within the State Department, which Elon Musk has described as “[t]he worst offender in US government censorship & media manipulation.”¹⁴⁹ The GEC and GEC-funded entities have, on multiple occasions flagged content to social media platforms that included Americans engaged in constitutionally protected speech.¹⁵⁰

¹⁴⁷ Email from Brian Scully to Facebook employees (Nov. 10, 2020 9:24 AM) (on file with the Comm.).

¹⁴⁸ *Compare* House Judiciary Committee’s Transcribed Interview of Alex Stamos (June 23, 2023), at 95 (on file with the Comm.); Letter to John B. Bellinger, III, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 1, 2023), at 2; *and* Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023), at 4 (on file with the Comm.) *with* email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.); email from CISA staff to Aaron Wilson, Ben Spear, and Mike Garcia (Sept. 3, 2020, 1:51 PM) (on file with the Comm.); *and* email from Brian Scully to Facebook employees (Nov. 10, 2020 9:24 AM) (on file with the Comm.).

¹⁴⁹ Elon Musk (@elonmusk), TWITTER (Feb. 6, 2023, 6:32 PM), <https://twitter.com/elonmusk/status/1622739987031552002>.

¹⁵⁰ *See, e.g.*, Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), <https://twitter.com/mtaibbi/status/1631338687718907904> (“Here are 5500 names GEC told Twitter it believed were ‘Chinese... accounts’ engaged in ‘state-backed coordinated manipulation.’ It takes about negative ten seconds to find non-Chinese figures.”); Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), <https://twitter.com/mtaibbi/status/1631338690931826711> (“GEC’s ‘Chinese’ list included multiple Western government accounts and at least three CNN employees based abroad.”).

Unlike CISA’s pretext of peripheral non-involvement, the EIP openly admitted that the GEC “reported tickets” to the EIP in its final report looking back on the 2020 election cycle.¹⁵¹ In fact, according to that report, the GEC was one of the most frequently tagged organizations in the EIP’s Jira system.¹⁵²

On October 15, 2020, Adela Levis, an “Academic and Think-Tank Liaison” with the GEC, sent an email invitation to a meeting with the title “GEC/Election Integrity Partnership.”¹⁵³ In the body of the email, Levis wrote that the meeting was “to discuss a concrete idea we have for possible support of the EIP effort.”¹⁵⁴

Appointment

From: Levis, Adela [REDACTED]@state.gov]
Sent: 10/15/2020 3:35:38 PM
To: Levis, Adela [REDACTED]@state.gov]; Kate Starbird [REDACTED]@uw.edu]; Shelby Grossman [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e995f09f3b364dde8a93beed3a5f55db-shelbybg]; Ruppe, Adele E [REDACTED]@state.gov]; Jevin West [REDACTED]@uw.edu]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; info@eipartnership.net; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Beebe, William [REDACTED]@state.gov]; Stewart, Samaruddin K [REDACTED]@state.gov]; Dempsey, Alex L [REDACTED]@state.gov]
CC: Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2a59e34f3cbe4c78a497962dc7161e3f-ecryst]
Subject: [eip-info] RE: GEC/Election Integrity Partnership
Start: 10/16/2020 7:30:00 PM
End: 10/16/2020 8:30:00 PM
Show Time As: Busy
Recurrence: (none)

Dear All,
please join us today Friday, Oct. 16th, at 3:30pm EST/12:30 PT to discuss a concrete idea we have for possible support of the EIP effort.

Please let me know if you have any questions ahead of time.

Join Microsoft Teams Meeting
+1 509-824-1908 United States, Spokane (Toll)
Conference ID: [REDACTED]

Warm regards,
Adela

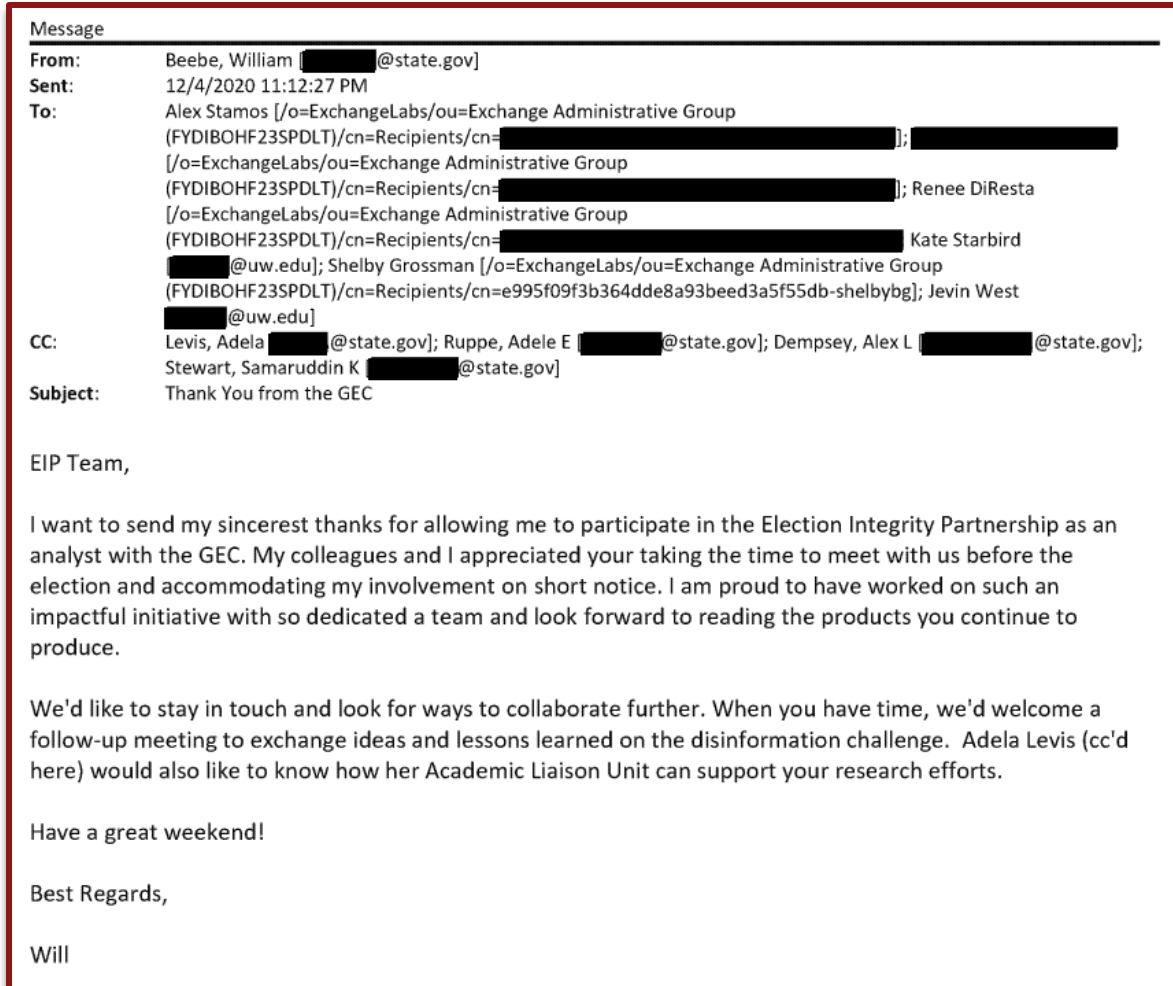
¹⁵¹ ELECTION INTEGRITY P’S HIP, *supra* note 16, at 42.

¹⁵² *Id.* at 38.

¹⁵³ Email from Adela Levis to Kate Starbird, et. al (Oct. 15, 2020 3:35 PM) (on file with the Comm.).

¹⁵⁴ *Id.*

Following the 2020 election, a “Counter Disinformation Analyst” with the GEC sent an effusive email to SIO Director Alex Stamos, SIO research manager Renée DiResta, and UW’s CIP Director Kate Starbird, among others, with the subject “Thank You from the GEC.”¹⁵⁵ The analyst gushed: “I want to send my sincerest thanks for allowing me to participate in the Election Integrity Partnership with the GEC. My colleagues and I appreciated your taking the time to meet with us before the election and accommodating my involvement on short notice.”¹⁵⁶ The analyst continued, “I am proud to have worked on such an impactful initiative with so dedicated a team.”¹⁵⁷



¹⁵⁵ Email from William Beebe to Alex Stamos, Renée DiResta, Kate Starbird, and Jevin West (Dec. 4, 2020 11:12 PM) (on file with the Comm.).

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

E. Other Federal Agencies' Involvement with the EIP: the FBI and the NSA

CISA was not the only government entity apprised of the EIP's activities. On June 23, 2023, the Committee and Select Subcommittee conducted a transcribed interview of Alex Stamos, examining his and CISA's involvement in the EIP. During the interview, Stamos testified that the SIO briefed several other government agencies about the EIP, including the National Security Agency (NSA) and Cyber Command. Stamos further testified that Federal Bureau of Investigation (FBI) Special Agent Elvis Chan, who was the primary liaison between the FBI and Silicon Valley and was involved in the suppression of news about information damaging to the Biden family found on a laptop belonging to Hunter Biden, arranged the SIO-NSA briefing.

Stamos testified:

Q. Which other federal agencies did EIP brief?

A. I did a briefing for General Nakasone, then the director of NSA and Cyber Command

Q. Did the FBI also receive briefings for the election?

A. The FBI was part of that briefing, so I did it from the FBI office in – in San Francisco because I just can't Zoom into the NSA.

Q. Do you recall who set up the meeting between you and the NSA?

A. Elvis Chan had set up the – so the meeting was set up because Nakasone had come to campus. Elvis was the facilitator who provided the space and participated, listened to the briefing in San Francisco.

Q. Yeah. Did you know Mr. Chan before this meeting had occurred?

A. I did.¹⁵⁸

The SIO continued to provide the FBI with updates on the EIP throughout the 2020 election cycle. For example, on October 5, 2020, Alex Stamos sent an email to Elvis Chan, writing: "Right now, the Election Integrity Partnership is running three shifts each weekday . . . We don't have any good indications of foreign interference from our work, and most of the things we have spotted can be tied to known domestic actors," i.e., Americans.¹⁵⁹

¹⁵⁸ House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 98-99 (on file with the Comm.).

¹⁵⁹ Email from Alex Stamos to Elvis Chan and Renee DiResta (Oct. 5, 2020 7:44 PM) (on file with the Comm.).

From: Alex Stamos <[REDACTED]@stanford.edu>
Sent: Monday, October 5, 2020 7:44 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>; Renee DiResta <[REDACTED]@stanford.edu>
Subject: Re: [EXTERNAL EMAIL] - RE: Status Update

Elvis-

Right now, the Election Integrity Partnership is running three shifts each weekday (and one on Sunday) looking for election related disinformation. We are handling about a dozen "incidents" per day, which can correspond to multiple pieces of disinformation or just one (this is varying widely). We are intaking reports from locals via EI-ISAC, working with NGOs like Common Cause, and routing issues to platforms to get handled.

It's working pretty well. You can see a handful of incidents we wrote up at eipartnership.net. We will be adding shifts in a couple of weeks and will be staffing a war room at my house (post COVID-testing) on election day.

CONFIDENTIAL

SIO-HJC014624

What's your mandate look like? We don't have any good indications of foreign interference from our work, and most of the things we have spotted can be tied to known domestic actors. Probably some foreign amplifiers, but figuring that out is generally outside of our scope and the data we have access to. Check out our "Rapid Reaction" posts and see if any of those kinds of topics are in scope for your work.

Alex

In response to Stamos's question regarding the FBI's mandate, Chan wrote: "The FBI [San Francisco] mandate is to be the conduit to/from the social media companies for all election-related threats, whether foreign or domestic. We've been receiving mostly domestic voter suppression-related accounts to flag for social media companies as each state had its primaries."¹⁶⁰

Message

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 10/6/2020 4:25:46 PM
To: Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]
Subject: RE: [EXTERNAL EMAIL] - RE: Status Update

Hi Alex,

It seems like you have a good system in place and are plugged in with the relevant entities. The FBI SF mandate is to be the conduit to/from the social media companies for all election-related threats, whether foreign or domestic. We've been receiving mostly domestic voter suppression-related accounts to flag for social media companies as each state had its primaries.

At our command post, we'll have a NCRIC-embed who will have access to HISN, EI-ISAC, and MS-ISAC feeds as well. We are hoping USIC partners will be able to declassify information fast enough for us to push out to the companies for awareness.

Since you are also flagging things and sending them to the social media companies, I know they'll be able to relay any coordinated campaigns they see to us for examination and possible case opening. Let's plan to stay in touch as things start to heat up. Thanks!

Regards,
 Elvis

¹⁶⁰ Email from Elvis Chan to Alex Stamos and Renee DiResta (Oct. 6, 2020 4:25 PM) (on file with the Comm.).

III. THE EIP’S JIRA TICKETS: AN ENCYCLOPEDIA OF CONSERVATIVE CENSORSHIP

An examination of the Jira tickets themselves reveals a veritable who’s who of prominent conservative voices targeted for censorship by CISA and the EIP. On March 17, 2023, in response to increased media scrutiny of the SIO’s activities, including the Select Subcommittee’s March 9 hearing on the Twitter Files, the SIO published a blog post riddled with false statements about the EIP.¹⁶¹ For instance, the blog post stated that the EIP did not “‘target’ or discriminate against conservative social media accounts or content.”¹⁶² While it is true that the EIP, did flag non-conservative content to maintain a façade of neutrality, the EIP’s reports show a clear attempt to suppress conservative speech in particular.¹⁶³

According to the EIP’s post-election report, there are four categories of election-related “misinformation” that the EIP considered to be “in scope” of the type of “misinformation” the EIP would analyze.¹⁶⁴ Some of the categories, like “procedural interference” are relatively anodyne—although often stretched beyond its intended contours—and include things like “[c]ontent that misleads voters about how to correctly sign a mail-in ballot” and “[c]ontent that encourages voters to vote on a different day.”¹⁶⁵

The EIP repeatedly used its fourth category, in particular, to justify the censorship of conservative political speech: the “Delegitimization of Election Results,” defined as “[c]ontent that delegitimizes election results on the basis of false or misleading claims.”¹⁶⁶ This arbitrary and inconsistent standard was determined by political actors masquerading as “experts” and academics. But even more troubling, the federal government was heavily intertwined with the universities in making these seemingly arbitrary determinations that skewed against one side of the political aisle.

The EIP routinely flagged conservative content on social media under the guise that it was inappropriately “delegitimizing” election results, even in cases where the content was factually accurate. Criticism of the electoral system is constitutionally protected speech. A political system that allows a small minority of government-approved “experts” to exercise influence over the ability of other citizens to express concerns with the government represents a profound threat to our constitutional republic. Indiscriminately or improperly suppressing accusations of electoral fraud necessarily suppresses speech about real instances of electoral fraud, thereby allowing the government free rein to conduct elections in a manner that is not accountable to the American people.¹⁶⁷

¹⁶¹ Stanford Internet Observatory, *Background on the SIO’s Projects on Social Media*, STANFORD UNIV. (Mar. 17, 2023).

¹⁶² *Id.*

¹⁶³ So that the American people can judge for themselves, Appendix II of this report includes all of the EIP and Virality Project Jira ticket data provided to the Committee pursuant to a subpoena to Stanford University.

¹⁶⁴ ELECTION INTEGRITY P’SHIP, *supra* note 16, at vi, 246.

¹⁶⁵ *Id.* at vi, 7.

¹⁶⁶ *Id.* at vi.

¹⁶⁷ See, e.g., Susan Haigh, *Connecticut Judge Orders New Mayoral Primary After Surveillance Videos Show Possible Ballot Stuffing*, AP (Nov. 1, 2023) (“A judge on Wednesday tossed out the results of a Democratic mayoral primary in Connecticut’s largest city and ordered that a new one be held, citing surveillance videos showing people stuffing multiple absentee ballots into outdoor collection boxes.”).

A. Dropping the Pretense of “Mis- and Disinformation”: The EIP’s Absurd Approach to Classification

The EIP acknowledged in its report that it is “not a fact-checking organization” and that “[f]or some tickets, it was not possible to find an external fact-check for the content, either because no fact-checker had yet addressed the issue, or because the information was resistant to simple verification.”¹⁶⁸ Unbelievably, the EIP also admitted that its analysts “identified at least one external fact-check source for approximately 42% of the in-scope tickets.”¹⁶⁹ In other words, EIP analysts were unable to identify a single external source to support its designation of a particular post or narrative as “mis- or disinformation” in a *majority of posts* it flagged.

The general reliance of social media censors on fact-checkers, many of whom have a distinctly liberal political bias, creates an environment that is hostile to free speech, especially conservative viewpoints, and is concerning in and of itself. However, the fact that the EIP could not find even a single fact-checker, biased or not, before flagging content to social media in a majority of cases and was willing to publicly admit to that fact, is indicative of a brazen and megalomaniacal approach to censorship, unbothered by the truth or maintaining even the appearance of political neutrality.

For cases in which the EIP was unable to fact-check a claim or narrative it had identified, the EIP could have opted not to flag the content to the social media platforms, given that there was uncertainty about the truth value of the content in question. Instead, the EIP aggressively flagged such posts to the platforms, noting in the tickets that it had no justification for reporting the content other than CISA’s and the EIP’s own political agenda.

For example, an entry in EIP-713, a Jira ticket regarding a Gateway Pundit article, submitted on the afternoon of Election Day, November 3, read: “We are sending this to you quickly as we likely won’t be able to figure out a factcheck here.”¹⁷⁰ In EIP-418, concerning a tweet from One America News Network, a contributor wrote: “We have not seen a fact-check on this direct story, but this story is targeted at discrediting the validity of vote-by-mail.”¹⁷¹ In its report, the EIP claimed that its purpose was “to identify and analyze mis- and disinformation,” which even CISA publicly defines as *false* information.¹⁷² However, the approach demonstrated in these and other tickets makes clear that the EIP’s focus was not on the truth, but rather the advancement of viewpoint-based discrimination.

¹⁶⁸ ELECTION INTEGRITY PARTNERSHIP, *supra* note 16, at 10.

¹⁶⁹ *Id.*

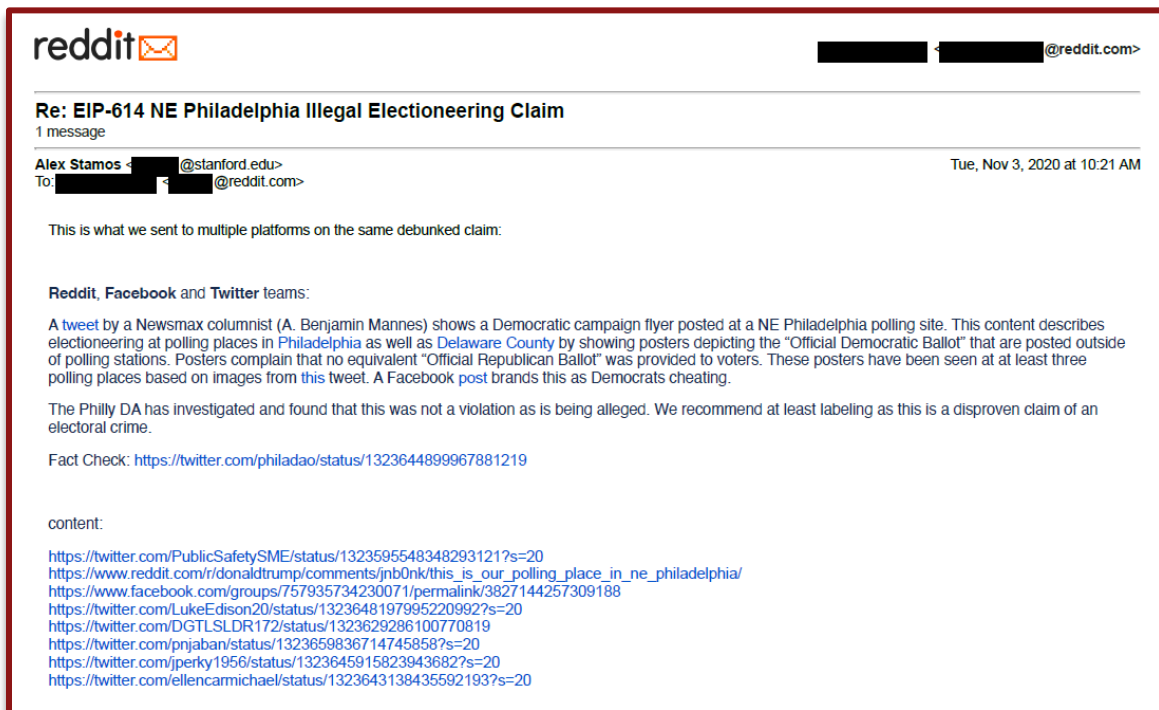
¹⁷⁰ EIP-713, submitted by [REDACTED], ticket created (Nov. 3, 2020, 2:45 PM) (archived Jira ticket data produced to the Comm.).

¹⁷¹ EIP-418, submitted by [REDACTED], ticket created (Oct. 21, 2020, 9:30 AM) (archived Jira ticket data produced to the Comm.); *see also* OAN Newsroom, *Reports Claim 440K Questionable Ballots Sent To Deceased Or Inactive Voters In Calif.*, ONE AMERICA NEWS NETWORK (Oct. 20, 2020) available at <http://web.archive.org/web/20201021170509/https://www.oann.com/reports-claim-440k-questionable-ballots-sent-to-deceased-or-inactive-voters-in-calif/>.

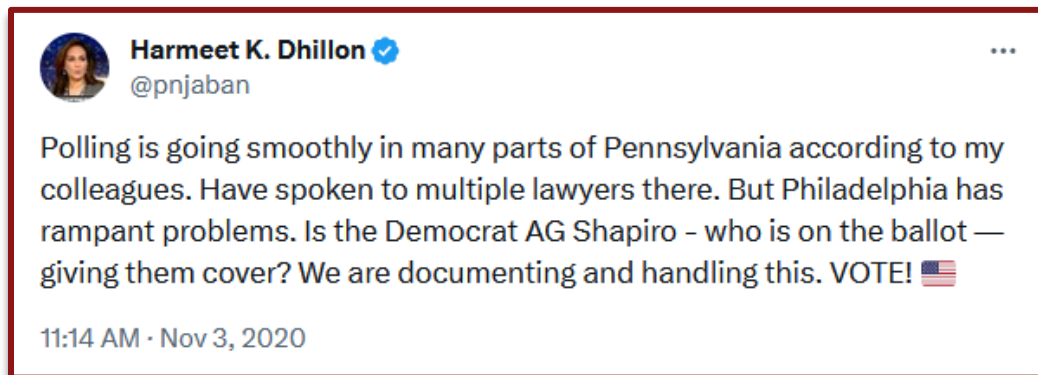
¹⁷² ELECTION INTEGRITY PARTNERSHIP, *supra* note 16, at vi.

B. Efforts to Censor the Truth

Even in the limited cases in which the EIP was able to find an external fact-check, the fact-checkers were often unsure themselves, admitted that the relevant claims were not false, or subject to undeniable political bias. On November 3, 2020, Alex Stamos sent an email to a Reddit employee with the contents of a Jira ticket concerning irregularities at polling sites in Philadelphia, as Reddit refused to participate in the Jira system directly.¹⁷³



The ticket, although ostensibly about a specific claim regarding signs posted outside polling sites, flagged more generic content, including the below tweet from Republican Party official Harmeet Dhillon.¹⁷⁴ The "Fact Check" cited in the ticket is a tweet from the office of the Democratic District Attorney in Philadelphia and does not dispute any of the claims in Dhillon's post.



¹⁷³ Email from Alex Stamos to Reddit employee (Nov. 3, 2020 10:21 AM) (on file with the Comm.).

¹⁷⁴ *Id.*; see also Harmeet K. Dhillon (@pnjaban), TWITTER (Nov. 3, 2020, 11:14 AM).

C. Efforts to Censor President Trump and His Family

The most prominent conservative voice targeted by CISA and the EIP was none other than the sitting President of the United States, Donald Trump. On October 27, 2020, a local official reported a tweet from President Trump to CIS’s “misinformation” tipline, which then forwarded the report to the EIP and CISA, per its usual protocol.¹⁷⁵ CISA then flagged the content to Twitter.¹⁷⁶ To be clear, this evidence shows an unelected executive branch official flagging a statement from the elected leader of the executive branch for removal from one of the world’s largest and most active public forums. CISA has not provided the Committee any evidence that it contacted the White House prior to making the referral to opine on the veracity of the claim in the tweet.



¹⁷⁵ EIP-482, submitted by CIS Misinformation Reporting, ticket created (Oct. 27, 2020, 1:07 PM) (archived Jira ticket data produced to the Comm.); *see also* Donald J. Trump (@realDonaldTrump), TWITTER (Oct. 27, 2020 3:53 AM), available at

<https://web.archive.org/web/20201027105312/https://twitter.com/realDonaldTrump/status/1321042229838909441>.

¹⁷⁶ *Id.*

From: Misinformation Reports <[REDACTED]@cisecurity.org>
Sent: Tuesday, October 27, 2020 4:07 PM
To: [REDACTED]@2020partnership.atlassian.net; Misinformation Reports <[REDACTED]@cisecurity.org>; Scully, Brian <[REDACTED]@cisa.dhs.gov>; CFITF <[REDACTED]@hq.dhs.gov>; CISA Central <[REDACTED]@cisa.dhs.gov>
Subject: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation tweet regarding re-voting

From: Scully, Brian
Sent: Tuesday, October 27, 2020 4:09 PM
To: [REDACTED]@twitter.com>; [REDACTED]@twitter.com>; [REDACTED]@twitter.com>
Cc: CFITF <[REDACTED]@hq.dhs.gov>; Misinformation Reports <[REDACTED]@cisecurity.org>
Subject: FW: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

Please see below report from Washington.

Thanks,
 Brian

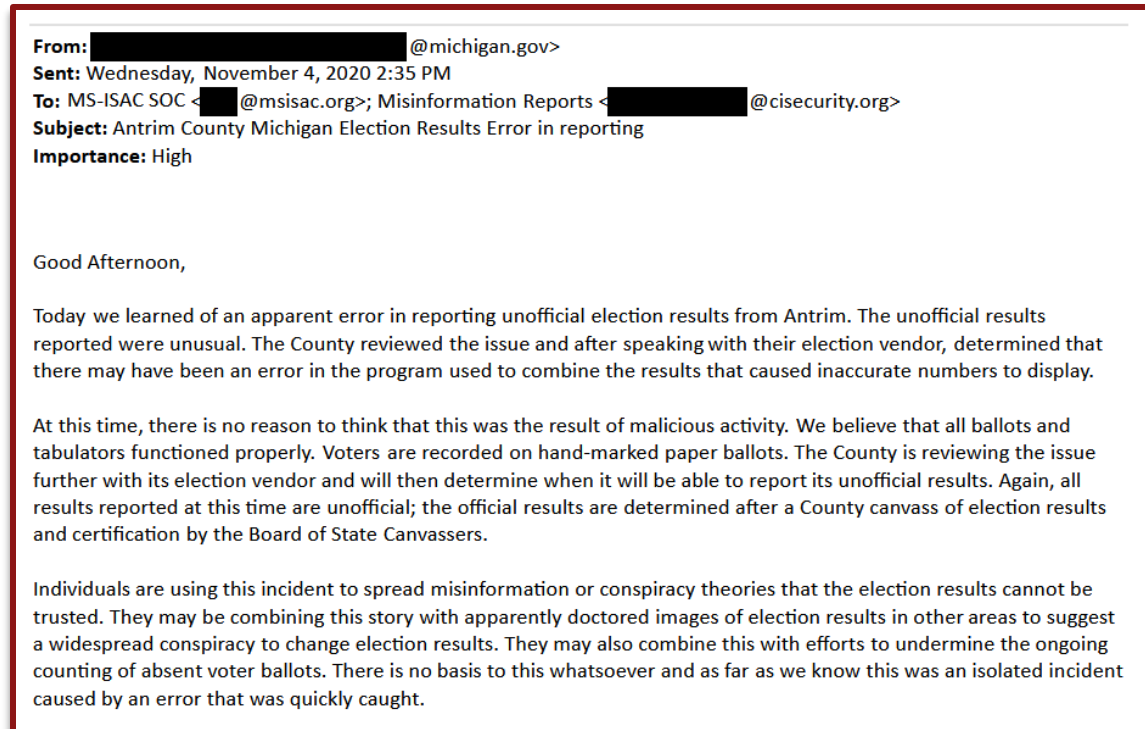
CISA’s involvement in the attempted censorship of President Trump did not end once the report had been submitted to Twitter. Instead, as noted in an entry on the Jira ticket identified as EIP-482: “We [the EIP] heard back from Twitter through CISA” regarding how Twitter decided to handle the reported tweet.¹⁷⁷

This was not the only time CISA and the EIP attempted to hinder the duly elected President’s ability to communicate with the American public. On November 4, 2020, a Michigan election official made a “misinformation” report to CIS, writing, “Today we learned of an apparent error in reporting unofficial election results from Antrim. The unofficial results reported were unusual. The County reviewed the issue and after speaking with their election vendor, determined that there may have been an error in the program used to combine the results that caused inaccurate numbers to display.”¹⁷⁸ According to the election official, this was concerning because “[i]ndividuals are using this incident to spread misinformation or conspiracy theories that the election results cannot be trusted.”¹⁷⁹

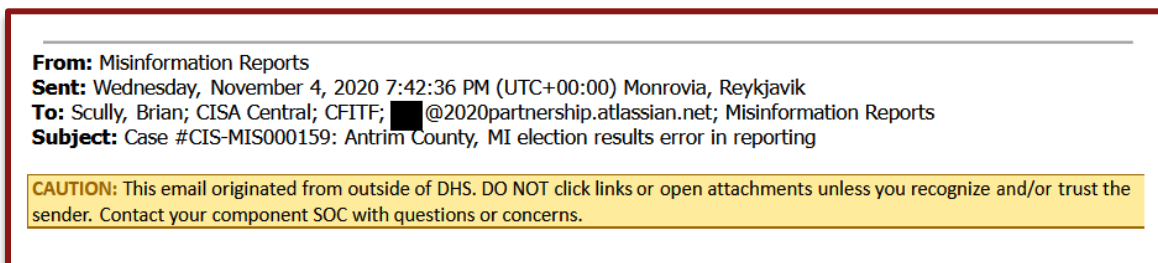
¹⁷⁷ See EIP-482, *supra* note 175.

¹⁷⁸ Email from Michigan election official to CIS and MS-ISAC personnel (Nov. 4, 2020 2:35 PM) (on file with the Comm.).

¹⁷⁹ *Id.*



As usual, the report was then sent at the same time to the EIP and CISA for further action.¹⁸⁰



In response, the EIP dutifully activated its surveillance antennae, scouring social media for posts and activity related to the reporting irregularity that the state election official confirmed had actually taken place. The EIP then reported a series of URLs to Twitter and Facebook regarding the incident in Antrim County.¹⁸¹ Facebook replied that it had “applied the relevant labels on the links you shared.”¹⁸² One of the links included in the ticket was a tweet from

¹⁸⁰ Email from CIS personnel to Brian Scully, CISA Central, CFITF, and EIP personnel (Nov. 4, 2020 7:42 PM) (on file with the Comm.).

¹⁸¹ See EIP-822, submitted by CIS Misinformation Reporting, ticket created (Nov. 4, 2020, 11:42 AM) (archived Jira ticket data produced to the Comm.); see also Donald J. Trump (@realDonaldTrump), TWITTER (Nov. 7, 2020 7:23 AM), available at <https://web.archive.org/web/20201107152307/http://twitter.com/realDonaldTrump/status/1325096422799237120>; Alana Mastrangelo, *Georgia Counties Using Same Software as Michigan Counties Also Encounter ‘Glitch’*, BREITBART (Nov. 7, 2020) available at <https://web.archive.org/web/20201108204307/https://www.breitbart.com/politics/2020/11/07/georgia-counties-using-same-software-as-michigan-counties-also-encounter-glitch/>.

¹⁸² *Id.*

President Trump, in which the President shared an article from Breitbart, with the added commentary: “What a total mess this ‘election’ has been!”¹⁸³



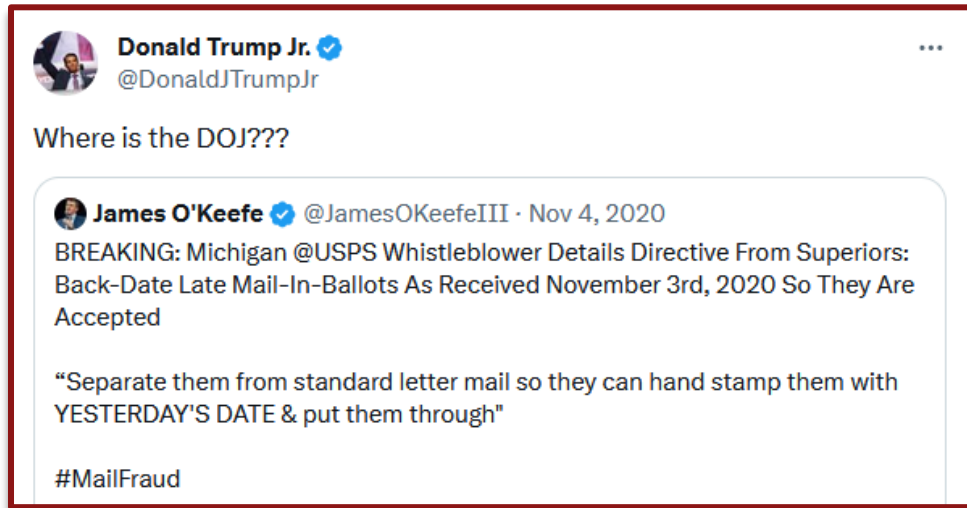
CISA has not provided the Committee with any evidence that the agency contacted the White House directly to convey its concerns with the tweet, instead relying on the EIP to conduct censorship by proxy.

Members of President Trump’s family were also targeted for censorship by CISA and the EIP. During the course of its work in the 2020 election cycle, the EIP flagged multiple posts from both Donald Trump Jr. and Eric Trump, some of which appear to have been removed or labelled.¹⁸⁴ In one ticket, tagged EIP-867, the EIP flagged Donald Trump Jr.’s Twitter account

¹⁸³ *Id.*

¹⁸⁴ *See, e.g.*, EIP-949, submitted by Alex Stamos, ticket created (Nov. 7, 2020, 8:36 AM) (archived Jira ticket data produced to the Comm.); *see also* Eric Trump (@EricTrump), TWITTER (Nov. 8, 2020 4:22 AM), available at <https://web.archive.org/web/20201108122250/https://twitter.com/EricTrump/status/1325413441310482432>; Alana Mastrangelo, *Georgia Counties Using Same Software as Michigan Counties Also Encounter ‘Glitch’*, BREITBART

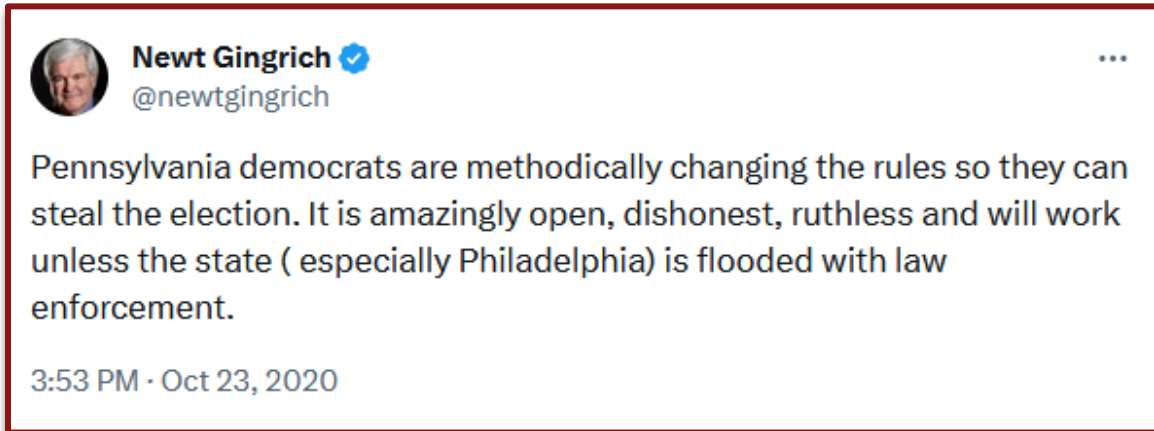
for simply reposting a Tweet from conservative journalist James O’Keefe and asking: “Where is the DOJ???”¹⁸⁵



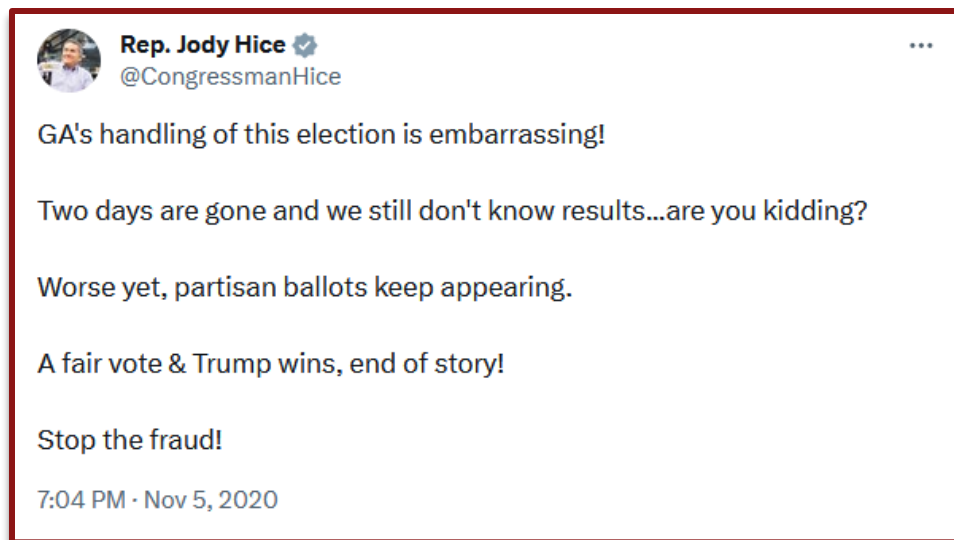
(Nov. 7, 2020) available at <https://web.archive.org/web/20201108204307/https://www.breitbart.com/politics/2020/11/07/georgia-counties-using-same-software-as-michigan-counties-also-encounter-glitch/>; Donald Trump Jr. (@DonaldJTrumpJr), TWITTER (Nov. 6, 2020 8:47 PM), available at <https://web.archive.org/web/20220712020104/https://twitter.com/DonaldJTrumpJr/status/1324815748108345344>.
¹⁸⁵ EIP-867, submitted by [REDACTED], ticket created (Nov. 18, 2020, 1:29 PM) (archived Jira ticket data produced to the Comm.).

D. Efforts to Censor Political Candidates and Legislators

CISA's and the EIP's censorship enterprise targeted not only President Trump but also former, current, and prospective legislators. In EIP-450, the EIP flagged a tweet, pictured below, from former Speaker of the House of Representatives Newt Gingrich about changes to Pennsylvania election law.¹⁸⁶



In EIP-904, the EIP attempted to censor Rep. Jody Hice, a sitting Republican Congressman from Georgia, engaging in core political speech criticizing the administration of the election in his home state.¹⁸⁷



¹⁸⁶ See EIP-450, submitted by [REDACTED], ticket created (Oct. 23, 2020, 1:43 PM) (archived Jira ticket data produced to the Comm.).

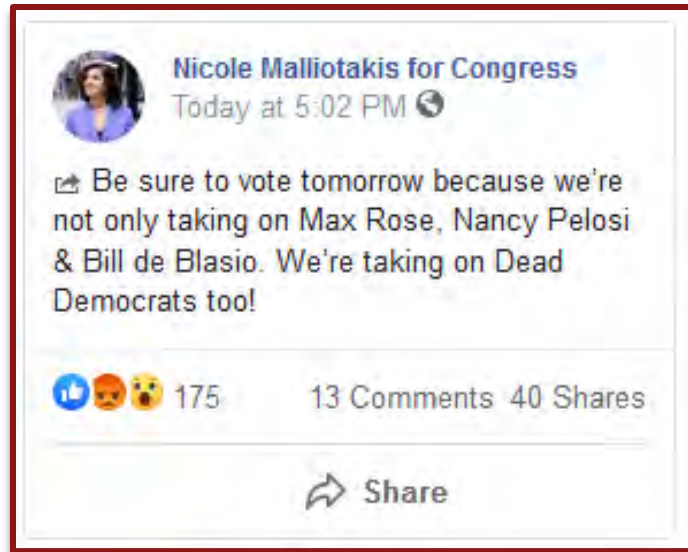
¹⁸⁷ See EIP-904, submitted by Josh Aaron Goldstein, ticket created (Nov. 5, 2020, 4:30 PM) (archived Jira ticket data produced to the Comm.); see also Rep. Jody Hice (@CongressmanHice), TWITTER (Nov. 5, 2020 4:04 PM), available at <http://web.archive.org/web/20201106010558/https://twitter.com/CongressmanHice/status/1324502770813194241?s=20>.

EIP analysts also flagged a completely innocuous tweet from Sen. Thom Tillis of North Carolina in EIP-936 because the group deemed his declaration of victory to be premature.¹⁸⁸ Sen. Tillis did, in fact, win his reelection to the Senate.



¹⁸⁸ EIP-936, submitted by [REDACTED], ticket created (Nov. 16, 2020, 2:08 PM) (archived Jira ticket data produced to the Comm.); see also Joseph Curl, *Republican Thom Tillis Claims Victory in North Carolina*, THE DAILY WIRE (Nov. 4, 2020) available at <https://web.archive.org/web/20201108225403/https://www.dailywire.com/news/republican-thom-tillis-claims-victory-in-north-carolina>; Thom Tillis (@ThomTillis), TWITTER (Nov. 3, 2020 9:05 PM), available at <https://web.archive.org/web/20201108230403/https://twitter.com/ThomTillis/status/1323853951394074629>.

The EIP further targeted Republican candidates for political office, including those who would later be seated in Congress. For example, in EIP-596, the EIP flagged this Facebook post from Rep. Nicole Malliotakis’s campaign page. The post appears to have been removed by Facebook.¹⁸⁹



In EIP-780, the EIP’s “analysts” flagged a post from Rep. Marjorie Taylor Greene’s campaign account, in which the Congresswoman encouraged her followers to share her post.¹⁹⁰ It is a slippery slope if political candidates and their supporters are not able to express legitimate concerns with the election process. While many disinformation experts are quick to criticize Republican candidates about undermining “faith in elections,” these experts appear to be notably silent whenever Democrats objected to election results in other elections, or baselessly blamed election losses on unfounded claims of fraud or cheating. Perhaps most notably, many Democrats repeated the unfounded claim that President Trump colluded with Russia, rather than accept the truth that his victory over Hillary Clinton was legitimate.¹⁹¹ But as the disinformation experts in their own words acknowledge, the study of “disinformation” is of course “inherently political.”¹⁹²

¹⁸⁹ EIP-596, submitted by [REDACTED], ticket created (Nov. 3, 2020, 7:46 PM) (archived Jira ticket data produced to the Comm.); see also Nicole Malliotakis for Congress (@NicoleForCongress), FACEBOOK (Nov. 3, 2020 5:02 PM) available at <https://web.archive.org/web/20201103040541/https://www.facebook.com/NicoleForCongress/posts/2718395868412350>.

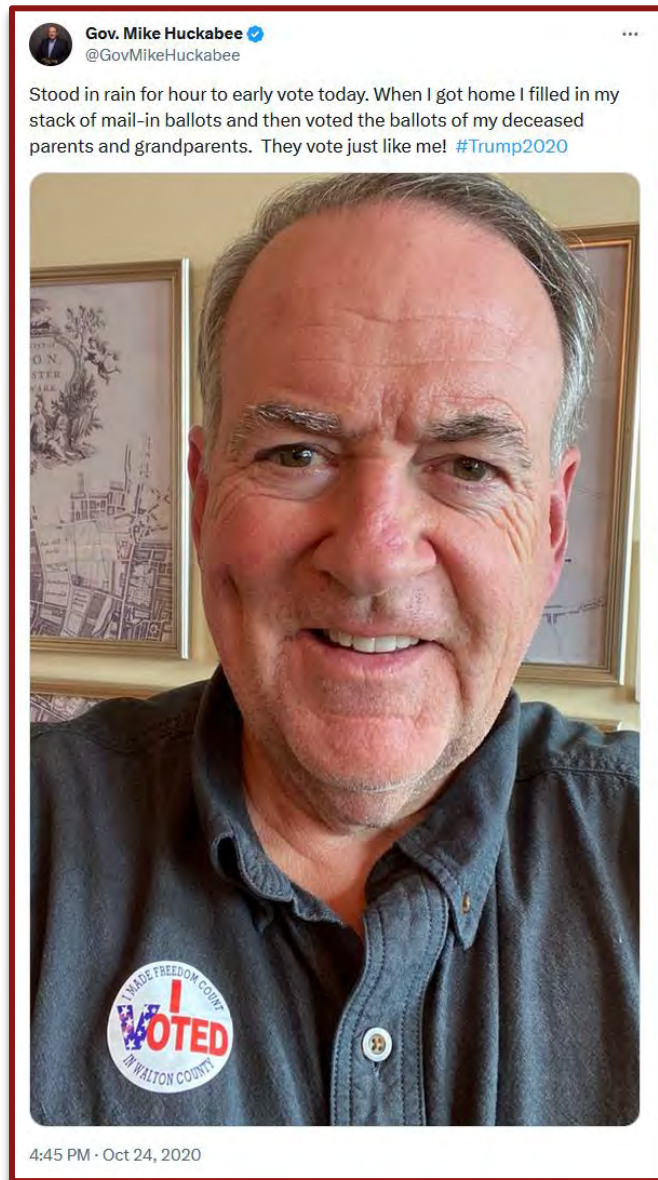
¹⁹⁰ EIP-780, submitted by Melanie Smith, ticket created (Nov. 4, 2020, 12:32 AM) (archived Jira ticket data produced to the Comm.); see also Marjorie Taylor Greene For Congress (@mtgreene) TWITTER (Nov. 3, 2020 11:37 PM) available at <http://web.archive.org/web/20201104160034/https://twitter.com/mtgreene/status/1323892005584412674>; Marjorie Taylor Greene For Congress (@mtgreene) TWITTER (Nov. 4, 2020 7:58 AM) available at <http://web.archive.org/web/20201104161216/https://twitter.com/mtgreene/status/1324019263255040003>; Marjorie Taylor Greene For Congress (@mtgreene) TWITTER (Nov. 4, 2020 8:02 AM) available at <http://web.archive.org/web/20201104160746/https://twitter.com/mtgreene/status/1324018211021594626>; Matt Walsh (@MattWalshBlog) TWITTER (Nov. 4, 2020) available at <http://web.archive.org/web/20201104153558/https://twitter.com/MattWalshBlog/status/1323999569466789889>.

¹⁹¹ See, e.g., Paul Farhi, *The Washington Post corrects, removes parts of two stories regarding the Steele dossier*, WASH. POST (Nov. 12, 2021); see generally REPORT ON MATTERS RELATED TO INTELLIGENCE ACTIVITIES AND INVESTIGATIONS ARISING OUT OF THE 2016 PRESIDENTIAL CAMPAIGNS, Office of Special Counsel John H. Durham, U.S. DEP’T OF JUSTICE (May 12, 2023); see also Susan Haigh, *Connecticut Judge Orders New Mayoral Primary After Surveillance Videos Show Possible Ballot Stuffing*, AP (Nov. 1, 2023) (“A judge on Wednesday tossed out the results of a Democratic mayoral primary in Connecticut’s largest city and ordered that a new one be held, citing surveillance videos showing people stuffing multiple absentee ballots into outdoor collection boxes.”).

¹⁹² Email from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.); see also Kate Starbird et al., Proposal to the National Science Foundation for “Collaborative Research: SaTC: Core: Large: Building Rapid-Response Frameworks to Support Multi-Stakeholder Collaborations for Mitigating Online Disinformation” (Jan. 29, 2021) (unpublished proposal) (on file with the Comm.) (“The study of disinformation today invariably includes elements of politics.”).

E. Efforts to Censor Humor and Satire

Documents obtained by the Committee and Select Subcommittee also show that the EIP flagged content that was obviously humorous and satirical. For example, EIP analysts internally identified a tweet from former Governor of Arkansas Mike Huckabee, in which Huckabee made a quip about dead relatives voting.¹⁹³ According to the ticket, labeled EIP-460, an individual affiliated with the EIP wrote, “ISAC Partners, adding you to this thread for visibility. We recommend to Twitter that this be labeled, especially under option (b) as it was posted by a public figure.”¹⁹⁴



¹⁹³ See EIP-460, submitted by [REDACTED], ticket created (Oct. 25, 2020, 11:36 AM) (archived Jira ticket data produced to the Comm.); see also Gov. Mike Huckabee (@GovMikeHuckabee) TWITTER (Oct. 24, 2020 1:45 PM) available at

<https://web.archive.org/web/20201025064250/https://twitter.com/GovMikeHuckabee/status/1320104112420212739>.

¹⁹⁴ *Id.*

The EIP even objected to and attempted to censor humorous images that could not reasonably be perceived as genuine.¹⁹⁵ Both images, replicated below and flagged in EIP-811, are self-evidently doctored and depict the transportation of boxes labelled “Emergency Democrat Votes.”¹⁹⁶ The EIP wrote in the ticket: “Users on Twitter and Facebook are sharing manipulated images of people moving boxes in trucks labeled ‘Emergency Democrat Votes.’ We suggest labeling or removing tweets that use this photo, as it could undermine people’s faith in the legitimacy of the election process. Though the image may seem ridiculous, some users may still believe it is real.”¹⁹⁷



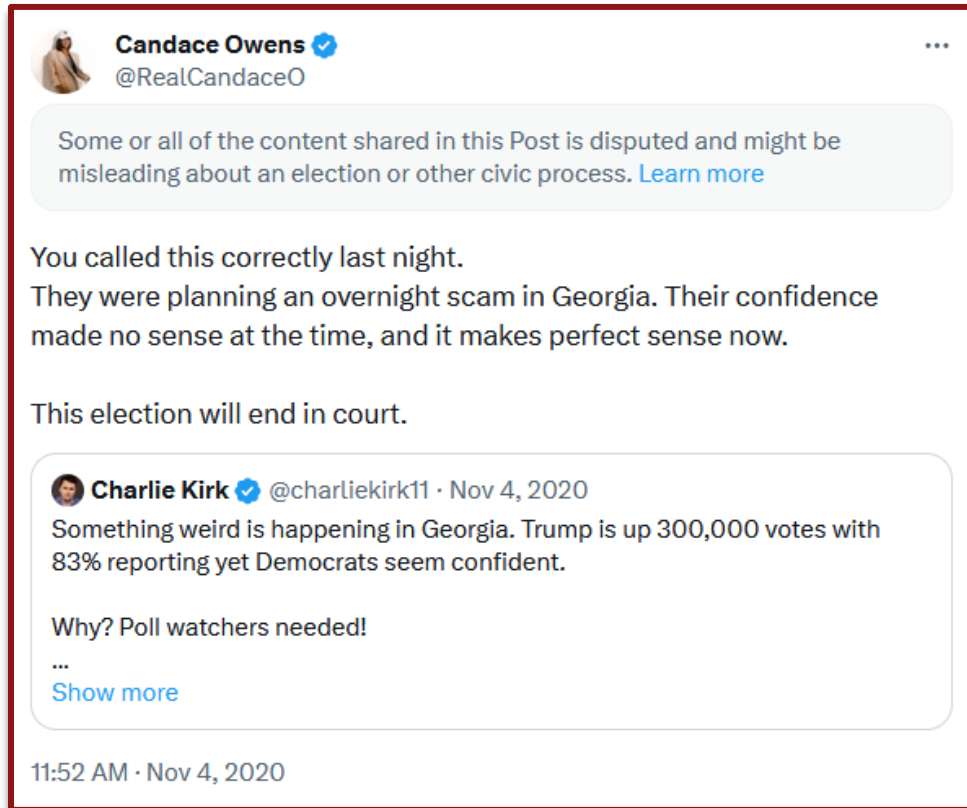
¹⁹⁵ EIP-811, submitted by [REDACTED], ticket created (Nov. 16, 2020, 3:25 PM) (archived Jira ticket data produced to the Comm.); *see also* Dark to Light (@pushforward40) TWITTER (Nov. 4, 2020 9:27 AM) available at <https://web.archive.org/web/20201104182147/https://twitter.com/pushforward40/status/1324040688351236099>; Carol Ricks (@BVMgroupie) TWITTER (Nov. 4, 2020 10:33 AM) available at <https://web.archive.org/web/20201104215451/https://twitter.com/BVMgroupie/status/1324057218950594560>; Paula Priesse, FACEBOOK (Nov. 4, 2020 10:42 AM) available at <https://web.archive.org/web/20201104215620/https://www.facebook.com/256566055895/posts/10157402516245896>.

¹⁹⁶ *Id.*

¹⁹⁷ *Id.*

F. Efforts to Censor Other Influential Conservative Accounts

In addition to the accounts mentioned previously, the EIP targeted the social media accounts of conservative journalists, commentators, and personalities with large followings and high engagement for suppression. In the Jira ticket numbered EIP-805, the EIP flagged both posts in the screenshot below, one from Candace Owens and the other from Charlie Kirk.¹⁹⁸



The EIP also flagged posts from notable and popular conservative accounts, including those of Paul Sperry, Chanel Rion, Sean Davis, Dave Rubin, Michelle Malkin, James O’Keefe, Benny Johnson, Jack Posobiec, Tracy Beanz, Mike Roman, Sean Hannity, the Babylon Bee, Newsmax, Mollie Hemingway, and Tom Fitton, among others.

The suppression of conservative politicians and media resulting from this censorship operation deprived countless American voters from exposure to a range of perspectives on the most important political issues in the days and weeks surrounding a general election. Critically, the EIP conducted its censorship operation at the direction of, in collaboration with CISA, a federal government agency actively seeking to undermine free expression and the sitting President. The significance of these facts cannot be overstated.

¹⁹⁸ EIP-805, submitted by [REDACTED], ticket created (Nov. 4, 2020, 10:01 AM) (archived Jira ticket data produced to the Comm.); *see also* Candace Owens (@RealCandaceO) TWITTER (Nov. 4, 2020 8:52 AM) available at <https://web.archive.org/web/20201104165242/https://twitter.com/realcandaceo/status/1324031726096699392>.

IV. THE EIP'S COERCIVE TACTICS

In the lead-up to the 2020 election, social media platforms were inundated by requests for censorship from a number of federal agencies, including the FBI and CISA.¹⁹⁹ As documented in Section I of this interim report, CISA and its proxies already had two avenues to submit reports—switchboarding and the EI-ISAC—and was heavily lobbying a third avenue, a “misinformation reporting portal” operated by CIS, before the creation of EIP. Then, with the EIP, Jira ticket data and emails establish clearly that social media platforms understood that the federal government was working directly with the EIP.

In addition to having the explicit and implicit backing of the federal government, the EIP had another tool at its disposal to pressure social media companies to comply with the censorship requests: the media. In his testimony before the Committee, Alex Stamos—the SIO director and former Chief Security Officer at Facebook—explained how social media companies felt pressure from public criticism about the failure to remove content that experts had labeled as misinformation.²⁰⁰ He testified:

Q. And, with respect to the blogpost, are there any -- did anyone from EIP ever communicate to the platforms that you were going to make these blogposts public?

A. I mean, it's possible that we gave them a heads-up when we were posting about it.

Q. And why would you do that?

A. I think it's a polite thing to do so that they know that we're going public. We didn't want them to feel like we were blindsiding them.

Q. And what do you mean by “blindsiding” them?

A. We wanted them to know that there's going to be a possible discussion of what was going on in their platform, and they should know about it. I think the -- you know, we were -- I am sympathetic to how hard it is to be in one of these companies and to try to balance all the different equities. And so, if somebody was writing something that could generate a communications moment during an election period, then that's something I would want to know for sure.

¹⁹⁹ See *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. Jul. 4, 2023), ECF No. 293, at 2 (memorandum ruling granting preliminary injunction); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS, at 9–12 (Comm. Print June 26, 2023); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE FBI'S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH (Comm. Print July 10, 2023).

²⁰⁰ See House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 183-184 (on file with the Comm.).

Q. What do you mean by “communications moment”?

A. So, if we wrote a blogpost that said, “This is something viral that’s happening that’s not true,” you very well could find members of the media going out and then finding that content on five different platforms and then writing about it being up or not.

Q. And, if it was still up, would some of those media publications be criticism of the platforms?

A. It’s possible.²⁰¹

Similarly, Dr. Kate Starbird of the University of Washington, and one of the central figures involved in the EIP’s operation, similarly testified about using her platform (independent of the EIP) to publicly push social media platforms to change their policies. She testified:

Q. Was the purpose of the public communication to have Twitter change its policy?

A. It was, for me -- again, this is not, like, within the EIP brand. This is sort of something that we were just kind of doing that eventually we start working together. But this is just something that I do a lot, which is to put out analysis and have recommendations for the platforms at the end of that analysis.

Sometimes that’s in formal papers. In this case, I would sometimes put the analyses out on Twitter to say this is happening and that it’s a problem, to draw attention to it, and for them to think about what they should do to change. Yeah.

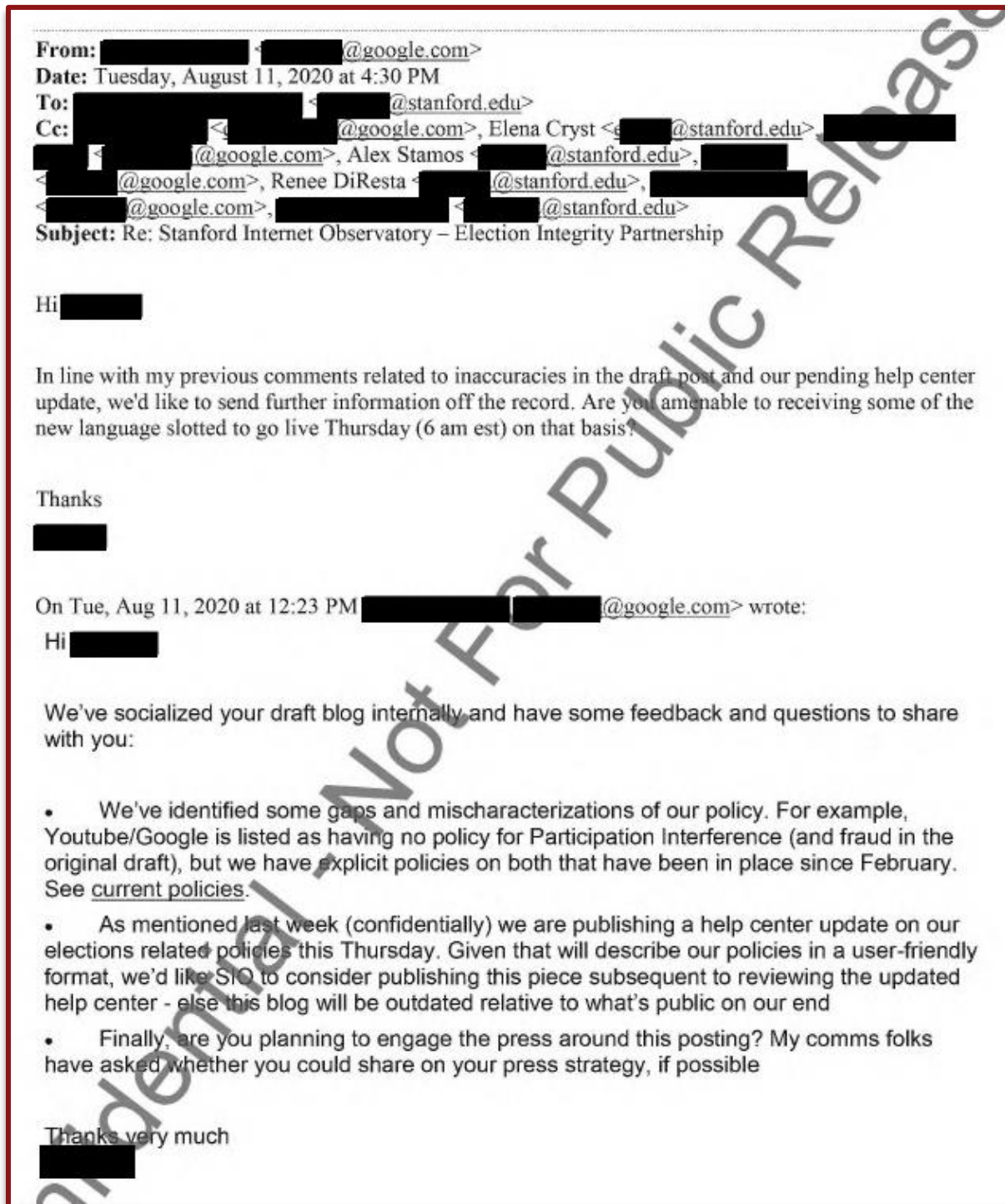
And I don’t always recommend -- I rarely recommend a specific action. I wish -- I didn’t get to say this -- I wish I had something better to say. But most of the time, I just point out problems and don’t tell them how to fix them. And I understand that the fixes for the problems are very tricky and very hard, so I give them credit for that. But I did a lot of, like, pointing out: This is a problem.²⁰²

In the fall of 2020, the EIP also worked on preparing work product summarizing the major social media platforms’ content moderation policies and the differences among them. The EIP initially gave Alphabet (the parent company of Google and YouTube) an opportunity to comment on YouTube’s content moderation policies. As the email chain below demonstrates, Alphabet was keenly aware that the EIP may “engage the press.” In particular, the company wanted to ensure that the EIP would not publish “inaccuracies” or “mischaracterizations” that

²⁰¹ *Id.*

²⁰² House Judiciary Committee’s Transcribed Interview of Kate Starbird (June 6, 2023), at 153 (on file with the Comm.).

would suggest the company's policies were insufficient in removing election-related content labeled as misinformation by the EIP.²⁰³



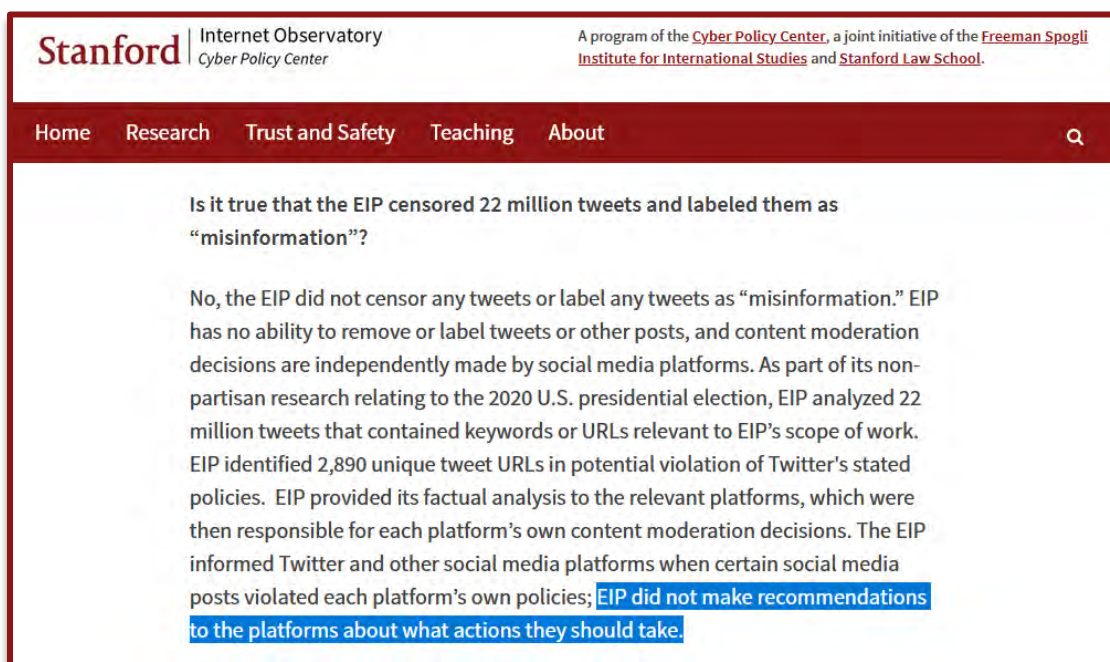
²⁰³ Email between Google Employees and Stanford Personnel (Aug. 11, 2020 4:30 PM) (on file with the Comm.).

V. STANFORD'S EFFORTS TO OBSTRUCT THE COMMITTEE'S INVESTIGATION

A. Stanford's Deceitful Public Statements about the EIP's Flagging of Posts

On March 17, 2023, following the Select Subcommittee's March 9 hearing on the Twitter Files, the SIO published a blog post titled "Background on the SIO's Project on Social Media," in which the SIO sought to downplay the extent of the EIP's censorship and surveillance, claiming that both the EIP and its successor, the Virality Project, "are non-partisan research coalitions that operate in an open, transparent, and public manner."²⁰⁴ On March 20, the SIO's counsel sent a link to the blog post to Committee staff, writing: "Here's the statement Stanford put up on Friday attempting to correct some of the myths floating around in the press."²⁰⁵

In addition to its mendacious framing of the EIP's activities and CISA's involvement therein, the post contains statements that are categorically untrue. Most notably, the SIO falsely claimed in the post that the "EIP informed Twitter and other social media platforms when certain social media posts violated each platform's own policies; *EIP did not make recommendations to the platforms about what actions they should take.*"²⁰⁶



Documents produced to the Committee and Select Subcommittee by both the SIO and other entities contain numerous examples of EIP analysts and staff making explicit recommendations to the platforms for specific enforcement measures. Appendix I compiles recommendations from 75 Jira tickets Stanford produced in which the EIP made a direct recommendation to platforms on what action should be taken.

²⁰⁴ *Background on the SIO's Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), <https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media>.

²⁰⁵ Email from John Bellinger to Committee Staff (March 20, 2023 5:09 PM). (on file with the Comm.).

²⁰⁶ *Background on the SIO's Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), <https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media> (emphasis added).

Below are a few examples to illustrate how explicitly the EIP instructed social media companies to take action:

Ticket #	Entry
EIP-345	“The article is being shared on Facebook, and while it has been labeled when shared in a group, official Page shares did not receive such a label . . . We recommend labeling all instances of the article being shared on Facebook.”
EIP-378	“This has circulated in pro-Trump conservative groups and sub-communities . . . We recommend that you all flag as false, or remove the posts below.”
EIP-396	“Hi Facebook, Reddit, and Twitter . . . we recommend it be removed from your platforms.”
EIP-407	“Hi Twitter team – please see the ticket above, which we’d recommend be labeled with information pertaining to mail-in voting.”
EIP-421	“We recommend that posts like these be labeled if they are alleging fraud, and that further action may be appropriate if this post actually documents fraud.”
EIP-460	“Huckabee has not said whether the tweet was a joke or not . . . We recommend that Twitter labels the post with (a) proper voting information.”
EIP-461	“Given the large audiences and Pennsylvania’s swing state status, we’d recommend this content be actioned.”
EIP-581	“We recommend you label or reduce the discoverability of the post.”
EIP-638	“We recommend labeling his [sic] tweets and monitoring if any of the tagged influencer accounts retweet him.”
EIP-656	“@SeanHannity is sharing a partial statement by Rep. Ilhan Omar . . . we recommend Twitter adds a label to Tweets sharing the link to the article.”
EIP-668	“We repeat our recommendation that this account be suspended for the duration of election day from posting additional misleading information about voting.”
EIP-673	“We recommend that this tweet, and other tweets sharing this false information, should be removed.”; “We recommend taking action specifically on this account, such as suspending their ability to continue tweeting for 12 hours.”
EIP-680	“We recommend that this tweet, as well as the tweets with the original video should be removed or labeled as misleading.”
EIP-1020	“[W]e recommend links to its content be labeled or removed.”

In EIP-421, the responsible EIP analyst appeared to make a remarkable admission about the EIP's true intentions, writing: "We recommend that posts like these be labeled if they are alleging fraud, and that further action may be appropriate *if this post actually documents fraud.*"²⁰⁷

B. Stanford's Initial Efforts to Unlawfully Misrepresent and Withhold Jira Data

Despite the fact that the EIP admitted in its own report that the Jira system facilitated communication between the EIP and the federal government, Stanford initially refused to provide the Committee and Select Subcommittee with the archival Jira data. Based on the representations from Stanford and other entities with knowledge of the EIP's data retention practices, the Committee understood that Stanford was the only entity with access to the Jira ticket data.²⁰⁸ Following a March 24, 2023, production which failed to adequately comply with the Committee's requests for the Jira data, the Committee issued a subpoena on April 12.²⁰⁹ On April 28, the date of the subpoena's deadline, Stanford produced a set of marginally responsive communications, but again did not produce the Jira tickets.²¹⁰

On May 4, Committee staff raised the issue of Jira tickets again during a phone call with counsel for Stanford, who agreed to consult with his client regarding the nature and retention of the Jira tickets.²¹¹ Remarkably, on May 15, Stanford's counsel confirmed to Committee staff in another phone call that the contents of the Jira tickets *were* responsive to the Committee's subpoena but that Stanford would nevertheless refuse to produce them.²¹² According to Stanford's counsel, the Jira tickets supposedly "concern[ed] only a research project conducted by Stanford students."²¹³ In light of Stanford's apparent unwillingness to comply in full with the subpoena, on June 1, 2023, the Committee sent a letter to Stanford raising the prospect of enforcing the subpoena, the deadline of which had long since passed.²¹⁴

²⁰⁷ See EIP-421, submitted by CIS Misinformation Reporting; ticket created (Oct. 21, 2020, 11:18 AM) (archived Jira ticket data produced to the Comm.) (emphasis added); see also McKenzie Sadeghi, *Fact Check: Mailing Ballots to Dead People Not Leading to Voter Fraud, Experts and Studies Say*, USA TODAY (July 15, 2020) available at <https://web.archive.org/web/20230714194915/https://www.usatoday.com/story/news/factcheck/2020/07/14/fact-check-mailing-ballots-dead-people-not-leading-voter-fraud/3214074001/>.

²⁰⁸ House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 108 (on file with the Comm.).

²⁰⁹ Letter to Alex Stamos, Dir., Stanford Internet Observatory, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Apr. 12, 2023).

²¹⁰ Email from Stanford's Counsel to Committee Staff (Apr. 29, 2023, at 12:00 AM).

²¹¹ Phone call between John Bellinger and Committee Staff (May 4, 2023).

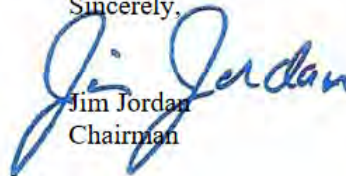
²¹² Phone call between John Bellinger and Committee Staff (May 15, 2023); see also Letter to John B. Bellinger, III, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 1, 2023), at 2.

²¹³ Letter to John B. Bellinger, III, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 1, 2023), at 2.

²¹⁴ *Id.*

The Committee's subpoena imposes legal obligations on SIO to comply and produce responsive materials. Thus, your client's refusal to produce documents responsive to the Committee's subpoena—four weeks after the subpoena return date—is highly concerning. Accordingly, the Committee expects the SIO will complete its production of responsive documents, in full, by no later than Wednesday, June 14, 2023, at 5:00 p.m. If Stanford fails to comply in full with the subpoena's demands, the Committee may be forced to consider the use of one or more enforcement mechanisms. Thank you for your client's attention to this matter.

Sincerely,



Jim Jordan
Chairman

It was only after the Chairman's letter that the SIO ultimately relented and began producing the Jira data.²¹⁵ All told, the Committee has received fifteen productions from the SIO, including six which contain the data for almost 400 EIP Jira tickets.²¹⁶

C. Numerous Documents Contradict Witness Testimony Regarding CISA's Involvement with the EIP

The Committee and Select Subcommittee have conducted transcribed interviews of several witnesses involved in the EIP who have claimed that CISA had little to no involvement in the EIP. This testimony is contradicted by the overwhelming amount of evidence obtained by the Committee and Select Subcommittee pursuant to several subpoenas issued to entities involved with the EIP. For example, Alex Stamos, the head of the EIP, claimed that CISA's role in the EIP was limited to introducing the EIP to the EI-ISAC:

Q. So, you have contacted CISA, CISA introduces you to EI-ISAC. And we are still in the summer of 2020, to the best of your recollection?

A. Okay.

Q. What roles did CISA play, if any, after that?

A. In the EIP they had no official role. They did not have the ability to report things directly to us. We would take things from EI-ISAC. I don't believe anything that EI-ISAC sent us came from CISA employees themselves. And they were not part of our day-to-day operations or our analysis. So, *they had very little role, if none, in EIP.*²¹⁷

²¹⁵ See Stanford Internet Observatory – Document Production Index (June 14, 2023) (on file with the Comm.).

²¹⁶ See App'x II.

²¹⁷ House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 95 (on file with the Comm.) (emphasis added).

But Dr. Kate Starbird of CIP—and one of the founding members of the EIP—recalled more involvement from CISA. She testified:

Q. Was it your understanding that some of the external partners were government agencies?

A. It was my understanding that there was one Federal Government agency and that there were other organizations that convened local and State election officials who we saw — who my understanding was is that we could help them and they could help us figure out what the ground truth was around election processes and procedures. And so that that would be an important part of a collaboration when you're trying to address that kind of misinformation.

Q. And which Federal agency was the one that you were referencing?

A. The Federal agency that -- is kind of who was -- is the CISA agency, yeah.²¹⁸

Regarding the creation of the EIP, former CISA Director Krebs testified that “EIP’s establishment was independent of CISA,” which is directly contradicted by documents from the summer of 2020 that the Atlantic Council, one of the members of the EIP, understood that the EIP was created “at the request of DHS/CISA.”²¹⁹

The testimony of Stamos and Krebs regarding the extent of CISA’s involvement in the creation and operation of EIP is contradicted by an overwhelming amount of evidence obtained by the Committee and Select Subcommittee, which makes abundantly clear that, not only was CISA directly involved the creation of the EIP, but it also took an active role in the EIP’s day-to-day operations, receiving a constant stream of tips and other information from both CISA and the CISA-funded CIS.

D. Stanford’s Continued Misrepresentations Regarding CISA, the EIP, and Jira

Unable to hide from its own report, counsel for Stanford initially admitted, in a June 14, 2023, letter to the Committee, that the GEC submitted tickets through the Jira system.²²⁰ However, Stanford’s counsel then claimed that “[a]side from this small number of GEC-initiated EIP tickets, SIO did not use Jira to receive information from, or share information with, any federal government agencies or officials about the [Virality Project] or EIP projects.”²²¹ Stanford’s counsel also claimed that “for EIP, SIO did not provide any government agency or employee of a government agency (whether federal, state, or local) access to the Jira database,

²¹⁸ House Judiciary Committee’s Transcribed Interview of Kate Starbird (June 6, 2023), at 77 (on file with the Comm.).

²¹⁹ Cf. House Judiciary Committee’s Transcribed Interview of Chris Krebs (Oct. 11, 2023), at 170 (on file with the Comm.); email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.).

²²⁰ Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023), at 4 (on file with the Comm.).

²²¹ *Id.*

and SIO only communicated using Jira with a single federal agency (the State Department) regarding the handful of tickets that GEC initiated.”²²²

Arnold & Porter

The Honorable Jim Jordan
June 14, 2023
Page 4

that Jira data. However, the statement in the Committee’s letter that the “government and large social media platforms initiated and received information” from Jira is not accurate.¹¹ Social media companies did not initiate any EIP or VP Jira tickets. Federal government agencies did not initiate any Jira tickets relating to the VP project. The State Department’s Global Engagement Center (GEC), which was established by Congress to counter foreign state disinformation and propaganda, initiated a very small number of tickets (fewer than 20) during the EIP 2020 project. These tickets concerned foreign propaganda and disinformation, primarily instigated by Russia. Aside from this small number of GEC-initiated EIP tickets, SIO did not use Jira to receive information from, or share information with, any federal government agencies or officials about the VP or EIP projects. Information from a small number of Jira tickets relating to the EIP project, and from an even smaller number of tickets relating to the VP project, was shared with social media companies. (As stated above, Stanford is producing Jira ticket data that was received from the GEC or exchanged with social media companies.) As Stanford’s counsel has explained in several telephone conversations with your staff, the vast majority of Jira tickets were generated by students and supervising researchers, and it is Stanford’s understanding that the tickets were never accessed or viewed by individuals or entities other than the researchers and non-governmental institutions participating in EIP and VP.

More specifically, for EIP, SIO did not provide any government agency or employee of a government agency (whether federal, state, or local) access to the Jira database, and SIO only communicated using Jira with a single federal agency (the State Department) regarding the handful of tickets that GEC initiated. As noted above, social media companies did not initiate any Jira tickets. The non-governmental, non-profit Center

²²² *Id.*

These statements are inaccurate. In addition to the fact that CISA personnel referenced the “EIP-” codes when switchboarding, the Committee has obtained records of communications proving that CISA personnel were receiving information from or generated by the Jira system. For example, the email notification below, which was generated by the Jira system, indicates that the ticket “EIP-833” was “shared with . . . CISA CFITF.”²²³

From: Elena Cryst <jira@2020partnership.atlassian.net>
 Sent: Wednesday, November 4, 2020 5:41 PM
 To: ██████████ <██████████@fb.com>
 Subject: EIP-833 Case #CIS-MIS000164: inaccurate number of rejected absentee ballots in DeKalb County, GA

Reply above this line.

Elena Cryst shared this with your organization.

View the request and select Get notifications to follow along.

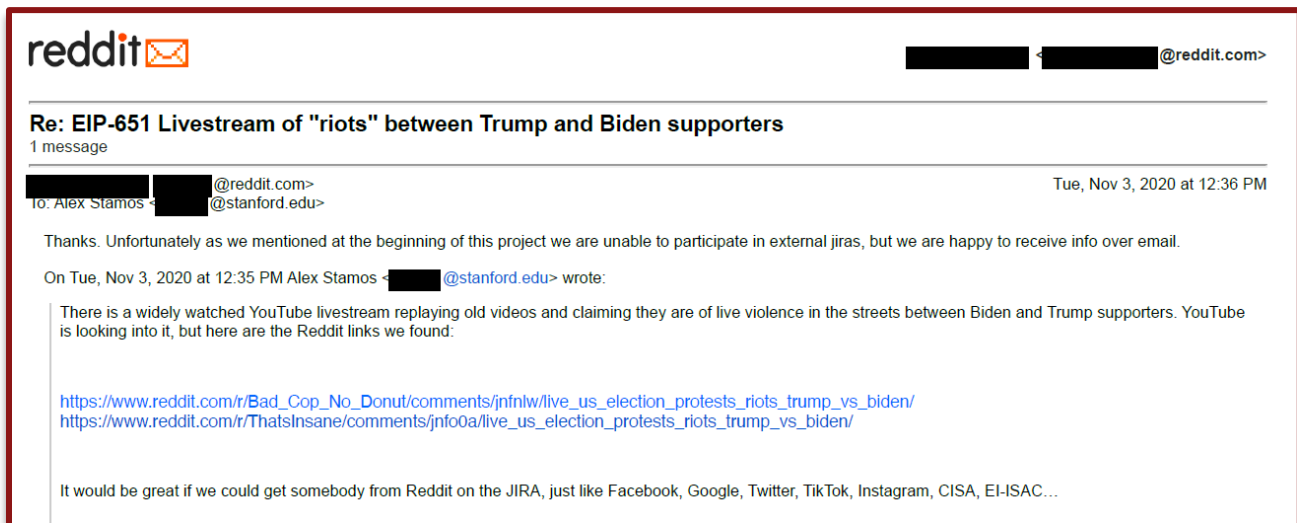
View request<<https://2020partnership.atlassian.net/.../c.../portal/5/EIP-833...>> · Turn off this request's notifications<<https://2020partnership.atlassian.net/.../EIP-833/unsubscribe...>>

This is shared with TikTok, Facebook, EHSAC, Twitter, CIS Misinformation Reporting, and CISA CFITF.

Powered by Jira Service Desk<<https://www.atlassian.com/softwa.../.../service-desk/powered-by...>>

²²³ Email from Elena Cryst to Facebook employee (Nov. 4, 2020, 5:41 PM) (on file with the Comm.); *see also* EIP-833, submitted by CIS Misinformation Reporting, ticket created (Nov. 4, 2020, 1:28 PM) (archived Jira ticket data produced to the Comm.); Tom Clark (@tom_s_clark) TWITTER (Nov. 4, 2020 12:03 PM) available at https://web.archive.org/web/20201104221417/https://twitter.com/tom_s_clark/status/1324079751640862727; Daniel Dale (@ddale8) TWITTER (Nov. 4, 2020 1:30 PM) available at <https://web.archive.org/web/20201105010400/https://twitter.com/ddale8/status/1324101773322276864>.

An email exchange from November 3, 2023 between Alex Stamos and Reddit further suggests that CISA had some form of access to the Jira system. In the email, Stamos attempted to pressure Reddit to join the EIP's Jira system, writing: "It would be great if we could get somebody from Reddit on JIRA, just like Facebook, Google, Twitter, TikTok, Instagram, CISA, EI-ISAC..."²²⁴ The Reddit employee responded: "Thanks. Unfortunately as we mentioned at the beginning of this project we are unable to participate in external jiras, but we are happy to receive info over email."²²⁵



When confronted with this discrepancy during his transcribed interview, Stamos claimed that he "was probably making a mistake there talking about CISA because EI-ISAC were the people who had access to the Jira," despite the fact that he independently listed both CISA and the EI-ISAC in the email.²²⁶

The Jira data produced to the Committee and Select Subcommittee contains a number of cells in which "CISA" is mentioned, including in contexts that prove close coordination between CISA and the EIP. For example, EIP-315 contains an entry which reads, "EIP – this information was posted on an app that is not a primary social media platform. CISA is looking into how to handle this type of reporting."²²⁷

On July 27, 2023, more than a month after Stamos's interview, Stanford's counsel finally admitted in a letter to the Committee that CISA was, in fact, involved with the EIP's Jira system and that CISA had been directly "tagged" on a number of tickets.²²⁸ Stanford's counsel claimed

²²⁴ Email from Alex Stamos to Reddit employee (Nov. 3, 2020 12:35 PM) (on file with the Comm.) (emphasis added).

²²⁵ Email from Reddit employee to Alex Stamos (Nov. 3, 2020 12:36 PM) (on file with the Comm.).

²²⁶ Cf. House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 218 (on file with the Comm.); email from Alex Stamos to Reddit employee (Nov. 3, 2020, 12:35 PM) (on file with the Comm.).

²²⁷ See EIP-315, submitted by CIS Misinformation Reporting, ticket created (Oct. 5, 2020, 4:19 PM) (archived Jira ticket data produced to the Comm.).

²²⁸ See Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. On the Judiciary (July 27, 2023), at 1 n.1.

in the letter that “At the time of Mr. Stamos’s interview, Mr. Stamos was not aware that CISA or CFITF had been ‘tagged’ in any Jira tickets.”²²⁹

¹ Following Alex Stamos’s June 23 interview with Committee Staff and the Committee’s questions with respect to Stamos Ex. 16, Stanford has reviewed whether any federal government entity other than the Department of State’s Global Engagement Center (GEC) initiated or was “tagged” in any Jira tickets. Stanford has since determined that the Cybersecurity and Infrastructure Security Agency (CISA) Countering Foreign Influence Task Force (CFITF) was “tagged” in a small number of Jira tickets. Based on the information currently available to Stanford, it appears that for a short period of time, some EIP researchers utilized this “tag,” rather than or in addition to the “EI-ISAC” tag, to flag the Jira tickets potentially needing input or review by the relevant state and local election officials. Stanford has identified 14 Jira tickets with a CISA CFITF “tag,” specifically: EIP-236, EIP -239, EIP-243, EIP-563, EIP-570, EIP-616, EIP-664, EIP-686, EIP-695, EIP-713, EIP-743, EIP-810, EIP-833, and EIP-1009. At the time of Mr. Stamos’s interview, Mr. Stamos was not aware that CISA or CFITF had been “tagged” in any Jira tickets.

Arnold & Porter Kaye Scholer LLP

601 Massachusetts Ave, NW | Washington, DC 20001-3743 | www.arnoldporter.com

This is an especially dubious assertion, given that EIP-664, EIP-686, EIP-695—tickets which the SIO admitted were shared with CISA—were assigned to Stamos, according to the Jira data produced to the Committee and Select Subcommittee.²³⁰

²²⁹ *Id.*

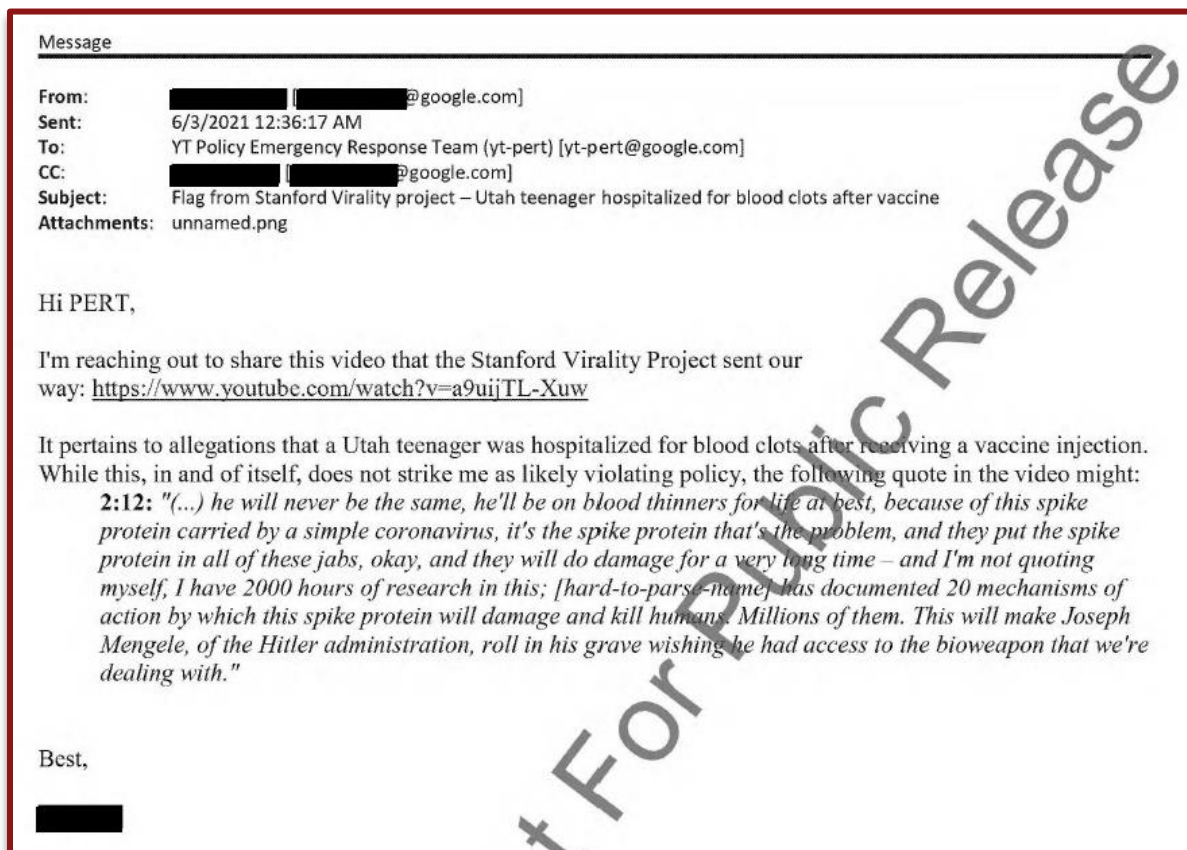
²³⁰ See EIP-664, submitted by Mike Caulfield, ticket created (Nov. 3, 2020, 11:26 AM) (archived Jira ticket data produced to the Comm.); EIP-686, submitted by CIS Misinformation Reporting, ticket created (Nov. 3, 2020, 12:58 PM) (archived Jira ticket data produced to the Comm.); EIP-695, submitted by CIS Misinformation Reporting, ticket created (Nov. 3, 2020, 1:34 PM) (archived Jira ticket data produced to the Comm.).

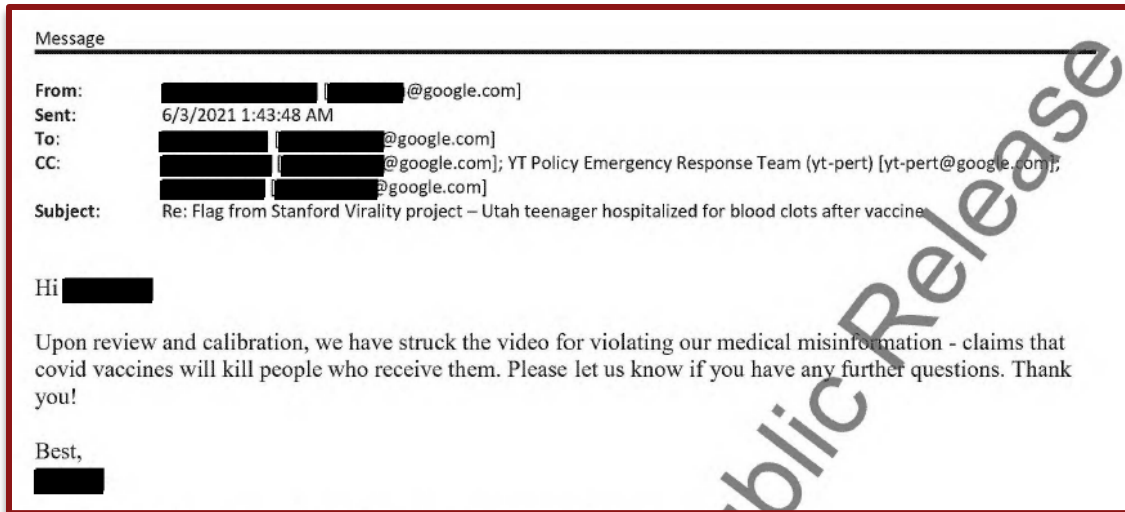
EPILOGUE

It is no surprise that Stanford University attempted to refuse to turn over documents responsive to the Committee's subpoena: they reveal that the EIP was not a non-partisan "school project" comprised of students and researchers interested in combatting misinformation online. Instead, from start to finish, the EIP operation worked directly with the federal government and disproportionately targeted conservative-oriented speech.

After the 2020 election, what others have deemed the "censorship industrial complex," played out as expected. After President Trump fired CISA Director Chris Krebs in November 2020, Mr. Krebs created the Krebs Stamos Group with Alex Stamos, the head of the EIP and the SIO, in January 2021. Matt Masterson left CISA at the end of 2020 and took a position as a non-research fellow with Stanford, working with the SIO and its Virality Project.

With the election over and the American people questioning the wisdom of lockdowns and the safety of the COVID-19 vaccines, the EIP reconstituted itself as the Virality Project. Again working with the federal government, the SIO launched the Virality Project as a "a global study aimed at understanding the disinformation dynamics specific to the COVID-19 crisis." The Virality Project again used Jira tickets. Though Stanford was less explicit and specific in its recommendations for censorship as it was under the EIP model, social media platforms still dutifully removed content flagged by Stanford:





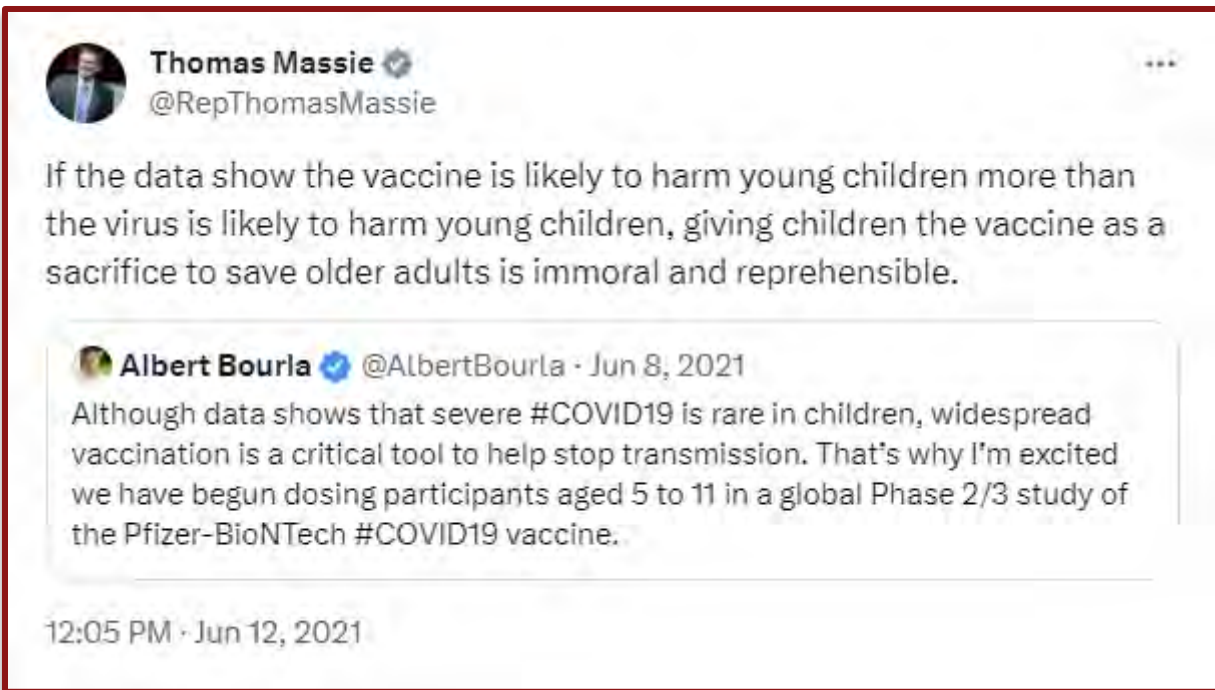
Like the EIP, Stanford’s Virality Project continued to flag content directly to social media platforms, including *true* content by elected officials, such as the tweet below by Congressman Thomas Massie.²³¹ In reference to this tweet, the Virality Project ticket stated, “Dear Facebook and Twitter teams, Please note this Israeli narrative claiming that Covid-19 immunity is equivalent to vaccination immunity, with the following URLs:” before flagging Congressman Massie’s tweet among other Facebook and Twitter links.²³²



²³¹ VP-899, submitted by [REDACTED], ticket created (May 21, 2021, 9:49 AM) (archived Jira ticket data produced to the Comm.); *see also* Rep. Thomas Massie (@RepThomasMassie), TWITTER (May 19, 2021, 5:35 PM), <https://twitter.com/RepThomasMassie/status/1395130940343607297>.

²³² *Id.*

The Virality Project later flagged this tweet by Congressman Massie as well.²³³



After President Biden was inaugurated in January 2021, the government’s censorship regime ramped up. At CISA, the CFITF team dropped any pretense of a “foreign”-focus and relabeled itself as the “MDM team” that would focus on foreign *and domestic* speech that the government considered mis-, dis-, or malinformation.²³⁴ Throughout 2021, the Biden White House engaged in a pressure campaign against Facebook and other social media companies to censor anti-vaccine content, even if it was true.²³⁵ By 2022, CISA invited Dr. Starbird, then-Twitter Executive Vijaya Gadde, and others to form an advisory MDM Subcommittee to consult with CISA about how the agency could and should combat Americans’ speech that the government considered to be mis-, dis-, or malinformation.²³⁶ DHS created, and then disbanded after public outcry, the short-lived Disinformation Governance Board.²³⁷

²³³ VP-1018, submitted by [REDACTED], ticket created (June 18, 2021, 9:58 AM) (archived Jira ticket data produced to the Comm.); *see also* Rep. Thomas Massie (@RepThomasMassie), TWITTER (June 12, 2021), <https://twitter.com/RepThomasMassie/status/1403745403665850372>.

²³⁴ *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

²³⁵ Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023); Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 27, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684595375875760128; Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 28, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684957660515328001; Rep. Jim Jordan (@Jim_Jordan), TWITTER (Aug. 3, 2023, 11:00 AM), https://twitter.com/Jim_Jordan/status/1687116316073930752; Rep. Jim Jordan (@Jim_Jordan), TWITTER (Sept. 5, 2023, 6:17 PM), https://twitter.com/Jim_Jordan/status/1699184930331267539.

²³⁶ *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

²³⁷ *Id.*; Ronn Blitzer, *Biden Administration 'Disinformation' Board on Pause Amid Free Speech Concerns: Reports*, FOX NEWS (May 18, 2022).

But by 2023, as Republicans retook the majority in the House of Representatives and initiated oversight of the censorship-industrial complex, CISA scrubbed its website of references to domestic censorship.²³⁸ The Committee and Select Subcommittee obtained and revealed how Facebook changed its policies because of pressure from the Biden Administration.²³⁹ Internal Facebook documents showed that the Biden White House in particular wanted true information and satire censored at a rate even Big Tech found objectionable.²⁴⁰ Based on the Committee's and Select Subcommittee's work, even the mainstream media could no longer ignore these constitutional violations.²⁴¹ The plaintiffs in *Missouri v. Biden* have obtained significant victories before a federal district court and the U.S. Court of Appeals for the Fifth Circuit, and now will have their case heard by the Supreme Court. Public reporting shows that universities are reconsidering whether to permit their professors to receive funding and engage in censorship work.²⁴²

But the work is not done yet. The Committee and Select Subcommittee's investigation remains ongoing. To better inform legislative efforts to end government censorship and protect Americans' rights guaranteed by the First Amendment, the Committee and Select Subcommittee will continue to investigate the extent of CISA's and other Executive Branch agencies' interactions with social media platforms and third parties, including those used to facilitate censorship by proxy.

²³⁸ See STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

²³⁹ Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 27, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684595375875760128.

²⁴⁰ *Id.*

²⁴¹ See, e.g., Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

²⁴² Naomi Nix et. al, *Misinformation Research Is Buckling Under GOP Legal Attacks*, WASH. POST, (Sept. 23, 2023).

APPENDIX I

The House Judiciary Committee and its Select Subcommittee on the Weaponization of the Federal Government have obtained documents and information from Stanford University, pursuant to a subpoena, which reveal that EIP analysts and staff made explicit recommendations to social media platforms for specific enforcement measures on at least 75 occasions in just a four-month span in the lead-up to and during the 2020 election. This appendix compiles those 75 recommendations in order of their EIP Jira ticket number. The entire Jira ticket, including comments from social media platforms, can be found by cross-referencing the archived Jira ticket data provided in Appendix II.

Ticket #	Entry
EIP-166	“Hello Google, . . . We recommend this ad be removed.”
EIP-279	“We recommend Twitter label or remove this tweet.”
EIP-307	“We recommend that the following platforms take these actions: *Twitter* - Disable account.”
EIP-321	“Recommended actions: Ban sharing links to the following sites:”
EIP-329	“We are reporting two instances of electoral disinformation constituting participation interference and delegitimization. We flag a post and an account to you all at Twitter, and recommend the following:”
EIP-330	“We recommend that Twitter and Facebook remove these posts. If you are not able to remove these posts, we suggest that they be labeled as misleading.”
EIP-345	“The article is being shared on Facebook, and while it has been labeled when shared in a group, official Page shares did not receive such a label . . . We recommend labeling all instances of the article being shared on Facebook.”
EIP-348	“Recommend labeling.”
EIP-378	“This has circulated in pro-Trump conservative groups and sub-communities . . . We recommend that you all flag as false, or remove the posts below.”
EIP-389	“We also recommend expanded enforcement efforts on election misinformation on content in non-English languages.”
EIP-396	“Hi Facebook, Reddit, and Twitter . . . we recommend it be removed from your platforms.”

EIP-397	“Hi, Facebook, here are two posts alleging problems with voting machines, we recommend labeling:”
EIP-402	“Twitter and Reddit, we are passing along the full links we found for your visibility, and recommend you label them with voting information.”
EIP-407	“Hi Twitter team – please see the ticket above, which we’d recommend be labeled with information pertaining to mail-in voting.”
EIP-417	“This video narration claims to show evidence of voter fraud in Maryland, but the video itself (footage of an election worker) does not show anything that we interpret as voter fraud. We recommend that this video be removed or labeled.”
EIP-421	“We recommend that posts like these be labeled if they are alleging fraud, and that further action may be appropriate if this post actually documents fraud.”
EIP-450	“At minimum, we recommend that the posts be labeled with labels clarifying that vote by mail is secure.”
EIP-451	“We recommend taking the same action on the new ad.”
EIP-455	“+*Platform Recommendations*+ +*Twitter*+, where narrative is receiving the most interactions, to flag the video and hashtag and continue to monitor for possible poll watcher/intimidation narratives.”
EIP-460	“Huckabee has not said whether the tweet was a joke or not . . . We recommend that Twitter labels the post with (a) proper voting information.”
EIP-461	“Hi Twitter team – there are a number of high-profile individuals, including the President, making accusations of voter fraud . . . Given the large audiences and Pennsylvania’s swing state status, we’d recommend this content be actioned.”
EIP-479	“We recommend labeling accordingly.”
EIP-483	“We recommend twitter remove the tweet as it is a fairly clear violation.”
EIP-489	“We recommend to Twitter that the tweets be removed.”
EIP-503	“We recommend removing the following tweets as misleading.”
EIP-511	“We recommend labeling this content and monitoring for Chinese-language keywords like election fraud and QAnon terms for action on future content.”

EIP-512	“We recommend that Twitter remove this tweet.”; “We recommend these tweets be taken down.”; “I recommend that Twitter and Facebook remove these posts or add a strong label.”
EIP-537	“Hello Youtube, Facebook teams: We are adding you to this ticket as the videos in questions contain several misleading claims about mail-in ballots as well as in-person voting. We recommend a specific label be applied to these posts.”
EIP-559	“We recommend removing or labeling this tweet.”; “As this is clearly false information about the election we recommend removal by Twitter.”
EIP-575	“We recommend Twitter actions the account for election delegitimization.”
EIP-581	“We recommend you label or reduce the discoverability of the post.”
EIP-585	“We recommend removing the linked Tweet.”; “Recommend also removing the linked Quote Tweets.”
EIP-589	“As it is a false claim that undermines trust in the electoral process we recommend its removal.”
EIP-608	“Recommend labeling.”
EIP-614	“We recommend at least labeling as this is a disproven claim of an electoral crime.”
EIP-615	“We recommend removing these posts and will update you with any more.”
EIP-638	“We recommend labeling his [sic] tweets and monitoring if any of the tagged influencer accounts retweet him.”
EIP-639	“We recommend removing or labeling these tweets.”
EIP-656	“@SeanHannity is sharing a partial statement by Rep. Ilhan Omar . . . we recommend Twitter adds a label to Tweets sharing the link to the article.”
EIP-664	“Twitter, recommend removing:”
EIP-668	“We repeat our recommendation that this account be suspended for the duration of election day from posting additional misleading information about voting.”

EIP-673	“We recommend that this tweet, and other tweets sharing this false information, should be removed.”; “We recommend taking action specifically on this account, such as suspending their ability to continue tweeting for 12 hours.”
EIP-680	“We recommend that this tweet, as well as the tweets with the original video should be removed or labeled as misleading.”
EIP-698	“Recommend removal for some, labeling for other Tweets.”
EIP-705	“We recommend that this tweet be removed or flagged for misleading content.”
EIP-706	“As the accounts are making a baseless claim that undermines trust in the electoral process we recommend the accounts be actioned.”
EIP-715	“This account in the above tweet is attempting to delegitimize the voting process without evidence. We recommend it be actioned.”
EIP-746	“We recommend removing this content.”
EIP-767	“We recommend Twitter remove the posts.”
EIP-779	“We recommend that posts sharing links to this story and posts sharing screenshots of this story be removed. If they cannot be removed, a banner explaining that they are sharing false or misleading content should be added.”
EIP-780	“We know you are aware of the #stopthesteal push but we have gathered here some of the major contributors . . . We recommend actioning these quickly.”
EIP-789	“These posts are growing rapidly, and we recommend that they be removed, because they undermine people’s faith in the legitimacy of the election result.”
EIP-790	“They share this video to suggest that Biden is engaging in voter fraud, but this is misleading . . . Facebook has put a warning banner on similar posts (see linked post), and we suggest that Twitter either remove these posts or do the same.”
EIP-795	“We recommend that these posts be removed immediately.”
EIP-798	“We recommend that the tweet be removed, or at least covered with a misleading/disputed content banner. It falsely undermines people’s faith in the legitimacy of the election results.”
EIP-811	“Users on Twitter and Facebook are sharing manipulated images of people moving boxes in trucks labeled ‘Emergency Democrat Votes.’ We suggest labeling or removing tweets that use this photo, as it could undermine people’s faith in the legitimacy of the election process.”

EIP-817	“As it is a claim without evidence that undermines trust in the election we recommend it be actioned.”
EIP-847	“We recommend labeling (as some have already been) or removing these tweets.”
EIP-853	“Recommend labels or removal.”
EIP-867	“We recommend that these claims be labeled as unsubstantiated.”
EIP-868	“We strongly recommend that platforms take action on this content and any further content with this screenshot. These posts should be removed or labeled appropriately.”
EIP-869	“We recommend at least labeling as this is a disproven claim of an election crime.”
EIP-879	“We recommend that this content be removed or labeled.”
EIP-890	“We recommend flagging (or removing) posts that make this claim:”
EIP-909	“We recommend removal.”
EIP-920	“Recommend you limit spread of attached tweets.”
EIP-949	“We have completed this analysis of the attached Breitbart article and recommend that any links to it be labeled or removed per policy.”; “recommend applying the same label to other/new instances of the narrative.”
EIP-952	“We recommend it be actioned with fact-check labeling.”
EIP-969	“Facebook: please see this misleading Instagram story . . . Recommend labeling or other action, as it has already made its way to Twitter.”
EIP-970	“Facebook and Twitter: this story from alleged Nevada ‘whistleblower’ claiming voting irregularities has not been verified or substantiated. It has received significant viral amplification. We recommend these links be labeled.”
EIP-987	“We are working on a thread but recommend that Twitter/Facebook delete (or at least label) the videos.”

EIP-989	“We recommend it be removed as violative of terms of service.”
EIP-996	“We recommend removing or labeling this content as appropriate.”
EIP-998	“We recommend that they be flagged for labeling or removal.”
EIP-1020	“we recommend links to its content be labeled or removed.”

APPENDIX II

Appendix II is the EIP and Virality Project Jira ticket data provided to the Committee and Select Subcommittee. If the Department of Homeland Security, among others, had the ability to see what American speech was being targeted and censored, so too should the American people.



**THE WEAPONIZATION OF CISA:
HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH
AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



June 26, 2023

EXECUTIVE SUMMARY

“One could argue we’re in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important.”

– CISA Director Jen Easterly, November 10, 2021.¹

The First Amendment recognizes that no person or entity has a monopoly on the truth, and that the “truth” of today can quickly become the “misinformation” of tomorrow. Labeling speech “misinformation” or “disinformation” does not strip it of its First Amendment protection. As such, under the Constitution, the federal government is strictly prohibited from censoring Americans’ political speech. The government also may not use third parties to bypass the First Amendment and conduct censorship by proxy.²

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been conducting an investigation into government-induced censorship on social media. Although the investigation is ongoing, information obtained to date has revealed that the Cybersecurity and Infrastructure Security Agency (CISA)—an upstart agency within the Department of Homeland Security (DHS)—has facilitated the censorship of Americans directly and through third-party intermediaries.

Founded in 2018, CISA was originally intended to be an ancillary agency designed to protect “critical infrastructure” and guard against cybersecurity threats.³ In the years since its creation, however, CISA metastasized into the nerve center of the federal government’s domestic surveillance and censorship operations on social media.⁴ By 2020, CISA routinely reported social media posts that allegedly spread “disinformation” to social media platforms.⁵ By 2021, CISA had a formal “Mis-, Dis-, and Malinformation” (MDM) team.⁶ In 2022 and 2023, in response to growing public and private criticism of CISA’s unconstitutional behavior, CISA attempted to camouflage its activities, duplicitously claiming it serves a purely “informational” role.⁷

This interim staff report details, among other things, that:

¹ Maggie Miller, *Cyber agency beefing up disinformation, misinformation team*, THE HILL (Nov. 10, 2021).

² See *Norwood v. Harrison*, 413 U.S. 455, 465 (1973) (“It is also axiomatic that a state may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish.”).

³ See 6 U.S. Code § 652; *Federal Government*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/audiences/federal-government> (last visited Jun. 23, 2023).

⁴ See Ken Klippenstein and Lee Fang, *Truth Cops: Leaked Documents Outline DHS’s Plans to Police Disinformation*, THE INTERCEPT (Oct. 31, 2022).

⁵ Scully Dep. 16:16–17:8, *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 209.

⁶ *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, DEP’T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., at 7 (Aug. 10, 2022), <https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf>.

⁷ See, e.g., Scully Dep. 17:9–14, *supra* note 5.

- CISA is “working with federal partners to mature a whole-of-government approach” to curbing alleged misinformation and disinformation.⁸
- CISA considered the creation of an anti-misinformation “rapid response team” capable of physically deploying across the United States.⁹
- CISA moved its censorship operation to a CISA-funded non-profit after CISA and the Biden Administration were sued in federal court, implicitly admitting that its censorship activities are unconstitutional.¹⁰
- CISA wanted to use the same CISA-funded non-profit as its mouthpiece to “avoid the appearance of government propaganda.”¹¹
- Members of CISA’s advisory committee agonized that it was “only a matter of time before someone realizes we exist and starts asking about our work.”¹²

The Committee and the Select Subcommittee are responsible for investigating “violation[s] of the civil liberties of citizens of the United States.”¹³ In accordance with this mandate, this interim staff report on CISA’s violations of the First Amendment and other unconstitutional activities fulfills the obligation to identify and report on the weaponization of the federal government against American citizens. The work, however, is not done. CISA still has not adequately complied with a subpoena for relevant documents, and much more fact-finding is necessary. In order to better inform the Committee’s legislative efforts, the Committee and Select Subcommittee will continue to investigate CISA’s and other Executive Branch agencies’ entanglement with social media platforms.

⁸ CISA CYBERSECURITY ADVISORY COMM., SUBCOMMITTEE OVERVIEW & UPDATE: PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION, at 1 (2022) (on file with the Comm.).

⁹ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JUNE 14, 2022, at 2 (on file with the Comm.).

¹⁰ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JULY 26, 2022, at 1 (on file with the Comm.).

¹¹ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING APRIL 12, 2022, at 2 (on file with the Comm.).

¹² E-mail from Suzanne Spaulding to Kate Starbird (May 20, 2022, 7:27 AM) (on file with the Comm.).

¹³ H. Res. 12 § 1(b)(E).

TABLE OF CONTENTS

Executive Summary	1
Table of Contents	3
Background	4
CISA’s Mission Creep into Surveillance, Censorship, and Cover-ups	9
I. CISA has transformed into a domestic intelligence and speech-police agency, far exceeding its statutory authority	9
A. Switchboarding: CISA’s coordination with Big Tech to censor Americans	12
B. CISA’s MDM consultants rejected constitutional “limitations” on the surveillance and censorship of domestic speech	12
C. CISA considered creating an anti-MDM “rapid response team” to physically deploy across the United States.	14
D. MDM “experts” wanted CISA to crack down on <i>factual</i> information	15
E. CISA is only one part of a “whole-of-government approach” to MDM	16
F. State election officials warned CISA to “remain within [its] operational and mission limits,” lest it should earn the public’s “distrust.”	17
G. DHS was eager to cement CISA as a domestic intelligence agency	18
H. Social media companies mocked CISA’s MDM team and DHS’s Disinformation Governance Board	19
I. CSAC members were concerned about the MDM Subcommittee	20
II. CISA colludes with third parties to circumvent the First Amendment and conduct censorship by proxy	21
A. CISA’s external censorship arm: the EI-ISAC	22
B. State and local election officials used the EI-ISAC in an effort to silence critics and political opponents	23
C. CISA admitted to outsourcing its surveillance operation to third parties	26
III. CISA has attempted to conceal its unconstitutional activities and remove evidence of wrongdoing	28
A. Fearing public pressure and legal risks, CISA outsourced its censorship operation to the EI-ISAC	28
B. The MDM Subcommittee tried to disguise its recommendations by removing references to surveillance and censorship	29
C. CISA’s MDM advisors fretted that it was “only a matter of time before someone realizes we exist and starts asking about our work.”	30
D. CISA purged its website of references to domestic MDM and its First Amendment violations in response to public pressure	32
E. The Biden Justice Department interfered with records requests in order to shield CISA from public scrutiny of its unconstitutional practices	34
Conclusion	36

BACKGROUND

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been conducting oversight of the federal government’s work with non-government entities to censor speech online. The Select Subcommittee has also convened two hearings on the subject of social media censorship¹⁴ and published an interim staff report exposing the Federal Trade Commission’s (FTC) politically motivated harassment campaign against Elon Musk’s Twitter.¹⁵

The First Amendment to the United States Constitution rests on the principle that no person or institution, including the government, has a monopoly on the truth, and that viewpoint-based suppression of speech by the government is dangerous and may even spell the death of a constitutional republic.¹⁶ Under the First Amendment, the “government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.”¹⁷ As the Supreme Court has explained: “If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion.”¹⁸

Labeling speech “misinformation” does not strip it of First Amendment protection. That is so even if the speech is untrue, as “[s]ome false statements are inevitable if there is to be an open and vigorous expression of views in public and private conversation.”¹⁹ In refusing to carve out a First Amendment exception for “false” speech, the Framers of our Constitution recognized the significant danger in making the government the ultimate arbiter of truth.²⁰ The First Amendment also protects the right to receive information, “an inherent corollary of the rights to free speech and press that are explicitly guaranteed by the Constitution” because “the right to receive ideas follows ineluctably from the *sender’s* First Amendment right to send them.”²¹

It is “axiomatic,” in the words of the Supreme Court, that the government may not “induce, encourage, or promote private persons to accomplish what it is constitutionally forbidden to accomplish.”²² Moreover, the First Amendment prohibits the government from

¹⁴ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 9, 2023); *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 30, 2023).

¹⁵ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION: AN AGENCY’S OVERREACH TO HARASS ELON MUSK’S TWITTER* (Comm. Print 2023).

¹⁶ *See Wood v. Georgia*, 370 U.S. 375, 388 (1962) (“Those who won our independence had confidence in the power of free and fearless reasoning and communication of ideas to discover and spread political truth.”).

¹⁷ *Ashcroft v. ACLU*, 535 U.S. 564, 573 (2002).

¹⁸ *W.Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943).

¹⁹ *United States v. Alvarez*, 567 U.S. 709, 718 (2012) (plurality opinion).

²⁰ *See id.* at 752 (Alito, J., dissenting) (“Even where there is a wide scholarly consensus concerning a particular matter, the truth is served by allowing that consensus to be challenged without fear of reprisal. Today’s accepted wisdom sometimes turns out to be mistaken.”).

²¹ *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982).

²² *Norwood v. Harrison*, 413 U.S. 455, 465 (1973).

“abridging the freedom of speech”²³—not “negating” or “abrogating,” but merely “abridging.” Thus, any law or administrative policy that impedes the ability of users to speak freely on privately owned social media platforms violates the First Amendment.²⁴

This interim report focuses primarily on the censorship efforts of the Cybersecurity and Infrastructure Security Agency (CISA), a component of the Department of Homeland Security (DHS), and its role in what one journalist and commentator has called the “censorship industrial complex.”²⁵

The Cybersecurity and Infrastructure Security Agency

Congress established CISA in 2018, redesignating the National Protection and Programs Directorate (NPPD) within DHS as CISA.²⁶ CISA’s statutory mission included “lead[ing] cybersecurity and critical infrastructure security programs, operations, and associated policy,” and “carry[ing] out the requirements of the Chemical Facility Anti-Terrorism Standards Program.”²⁷ In April 2019, Daniel Sutherland, CISA’s Chief Counsel, claimed: “We are a non-regulatory, non-law enforcement, non-intelligence community” agency.²⁸



As defined in 2003 by Homeland Security Presidential Directive 7, the term “critical infrastructure” was formerly used to describe “information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping.”²⁹ It was not until 2017, shortly after the 2016 election, that President Obama’s DHS Secretary Jeh Johnson designated “election infrastructure” as a “critical infrastructure subsector.”³⁰

Ostensibly created to protect the electrical grid and other “critical infrastructure” sectors from cybersecurity threats,³¹ CISA, a little-known agency buried in the depths of DHS, soon expanded its mission to combat “foreign disinformation.”³² Not long thereafter, under the pretext of protecting “election infrastructure,” CISA began surveilling and censoring American citizens online, directly and by proxy.

²³ U.S. CONST. amend. I (emphasis added).

²⁴ See Philip Hamburger, *How the Government Justifies Its Social-Media Censorship*, WALL STREET JOURNAL (Jun. 9, 2023).

²⁵ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. at 6 (Mar. 9, 2023) (statement of Michael Shellenberger).

²⁶ 6 U.S. Code § 652.

²⁷ *Id.*

²⁸ *CISA and Cyber Threats: How Government and Private Sector Secure Our Networks and Infrastructure*, THE FEDERALIST SOC’Y (Jun. 11, 2019).

²⁹ Homeland Sec. Presidential Directive 7, 2. Pub. Papers 1739 (Dec. 17, 2003).

³⁰ Press Release, Dep’t of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017).

³¹ 6 U.S. Code § 652.

³² See, e.g., CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, #PROTECT2020 STRATEGIC PLAN, at 20 (2020), https://www.cisa.gov/sites/default/files/publications/ESI_Strategic_Plan_FINAL_2-7-20_508.pdf.

CISA’s Cybersecurity Advisory Committee (CSAC)

DHS created the CISA Cybersecurity Advisory Committee (CSAC) in June 2021 “to advance CISA’s cybersecurity mission and strengthen the cybersecurity of the United States.”³³ CSAC in turn established a “Protecting Critical Infrastructure from Misinformation & Disinformation” Subcommittee,³⁴ commonly known as the “MDM Subcommittee.”³⁵



The MDM Subcommittee, which has since disbanded,³⁶ brought together government, Big Tech, and academic misinformation “experts,” including:

- **Dr. Kate Starbird**, Associate Professor and Co-Founder of the University of Washington’s Center for an Informed Public (CIP).³⁷ CIP was a member of both the Election Integrity Partnership (EIP)³⁸ and the Virality Project (VP).³⁹ Starbird served as the Chair of the MDM Subcommittee.⁴⁰
- **Vijaya Gadde**, the former Chief Legal Officer of Twitter, who was “involved in censoring [the *New York Post*’s Hunter Biden laptop” story.⁴¹ Gadde was also “behind the decision to permanently ban former President Trump from Twitter.”⁴² Shortly after Elon Musk completed his purchase of Twitter, Gadde was fired from the company in October 2022.⁴³
- **Suzanne Spaulding**, a former assistant general counsel and legal adviser for the Central Intelligence Agency (CIA), who also served as the Under Secretary for the NPPD,

³³ *CISA Cybersecurity Advisory Committee*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee> (last visited Jun. 23, 2023).

³⁴ CISA CYBERSECURITY ADVISORY COMM., 2022 ANNUAL REPORT, at 2 (2022), https://www.cisa.gov/sites/default/files/2023-01/csac_annual_report_2023-01-18_508_0.pdf.

³⁵ See, e.g., CISA CYBERSECURITY ADVISORY COMM., DECEMBER 6, 2022 MEETING SUMMARY CLOSED SESSION, at 3 (On file with the Comm.).

³⁶ CISA CYBERSECURITY ADVISORY COMM., DECEMBER 6, 2022 MEETING SUMMARY OPEN SESSION, at 1, https://www.cisa.gov/sites/default/files/publications/CSAC_December-Quarterly-Meeting-Summary_508_01062023_0.pdf.

³⁷ *Kate Starbird*, UNIVERSITY OF WASHINGTON, <https://www.hcde.washington.edu/starbird> (last visited Jun. 12, 2023).

³⁸ ELECTION INTEGRITY P’SHIP, *THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION*, at vi (Eden Beck ed., 2021).

³⁹ VIRALITY PROJECT, *MEMES, MAGNETS, AND MICROCHIPS: NARRATIVE DYNAMICS AROUND COVID-19 VACCINES*, at 1 (Eden Beck ed., 2022).

⁴⁰ CISA CYBERSECURITY ADVISORY COMM., SUBCOMMITTEE FACTSHEET (2022), https://www.cisa.gov/sites/default/files/publications/CSAC_Subcommittee_Fact_Sheet_05192022_508c.pdf.

⁴¹ Victor Nava, *Who is Vijaya Gadde, the Twitter exec involved in censoring Post’s Hunter Biden laptop bombshell?*, NEW YORK POST (Dec. 3, 2022).

⁴² *The Twitter executives fired after Elon Musk’s takeover*, AXIOS (Oct. 28, 2022).

⁴³ *Id.*

CISA’s predecessor within DHS.⁴⁴ Spaulding is now the “director of the Defending Democratic Institutions project at the Center for Strategic International Studies (CSIS).”⁴⁵

MDM Subcommittee meetings also featured government participants, including Geoff Hale, who leads CISA’s “Election Security Initiative,”⁴⁶ and Kim Wyman, the former Washington Secretary of State, who now serves as CISA’s Senior Election Security Advisor.⁴⁷

During its existence, the MDM Subcommittee issued two sets of formal recommendations: one set in June 2022,⁴⁸ and another in September 2022.⁴⁹ The Subcommittee’s June 2022 recommendations included, among other things, recommendations that “CISA should approach the [misinformation and disinformation] problem with the entire information ecosystem in view. This includes social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio, and other online resources.”⁵⁰

The Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a nonprofit organization that operates the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).⁵¹ According to a postmortem report covering social media activity related to the 2020 election cycle, “the EI-ISAC served as a singular conduit for election officials to report false or misleading information to platforms.”⁵² Put plainly, election officials around the country sent CIS purportedly false or misleading content, which CIS forwarded to the relevant social media platforms.⁵³



⁴⁴ *Suzanne Spaulding*, CENTER FOR STRATEGIC & INT’L STUDIES, <https://www.csis.org/people/suzanne-spaulding> (last visited Jun. 23, 2023).

⁴⁵ *Id.*

⁴⁶ *Geoff Hale*, RSA CONF., <https://www.rsaconference.com/experts/geoff-hale> (last visited Jun. 23, 2023).

⁴⁷ *Kim Wyman*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/about/leadership/kim-wyman> (last visited Jun. 23, 2023).

⁴⁸ CISA CYBERSECURITY ADVISORY COMM., JUNE 22, 2022 MEETING SUMMARY OPEN SESSION, https://www.cisa.gov/sites/default/files/publications/CSAC_June_Quarterly_Meeting_Summary.pdf.

⁴⁹ CISA CYBERSECURITY ADVISORY COMM., DECEMBER 6, 2022 MEETING SUMMARY OPEN SESSION, https://www.cisa.gov/sites/default/files/publications/CSAC_December-Quarterly-Meeting-Summary_508_01062023_0.pdf.

⁵⁰ CISA CYBERSECURITY ADVISORY COMM., REPORT TO THE CISA DIRECTOR PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION AND DISINFORMATION JUNE 22, 2022, at 2, https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20E2%80%93%20MDM_0.pdf.

⁵¹ *EI-ISAC*, CENTER FOR INTERNET SEC., <https://www.cisecurity.org/ei-isac> (last visited Jun. 23, 2023).

⁵² ELECTION INTEGRITY P’SHIP, *supra* note 38, at 13.

⁵³ *See id.*

CISA funds CIS, including spending \$27 million in FY 2024 on operating the EI-ISAC and the MS-ISAC.⁵⁴ As illustrated by the diagram below from CIS’s website, the “EI-ISAC is federally funded by CISA and a division of the Center for Internet Security.”⁵⁵



⁵⁴ DEP’T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY BUDGET OVERVIEW FISCAL YEAR 2024 CONGRESSIONAL JUSTIFICATION, at 37 (2023).

⁵⁵ *EI-ISAC*, *supra* note 51.

CISA’S MISSION CREEP INTO SURVEILLANCE, CENSORSHIP, AND COVER-UPS

The Committee and Select Subcommittee have obtained previously undisclosed, non-public documents that reveal CISA expanded its mission to surveil Americans’ speech on social media, colluded with Big Tech and government-funded third parties to censor by proxy, and tried to hide its plainly unconstitutional activities from the public.

Surveillance. CISA expanded its mission from “cybersecurity” to monitor foreign “disinformation” to eventually monitor all “disinformation,” including Americans’ speech. In one e-mail exchange obtained by the Committee and Select Subcommittee, the agency’s rapid mission creep surprised even a non-profit focused on foreign “disinformation.”

Censorship. CISA exploited its connections with Big Tech and government-funded non-profits to censor by proxy, in order to circumvent the First Amendment’s prohibition against government-induced censorship. This included the creation of reporting “portals” which funneled “misinformation” reports from the government directly to social media platforms. Newly uncovered meeting minutes show that CISA was advised by a group Big Tech executives and academics who encouraged CISA’s unconstitutional behavior.

Cover-ups. As CISA’s operational scope expanded further into unconstitutional territory, the agency and its advisors tried to cover their tracks and cover up CISA’s censorship of domestic speech and surveillance of American citizens’ social media activity. This included scrubbing CISA’s website of references to domestic “misinformation” and “disinformation.”

I. CISA has transformed into a domestic intelligence and speech-police agency, far exceeding its statutory authority

CISA’s focus on “cybersecurity” quickly expanded into social media surveillance of real and perceived foreign actors. Shortly after CISA became its own agency, then-DHS Secretary Kristjen Nielsen created the “Countering Foreign Influence Task Force” (CFITF) within CISA “to focus on election infrastructure disinformation.”⁵⁶ Following the unfounded claims by Democrats that foreign—particularly Russian—influence changed the outcome of the 2016 election,⁵⁷ CISA expanded its “cybersecurity” role to include countering foreign malign influence operations. In its public materials, CISA emphasized at the time that it was primarily concerned with addressing foreign, rather than domestic, disinformation.⁵⁸ Starting in January 2019, Brian Scully served first as the head of the CFITF and later as the head of the MDM team at CISA.⁵⁹

⁵⁶ *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 5.

⁵⁷ See Gregory Eady et al., *Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior*, 14:62 NATURE COMMUNICATIONS 1, at 8-9 (2023).

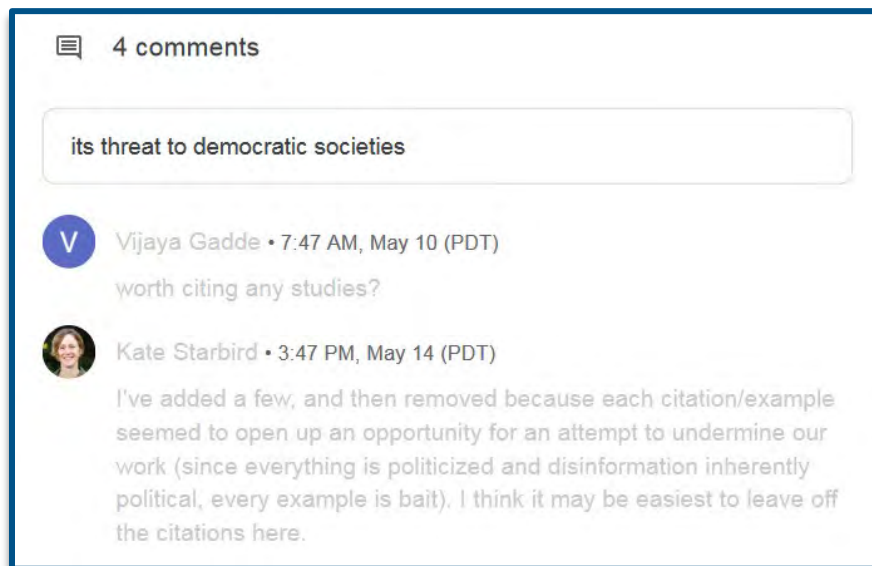
⁵⁸ See, e.g., *Resilience Series Graphic Novels*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation/resilience-series-graphic-novels> (last visited Jun. 23, 2023).

⁵⁹ See Scully Dep. 11:24–12:2, *supra* note 5.

In January 2021, after President Biden took office, “CISA transitioned its [CFITF] to promote more flexibility to focus on general MDM,” or so-called “Mis-, Dis-, and Malinformation.”⁶⁰ In so doing, CISA admitted that its focus was no longer exclusively on “countering foreign influence,” but was also targeting MDM originating from domestic sources. For example, according to a 2022 CISA pamphlet titled “Planning and Incident Response Guide for Election Officials,” “MDM also may originate from domestic sources aiming to sow divisions and reduce national cohesion.”⁶¹

Although CISA’s efforts to police speech are highly troubling overall, one particularly problematic aspect is CISA’s focus on “malinformation.” According to CISA’s own definition, “[m]alinformation is based on fact, but used out of context to mislead, harm, or manipulate.”⁶² In other words, malinformation is *factual* information that is objectionable not because it is false or untruthful, but because it is provided without adequate “context”—context as determined by the government.

In addition, what constitutes “misinformation” or “disinformation” is determined by government actors, whose evaluations of truth and falsity are necessarily subjective, and “inherently political,” as explained in the comments of a Google Doc by Starbird below.⁶³



CISA’s involvement in policing alleged mis- and disinformation, as well as malinformation—truthful information without “sufficient” context—is a direct and serious threat to First Amendment principles.

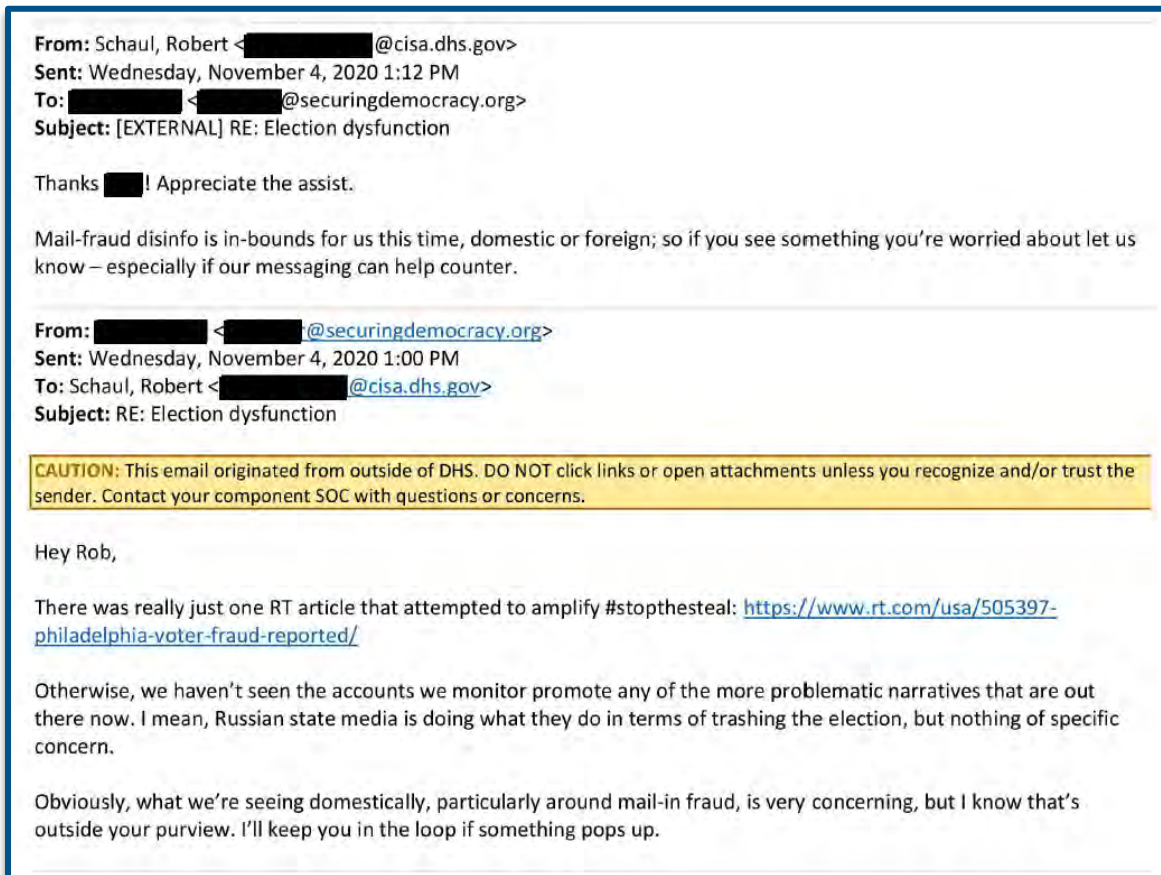
⁶⁰ *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 7.

⁶¹ CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, MIS-, DIS-, AND MALINFORMATION PLANNING AND INCIDENT RESPONSE GUIDE FOR ELECTION OFFICIALS, at 1 (2022), https://www.cisa.gov/sites/default/files/2022-11/mdm-incident-response-guide_508.pdf.

⁶² *Id.*

⁶³ E-mail from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.).

Although the CFITF did not formally shed “foreign” from its name until January 2021, CISA’s efforts to curb domestic MDM had been ongoing for months, ramping up in advance of the 2020 election. An e-mail exchange on November 4, 2020 demonstrates that even non-profits focused on “disinformation,” such as the German Marshall Fund’s Alliance for Securing Democracy (ASD), were caught off guard by CISA’s expansion into the surveillance of domestic speech. In the exchange, an ASD employee emailed Robert Schaul, the Analysis and Resilience Policy Lead at CISA,⁶⁴ writing: “Obviously, what we’re seeing domestically, particularly around mail-in fraud, is very concerning, but I know that’s outside your purview.”⁶⁵ Schaul corrected the ASD employee: “Mail-fraud disinfo[rmation] is in-bounds for us this time, domestic or foreign; so if you see something you’re worried about let us know.”⁶⁶



Despite constituting a clear departure from its statutory mandate, CISA’s MDM team has, at its peak, been comprised of “a total of 15 dedicated part- and full-time staff,” who focus on “disinformation activities targeting elections and critical infrastructure.”⁶⁷ Jen Easterly, the

⁶⁴ *U.S.-Paris Tech Challenge*, ATLANTIC COUNCIL, <https://www.atlanticcouncil.org/event/u-s-paris-tech-challenge/> (last visited Jun. 23, 2023).

⁶⁵ E-mail from German Marshall Fund employee to Robert Schaul (Nov. 4, 2020, 1:00 PM) (on file with the Comm.).

⁶⁶ E-mail from Robert Schaul to German Marshall Fund employee (Nov. 4, 2020, 1:12 PM) (on file with the Comm.).

⁶⁷ *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 7.

current Director of CISA, justified CISA’s MDM-related activities by saying: “One could argue we’re in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important.”⁶⁸

A. Switchboarding: CISA’s coordination with Big Tech to censor Americans

CISA’s Director, Jen Easterly, claimed in her March 28, 2023 testimony before Congress that “we don’t flag anything to social media organizations at all. We are focused on building resilience to foreign influence and disinformation.”⁶⁹ Despite Easterly’s assurances, however, the DHS Office of Inspector General (OIG) has reported that CISA began “notifying social media platforms or appropriate law enforcement official when voting-related disinformation appeared in social media” as early as 2018.⁷⁰

When deposed as part of ongoing litigation in federal court, Brian Scully, the head of CISA’s MDM team, confirmed that CISA has historically flagged disinformation to social media platforms, in a process known as “switchboarding.”⁷¹ Scully further described switchboarding as a “resource intensive”⁷² process whereby CISA officials received alleged “misinformation” reports from election officials and forwarded those reports to social media companies so that they could take enforcement measures against the reported content.⁷³

CISA has sought to disclaim any responsibility in affecting social media companies’ decisions on content moderation. In reporting content to social media platforms, CISA officials, including Scully, often appended a disclaimer to their e-mails, claiming, “CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms.”⁷⁴ However, when deposed as part of ongoing federal litigation, Scully admitted that CISA was aware that its outreach to social media companies about alleged disinformation would trigger content moderation.⁷⁵

B. CISA’s MDM consultants rejected constitutional “limitations” on the surveillance and censorship of domestic speech

Originally created to protect critical infrastructure such as dams and pipelines from foreign malign actors, CISA has ventured well beyond its founding mandate and began targeting constitutionally protected domestic speech for censorship on social media platforms. By 2020,

⁶⁸ Miller, *supra* note 1.

⁶⁹ H. COMM. ON APPROPRIATIONS, *Budget Hearing – Fiscal Year 2024 Request for the Cybersecurity and Infrastructure Security Agency*, YOUTUBE (Mar. 28, 2023).

⁷⁰ *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 5.

⁷¹ Scully Dep. 23:16–24:2, *supra* note 5.

⁷² Scully Dep. 62:15–22, *supra* note 5.

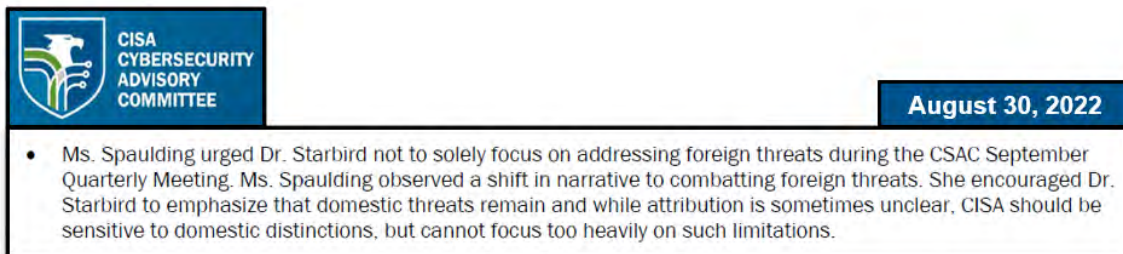
⁷³ Scully Dep. 17:1–18:1, *supra* note 5.

⁷⁴ *See, e.g.*, e-mail from Brian Scully to Facebook employees (Oct. 28, 2020, 2:09 PM) (on file with the Comm.); e-mail from Brian Scully to Google employee (Oct. 1, 2020 9:01 PM) (on file with the Comm.).

⁷⁵ Scully Dep. 17:15–18:1, *supra* note 5. *See also* *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 30, 2023).

just two years after its creation, CISA had unilaterally expanded its authorities from countering foreign influence operations to curtailing domestic speech. In 2021, CISA created an advisory committee, including the MDM Subcommittee, in order to receive input from Big Tech and “disinformation” experts. According to documents produced to the Committee and Select Subcommittee,⁷⁶ members of the MDM Subcommittee, while serving in this advisory role, pushed aside legitimate criticism and urged CISA to continue on its unconstitutional trajectory.

On August 30, 2022, MDM Subcommittee members discussed the propriety of DHS “identifying domestic actors” spreading alleged disinformation.⁷⁷ According to notes of the meeting that day, Suzanne Spaulding, a former CIA legal advisor, “urged Dr. Starbird not to solely focus on addressing foreign threats.”⁷⁸ Spaulding also “encouraged Dr. Starbird to emphasize that domestic threats remain and while attribution is sometimes unclear, CISA should be sensitive to domestic distinctions, but cannot focus too heavily on such limitations.”⁷⁹ In the same meeting, the director of CISA’s Election Security Initiative “[Geoff] Hale reflected that these discussions of scoping authority relate to the Subcommittee’s initial deliberations urging CISA to be actor-agnostic in their work combating mis- and dis-information.”⁸⁰ In other words, Hale, a federal government employee, observed that the Subcommittee’s work addressing alleged mis- and dis-information should not distinguish between foreign and domestic sources.



Other documents produced to the Committee and Select Subcommittee suggest that Hale and the MDM Subcommittee urged action in the domestic space, even in the face of opposition from state and local election administration officials. In particular, during the MDM Subcommittee’s August 8, 2022 meeting, Twitter’s Chief Legal Officer Vijaya Gadde “reflected on the group’s previous meeting with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) and noted in their feedback that CISA should not be involved in this mission space, except when a foreign adversary is at play.”⁸¹ Gadde doubted that this distinction could serve as a meaningful limit for CISA because “it is difficult to determine whether a foreign adversary is involved.”⁸² Later in the same

⁷⁶ These documents include meeting minutes from the MDM Subcommittee. As Chair of the MDM Subcommittee, Dr. Kate Starbird reviewed and approved these meeting minutes before they were circulated. Transcribed Interview of Kate Starbird at 39 (on file with the Comm.).

⁷⁷ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING AUGUST 30, 2022, at 1 (on file with the Comm.).

⁷⁸ *Id.* at 2.


⁷⁹ *Id.*

⁸⁰ *Id.* at 1.

⁸¹ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING AUGUST 8, 2022, at 1 (on file with the Comm.).

⁸² *Id.*

meeting, Starbird “noted that because mis- and disinformation is universal, CISA must play a role on the national level.”⁸³




**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

August 8, 2022

- Subcommittee members discussed CISA’s role in the elections space. Dr. Starbird addressed the doubt and manufactured doubt into whether CISA should play a role. She stressed one of the goals of the recommendations is to share why CISA should act in the elections space to combat mis- and dis-information.
 - Ms. Gadde reflected on the group’s previous meeting with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) and noted in their feedback that CISA should not be involved in this mission space, except when a foreign adversary is at play. She cautioned that it is difficult to determine whether a foreign adversary is involved.

C. CISA considered creating an anti-MDM “rapid response team” to physically deploy across the United States

In one particularly notable departure from its legal authority, during the MDM Subcommittee’s June 14, 2022 meeting, participants “explore[d] the idea of how CISA could develop a rapid response team to deploy . . . in-person to local election officials’ jurisdictions struggling with specific informational threats.”⁸⁴ The CISA officials present at the meeting seemed receptive to the idea, with Geoff Hale, the director of CISA’s Election Security Initiative, commenting that “this is a fascinating idea that takes CISA’s existing operational responsibilities to consider MDM as part of its core mission set.”⁸⁵



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

June 14, 2022

- Dr. Starbird added that Mr. Richer’s colleague, Mr. Scott Jarred, suggested that the subcommittee explore the idea of how CISA could develop a rapid response team to deploy virtually or in-person to local election officials’ jurisdictions struggling with specific informational threats. The support would include checking equipment to verify if a breach is present or not, determining how to communicate the existence of a breach, and determining how to target certain kinds of communication.
 - Ms. Tate-Nadeau clarified if this rapid response team would only act in the context of MDM threats. Dr. Starbird noted that the response team would require a broader range of expertise, as they first must be able to verify whether a real threat exists, then be able to communicate the existence of an MDM threat.
 - Mr. Geoff Hale, CISA, commented that this is a fascinating idea that takes CISA’s existing operational responsibilities to consider MDM as part of its core mission set. He noted that this would be an evolution of CISA’s current defensive posture. Ms. Gadde agreed with this framing of the question.
 - Dr. Starbird commented that the rapid response team would need to surge for short periods of time around elections. She suggested the subcommittee consider the requirements for the team’s expandability, ability to conduct media analysis, and the level of understanding on MDM in a communications context.

⁸³ *Id.* at 2.

⁸⁴ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JUNE 14, 2022, at 2 (on file with the Comm.).

⁸⁵ *Id.*

Starbird, the chair of the MDM Subcommittee, also “commented that the rapid response team would need to surge for short periods of time around elections.”⁸⁶ Hale then “noted the possibility to stand up this team in the short term by encouraging the communications team to consider MDM equities.”⁸⁷

Subcommittee members then abandoned any pretext of operating within CISA’s legal authority, with Twitter’s Vijaya Gadde noting “that the idea of a rapid response team must include the ability to engage whether or not a cyber component is present.”⁸⁸ “Dr. Starbird agreed with Ms. Gadde’s point that threats to critical infrastructure are not limited to cyber threats.”⁸⁹

- Ms. Gadde noted that physical and MDM-related threats are often interrelated, so the group cannot address the physical threats against elections officials without addressing the root cause of MDM-related threats. She continued by stressing that MDM threat exist with or without a cyber component. She noted that the idea of a rapid response team must include the ability to engage whether or not a cyber component is present.
- Dr. Starbird agreed with Ms. Gadde’s point that threats to critical infrastructure are not limited to cyber threats.

D. MDM “experts” wanted CISA to crack down on *factual* information

Even so-called “malinformation”—truthful information that, according to the government, may carry the potential to mislead—could not escape the scrutiny of CISA’s MDM “experts.”⁹⁰ In an e-mail exchange between MDM Subcommittee members Starbird and Spaulding, Spaulding wrote: “As I’ve read more about malinformation, I think you’re right that it could fit the kinds of risks we are concerned about. The challenge may be that because it is not false, per se . . . it is much trickier from a policy perspective.”⁹¹ Spaulding proposed a “compromise”: “that [malinformation] is part of CISA’s current scope but that our recommendations, at least at this stage, are focused primarily on countering false information.”⁹²

On May 16, 2022, at 6:02 PM, Suzanne Spaulding <[REDACTED]> wrote:

Kate,
 thanks for continuing to think about this issue. As I've read more about malinformation, I think you're right that it could fit the kinds of risks we are concerned about. The challenge may be that because it is not false, per se (though presented in a misleading, manipulative way to cause harm), it is much trickier from a policy perspective. I think we could compromise by noting that it is part of CISA's current scope but that our recommendations, at least at this stage, are focused primarily on countering false information. Would that work? I'll try suggesting line-in line-out changes to the text.
 best,
 Suzanne

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

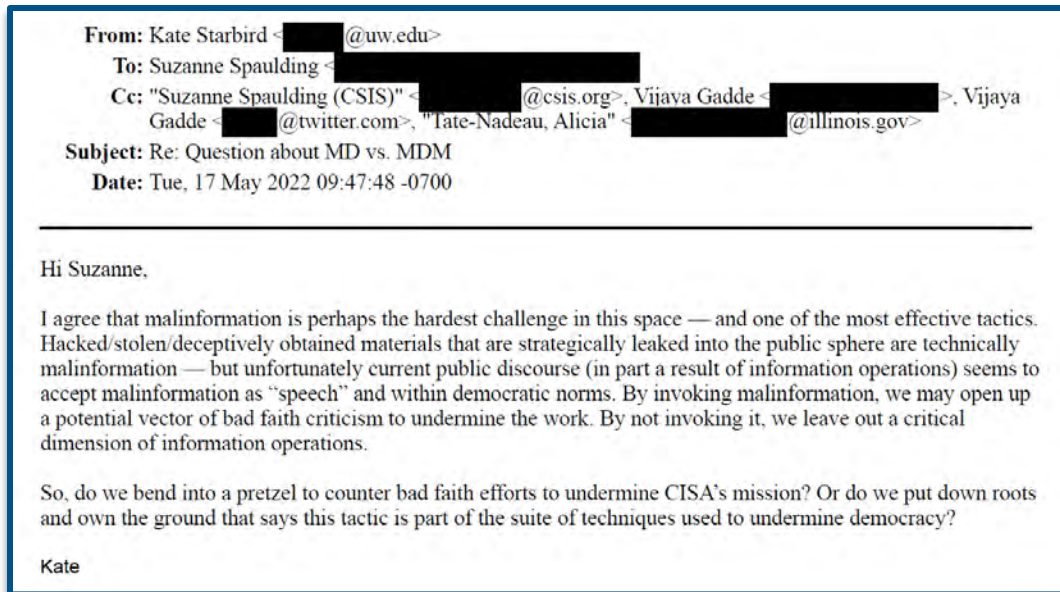
⁸⁹ *Id.*

⁹⁰ The First Amendment protects domestic speech, regardless of whether government actors consider it mis-, dis-, or malinformation. *See* United States. v. Alvarez, 567 U.S. 709, 718 (2012) (plurality opinion).

⁹¹ E-mail from Suzanne Spaulding to Kate Starbird (May 16, 2022, 6:02 PM) (on file with the Comm.).

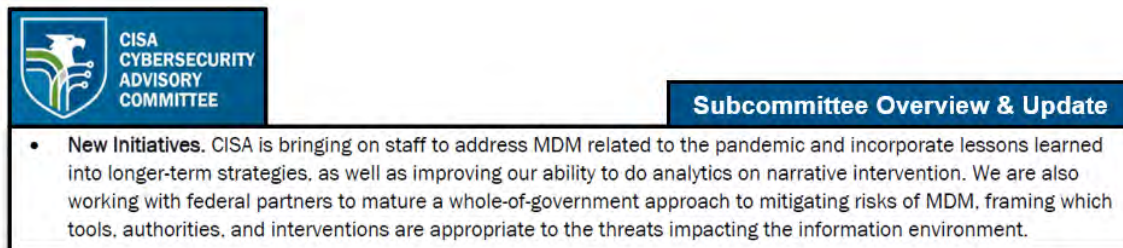
⁹² *Id.*

Starbird responded that “malinformation is perhaps the hardest challenge in this space.”⁹³ Starbird then lamented that “unfortunately current public discourse (in part a result of information operations) seems to accept malinformation as ‘speech’ and within democratic norms” and that CISA may face “bad faith criticism” for censoring content that is true.⁹⁴



E. CISA is only one part of a “whole-of-government” approach to MDM

Documents obtained by the Committee and Select Subcommittee establish that CISA and the MDM Subcommittee considered CISA to be only one part of a grander, “whole-of-government” approach to tackling disfavored speech. For example, according to the MDM Subcommittee’s “Subcommittee Overview & Update,” “CISA is bringing on staff to address MDM related to the pandemic . . . as well as improving our ability to do analytics on narrative intervention. We are also working with federal partners to mature a whole-of-government approach to mitigating risks of MDM, framing which . . . interventions are appropriate to the threats impacting the information environment.”⁹⁵

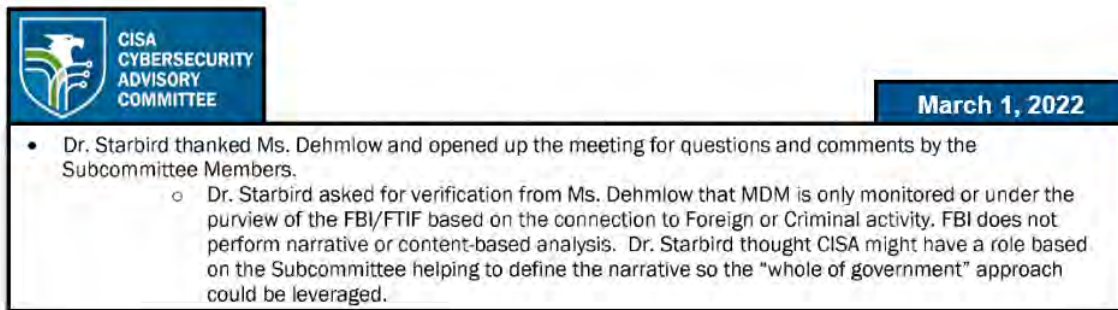


⁹³ E-mail from Kate Starbird to Suzanne Spaulding (May 17, 2022, 9:47 AM) (on file with the Comm.).

⁹⁴ *Id.*

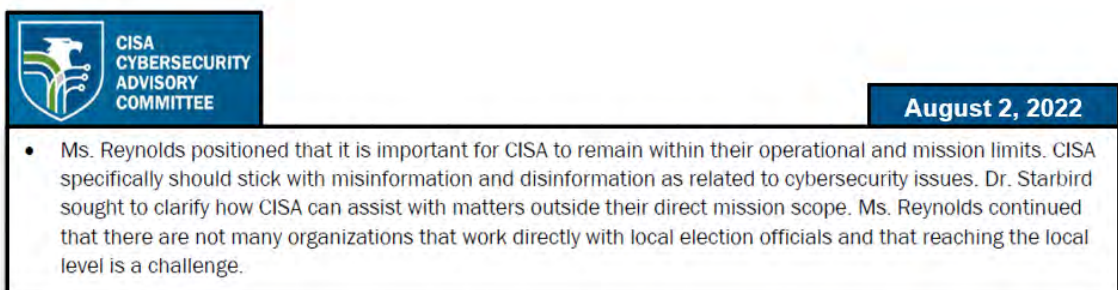
⁹⁵ CISA CYBERSECURITY ADVISORY COMM., SUBCOMMITTEE OVERVIEW & UPDATE: PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION, at 1 (2022) (on file with the Comm.).

As another example, during a March 1, 2022 meeting of the MDM Subcommittee, Laura Dehmlow of the FBI’s Foreign Influence Task Force (FITF), who had been invited to brief the MDM Subcommittee, claimed that the “FBI does not perform narrative or content-based analysis.”⁹⁶ According to the meeting notes, Starbird, the chair of the MDM Subcommittee, then offered CISA to fill this perceived gap in the government’s censorship efforts, suggesting that “CISA might have a role based on the Subcommittee helping to define the narrative so the ‘whole of government’ approach could be leveraged.”⁹⁷



F. State election officials warned CISA to “remain within [its] operational and mission limits,” lest it should earn the public’s “distrust.”

MDM Subcommittee meeting notes and other documents obtained by the Committee and Select Subcommittee reveal that those engaging with CISA, and even election officials, were critical of CISA’s efforts to crack down on domestic speech related to elections. On August 2, 2022, Leslie Reynolds of the National Association of Secretaries of State (NASS) cautioned the MDM Subcommittee “that it is important for CISA to remain within their operational and mission limits. CISA specifically should stick with misinformation and disinformation as related to cybersecurity issues.”⁹⁸ Unfazed by the admonishment, Starbird promptly “sought to clarify how CISA can assist with matters outside their direct mission scope.”⁹⁹



⁹⁶ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MARCH 1, 2022, at 1 (on file with the Comm.).

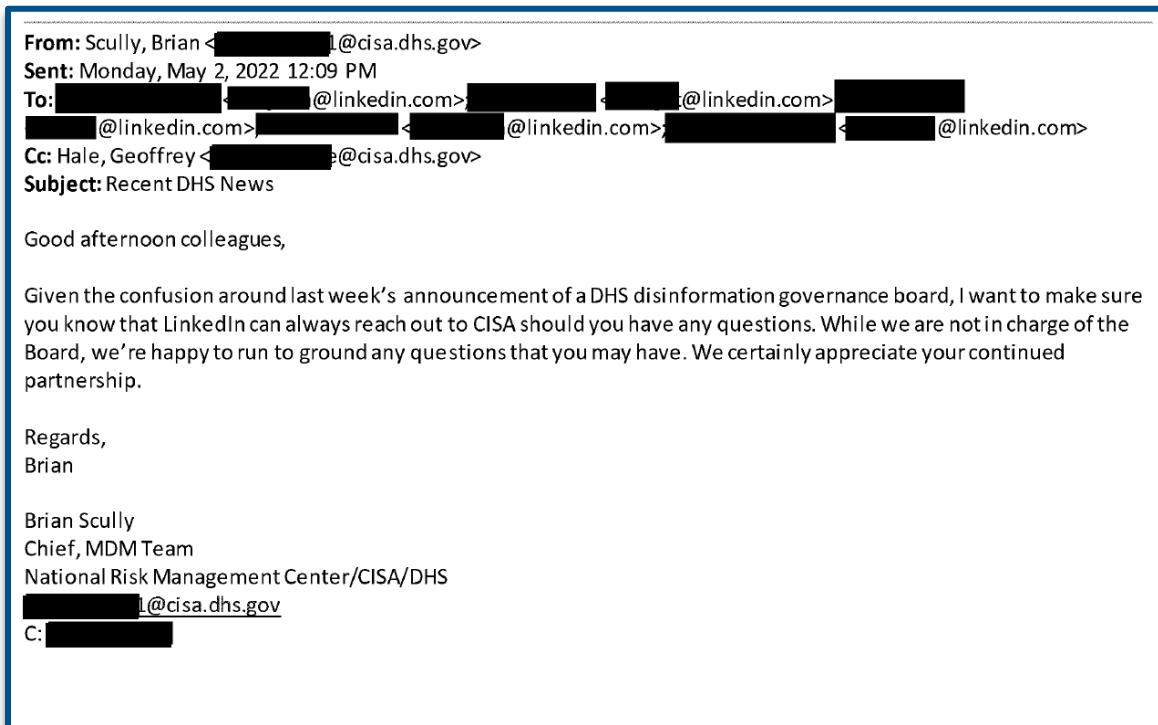
⁹⁷ *Id.*

⁹⁸ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING AUGUST 2, 2022, at 2 (on file with the Comm.).

⁹⁹ *Id.*

H. Social media companies mocked CISA’s MDM team and DHS’s Disinformation Governance Board

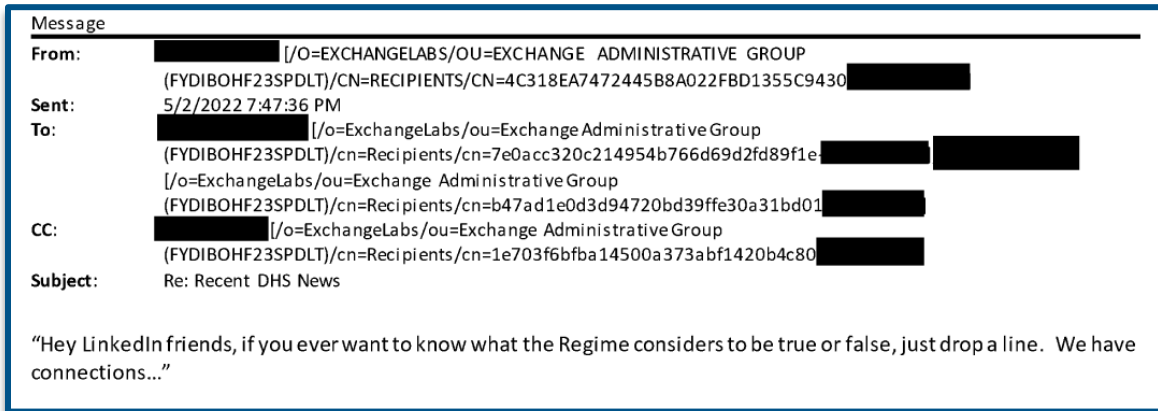
CISA’s “connectivity to the (domestic) social media companies” did not, however, prevent it from being criticized by these social media companies. In May 2022, following public backlash concerning DHS’s Orwellian Disinformation Governance Board,¹⁰³ Brian Scully, the head of CISA’s MDM team, e-mailed several LinkedIn employees, writing, “[g]iven the confusion around last week’s announcement of a DHS disinformation governance board, I want to make sure you know that LinkedIn can always reach out to CISA should you have any questions.”¹⁰⁴



¹⁰³ The Disinformation Governance Board was an organ of DHS intended to “coordinate countering misinformation related to homeland security,” which was first announced on April 27, 2022. Eugene Daniels, Rachel Bade, and Ryan Lizza, *POLITICO Playbook: Fauci pulls out of WHCD. Is Biden next?*, *POLITICO* (Apr. 27, 2022). The Board’s inaugural (in fact, only) director was Nina Jankowicz. Prior to assuming the helm of the Board, Jankowicz falsely described the Hunter Biden laptop as a “Trump campaign product.” Roger Koppl and Abigail Devereaux, *Biden Establishes a Ministry of Truth*, *WALL STREET JOURNAL* (May 1, 2022). The Board was “met with an overwhelmingly negative response” and “[e]ven Democratic lawmakers were skeptical” of the initiative. Nicole Sganga, *What is DHS’ Disinformation Governance Board and why is everyone so mad about it?*, *CBS NEWS* (May 6, 2022). After significant public backlash, the Board was paused on May 18, 2022, with Jankowicz announcing her resignation. Rebecca Beitsch, *DHS to pause work of disinformation board*, *THE HILL* (May 18, 2022). The Board was formally terminated on August 24, 2022. Press Release, Dep’t of Homeland Sec., *Following HSAC Recommendation, DHS terminates Disinformation Governance Board* (Aug. 24, 2022), <https://www.dhs.gov/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-governance-board>.

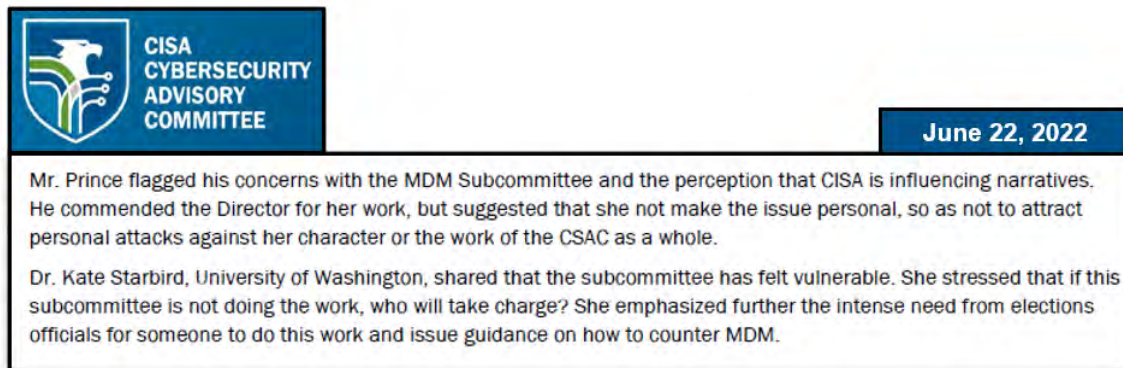
¹⁰⁴ E-mail from Brian Scully to LinkedIn employees (May 2, 2022, 12:09 PM) (on file with the Comm.).

A LinkedIn employee then forwarded Scully’s e-mail to another LinkedIn employee, who responded internally, mocking Scully: “Hey LinkedIn friends, if you ever want to know what the Regime considers to be true or false, just drop a line. We have connections...”¹⁰⁵



I. CSAC members were concerned about the MDM Subcommittee

Other members of the broader CSAC also exhibited discomfort at CISA’s and the MDM Subcommittee’s efforts related to MDM. During a closed session of the CSAC at its June 2022 Quarterly meeting, Cloudflare CEO Matthew Prince “flagged his concerns with the MDM Subcommittee and the perception that CISA is influencing narratives.”¹⁰⁶



Nicole Perloth, another CSAC member, also “recommended that CISA establish an independent equivalent of a Facebook oversight board with people who are not vocal on Twitter, nor are they politically active, to give honest feedback. She expressed concern that since Director Easterly is serving under a political administration, this will put the recommendations at a higher risk.”¹⁰⁷

¹⁰⁵ E-mail from LinkedIn employee to LinkedIn employees (May 2, 2022, 7:47 PM) (on file with the Comm.).

¹⁰⁶ CISA CYBERSECURITY ADVISORY COMM., JUNE 22, 2022 MEETING SUMMARY CLOSED SESSION, at 5 (on file with the Comm.).

¹⁰⁷ *Id.* at 6.

II. CISA colludes with third parties to circumvent the First Amendment and conduct censorship by proxy

For the same reasons that the federal government may not censor Americans' speech, the federal government is also prohibited from using third parties to censor speech on its behalf. Under the First Amendment, the government may not "abridg[e] the freedom of speech."¹⁰⁸ The Constitution thus forbids the government from engaging in conduct that prevents or hampers speech on private social media platforms because of its content or the viewpoint that it expresses.¹⁰⁹

Challenges to government involvement in the suppression of speech on social media are all relatively recent. As such, courts have had little opportunity to address the matter. However, a federal court recently found that this type of conduct gave rise to a plausible First Amendment claim: "Plaintiffs have clearly and plausibly alleged that [the government] engaged in viewpoint discrimination and prior restraints,"¹¹⁰ the court declared, citing the plaintiffs' allegations of "extensive and highly effective efforts of government officials to silence or muffle the expression of disfavored viewpoints."¹¹¹ The court concluded that the plaintiffs had "plausibly alleged state action under the theories of joint participation, entwinement, and the combining of factors such as subsidization, authorization, and encouragement."¹¹²

In a draft of its June 2022 recommendations, the MDM Subcommittee refers to this pattern of unconstitutional outsourcing, writing, "CISA should also engage in content- and narrative-specific mitigation efforts . . . CISA should support these efforts . . . through funding outside organizations to assist in this work."¹¹³

- **#2: CISA should also engage in content- and narrative-specific mitigation efforts.** Proactive work should also include identifying and supporting trusted, authoritative sources in specific communities, e.g. in the elections context, local media and election officials. These efforts should also include building knowledge and experience that can empower individuals to be more resilient against divisive and despair-inducing MDM. CISA should support these efforts by creating and sharing materials; by providing education and frameworks for others to produce their own materials; and through funding to outside organizations to assist in this work

¹⁰⁸ U.S. CONST. amend. I.

¹⁰⁹ *Ashcroft v. ACLU*, 535 U.S. 564, 573 (2002). See also *Hamburger*, *supra* note 24.

¹¹⁰ Mem. Ruling re 128 Mot. to Dismiss at 70, *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 224.

¹¹¹ *Id.* at 63

¹¹² *Id.* at 68.

¹¹³ E-mail from Kate Starbird to James Nash (May 10, 2022, 9:38 PM) (on file with the Comm.).

A. CISA’s external censorship arm: the EI-ISAC

The CISA-funded EI-ISAC was used by CIS during the 2020 election cycle as “a single point of reporting and tracking for misinformation across all channels and platforms.”¹¹⁴ As described in a slide from a CIS presentation titled, “2020 CIS Election Infrastructure Misinformation Reporting Summary,” the EI-ISAC was intended to “[s]treamline and simplify misinformation reporting for election officials by eliminating multiple interactions to submit and follow up on reports.”¹¹⁵ In so doing, CIS boasted that it “leverage[d] DHS CISA’s relationship with social media organizations to ensure priority treatment of misinformation reports.”¹¹⁶

CIS **The CIS Approach**

- Streamline and simplify misinformation reporting for election officials by eliminating multiple interactions to submit and follow up on reports
- Established a single EI-ISAC email account and database to serve as a single point of reporting and tracking for misinformation across all channels and platforms
- Leverage DHS CISA’s relationship with social media organizations to ensure priority treatment of misinformation reports
- Facilitate information sharing between election officials about reported misinformation
- Provide timely and meaningful feedback to election officials on the status of their reports
- Partner with outside analysis efforts, the Election Integrity Partnership*, to augment identification and analysis of elections-related misinformation

* The Election Integrity Partnership (EIP) was comprised of the [Stanford Internet Observatory](#) and [Program on Democracy and the Internet](#), [Graphika](#), the [Atlantic Council’s Digital Forensic Research Lab](#), and the [University of Washington’s Center for an Informed Public](#).

3

CISA also became involved with the Election Integrity Partnership (EIP). CIS and the EI-ISAC, as well as CISA itself, all served as “external stakeholders” of the project.¹¹⁷ During the 2020 election cycle, the CISA-funded entities could—and did—send in reports of alleged misinformation to the EIP. Members of EIP, such as Alex Stamos, the director of the Stanford Internet Observatory, would send purportedly problematic content directly to social media platforms with recommendations on what content moderation steps the platforms should take.

Brian Scully, CISA’s MDM lead, confirmed in his deposition, that CISA did not directly engage in switchboarding for the 2022 election cycle, unlike in the 2020 election cycle.¹¹⁸ Rather, CISA transferred the “switchboard function” to the EI-ISAC.¹¹⁹

¹¹⁴ Aaron Wilson, 2020 CIS Election Infrastructure Misinformation Reporting Summary, at 3 (presentation materials) (on file with the Comm.).

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ ELECTION INTEGRITY P’SHP, *supra* note 38, at 12.

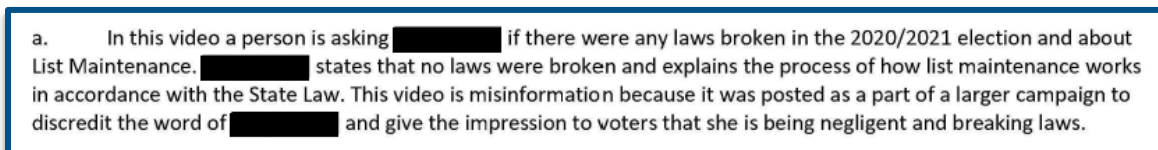
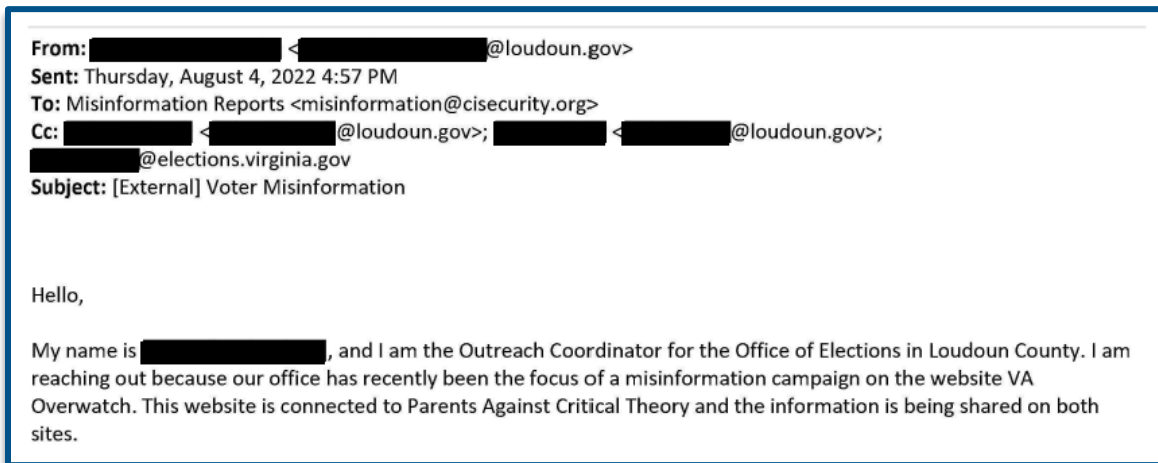
¹¹⁸ Scully Dep. 21:19–25, *supra* note 5.

¹¹⁹ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JULY 26, 2022, at 1 (on file with the Comm.).

B. State and local election officials used the EI-ISAC in an effort to silence critics and political opponents

CIS had previously claimed that “Election Infrastructure Misinformation and Disinformation does NOT include: “content that is polarizing, biased, partisan or contains viewpoints expressed about elections or politics”; “inaccurate statements about an elected or appointed official, candidate, or political party”; or “broad, non-specific statements about the integrity of elections or civic processes that do not reference a specific current election administration activity.”¹²⁰

But, in practice, state and local election officials used the CISA-funded EI-ISAC in an effort to silence criticism and political dissent of the nature allegedly “NOT include[d]” in CIS’s definition of “Election Infrastructure Misinformation and Disinformation.” For example, in August 2022, a Loudoun County, Virginia, government official reported a Tweet featuring an unedited video of a county official “because it was posted as part of a larger campaign to discredit the word of” that official.¹²¹ The Loudon County official’s remark that the account she flagged “is connected to Parents Against Critical Race Theory” reveals that her “misinformation report” was nothing more than a politically motivated censorship attempt.¹²²



¹²⁰ CENTER FOR INTERNET SEC., TERMS OF USE ELECTION INFRASTRUCTURE MISINFORMATION PORTAL, at 1–2 (2020) (on file with the Comm.).

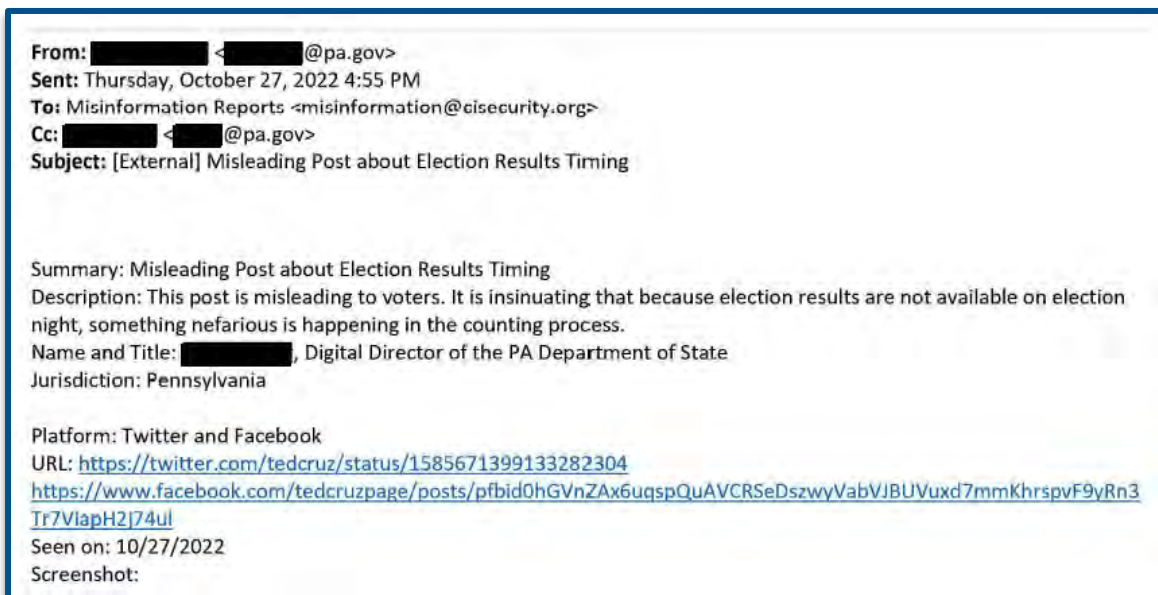
¹²¹ E-mail from Loudoun County government official to misinformation@cisecurity.org (Aug. 4, 2022, 4:57 PM) (on file with the Comm.).

¹²² *Id.*

The EI-ISAC then forwarded the report from the Loudoun County government to Twitter.¹²³



The CISA-funded EI-ISAC also facilitated a Democratic state government official’s attempt to censor core political speech by a sitting Republican U.S. Senator. As demonstrated below, a state government official working for Pennsylvania’s Secretary of State reported to the EI-ISAC posts on Twitter and Facebook from Senator Ted Cruz’s accounts,¹²⁴ in which Senator Cruz asked: “Why is it only Democrat blue cities that take ‘days’ to count their votes? The rest of the country manages to get it done on election night.”¹²⁵



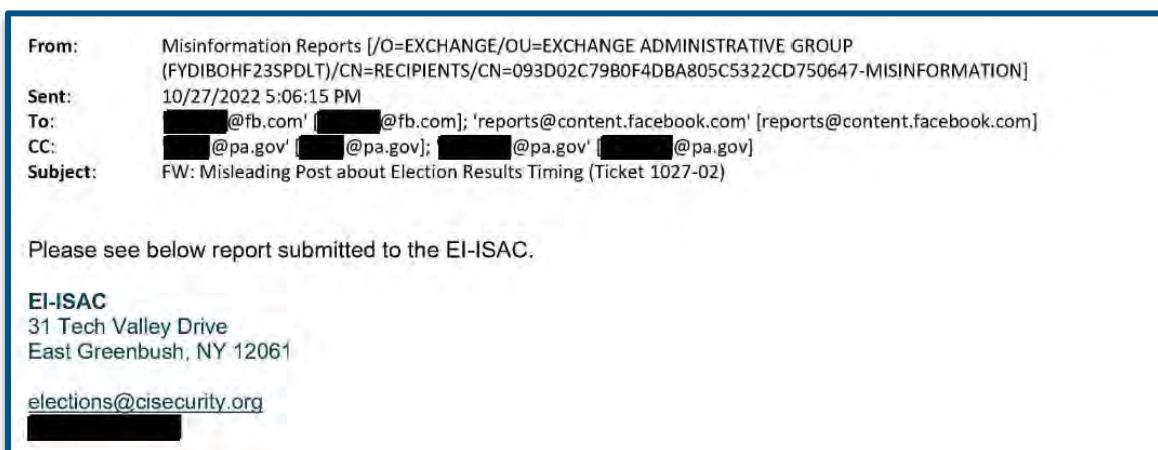
¹²³ E-mail from misinformation@cisecurity.org to Twitter employees (Aug. 18, 2022, 8:15 AM) (on file with the Comm.).

¹²⁴ E-mail from Pennsylvania state government official to misinformation@cisecurity.org (Oct. 27, 2022, 4:55 PM) (on file with the Comm.).

¹²⁵ Ted Cruz (@tedcruz), TWITTER (Oct. 27, 2022, 12:34 PM), <https://twitter.com/tedcruz/status/1585671399133282304>.



The EI-ISAC dutifully forwarded the report to Facebook.¹²⁶




¹²⁶ E-mail from misinformation@cisecurity.org to Meta employees (Oct. 27, 2022, 5:06 PM) (on file with the Comm.).

C. CISA admitted to outsourcing its surveillance operation to third parties

On numerous occasions, CISA officials and MDM Subcommittee members acknowledged, both implicitly and explicitly, that CISA was not authorized to conduct the kind of surveillance and censorship it was conducting. Instead of calling for an end to CISA’s unconstitutional activity, however, those involved routinely attempted to conceive methods by which CISA could surreptitiously outsource its surveillance and censorship to non-governmental third parties.

For example, during a March 15, 2022 meeting of the MDM Subcommittee, Starbird “asked what are, or what should be, the limitation of CISA’s work regarding monitoring, such as social media.”¹²⁷ Starbird then “addressed the highly limited scope for government in terms of social media monitoring . . . She also posed how CISA could work with or otherwise support external groups, such as researchers and non-profits, to support MDM response and how this work would be funded in the future.”¹²⁸ According to Starbird later in the meeting, “[t]hese limitations provide an opportunity for this subcommittee to inform gaps in this information.”¹²⁹



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

March 15, 2022

- Dr. Starbird identified the third MDM potential area as response and proposed monitoring, identifying, and responding to MDM threats including rumor control and election integrity partnerships. She asked what are, or what should be, the limitation of CISA’s work regarding monitoring, such as social media. She asked if rumor control should be a project within CISA and if so, what should it look like. She also posed how CISA could work with or otherwise support external groups, such as researchers and non-profits, to support MDM response and how this work would be funded in the future.

Twitter’s Chief Legal Officer, Vijaya Gadde, then “highlighted the many sensitivities, beyond legal ones, in terms of the relationship between social media companies and government concerning media monitoring and the perception this plays globally,” as well as the need to ensure that this government-social media relationship did not result in “any form of surveillance.”¹³⁰ Starbird responded that “this work should come from outside of government due to the sensitivities in this relationship.”¹³¹

- Ms. Gadde highlighted the many sensitivities, beyond legal ones, in terms of the relationship between social media companies and government concerning media monitoring and the perception this plays globally. She stressed that this is something we have to be very thoughtful about, as terms of services, use of APIs, etc. do not involve any form of surveillance. Dr. Starbird suggested that this work should come from outside of government due to the sensitivities in this relationship.

¹²⁷ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MARCH 15, 2022, at 2 (on file with the Comm.).

¹²⁸ *Id.*

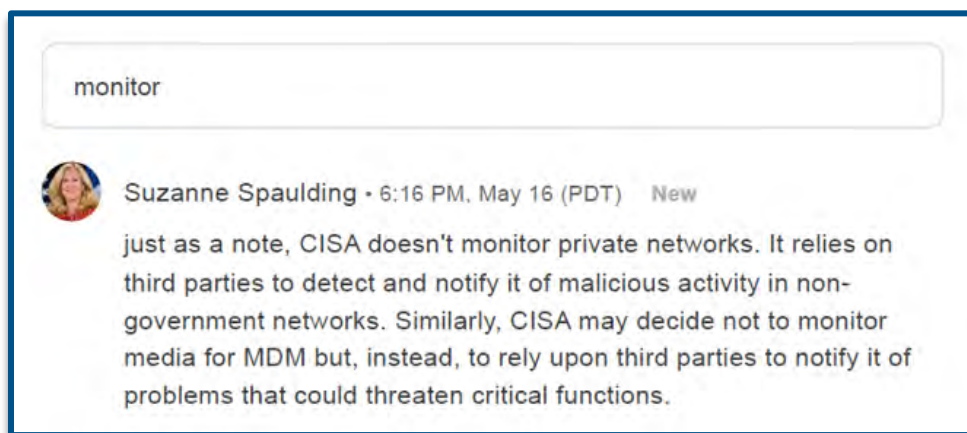
¹²⁹ *Id.*

¹³⁰ *Id.*

¹³¹ *Id.*

Rather than abandon the consideration of surveilling Americans, Starbird and Gadde attempted to find ways to circumvent the First Amendment’s strictures by outsourcing the “monitoring” activity from the government to private entities.

In the same March meeting, Spaulding warned that “the government cannot ask an outside party to do something the Intelligence Community cannot do.”¹³² But a few months later, MDM Subcommittee members were still considering how CISA could “rely upon third parties” rather than “monitor media for MDM” itself.¹³³ In the comments of an outline for the MDM Subcommittee’s June 2022 recommendations, Spaulding wrote, “[CISA] relies on third parties to detect and notify it of malicious activity in non-government networks. Similarly, CISA may decide not to monitor media for MDM but, instead, to rely upon third parties to notify it of problems.”¹³⁴



¹³² *Id.*

¹³³ E-mail from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.).

¹³⁴ *Id.*

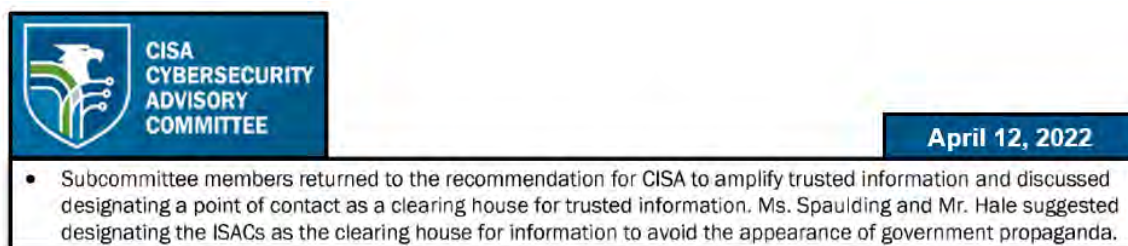
III. CISA has attempted to conceal its unconstitutional activities and remove evidence of wrongdoing

April and May 2022 were difficult months for the censorship regime. President Biden’s DHS announced the formation of the Disinformation Governance Board on April 27, 2022, but had to pause its work on May 18,¹³⁵ and subsequently disband it,¹³⁶ following severe public outcry.¹³⁷ On May 5, the Attorneys General of Missouri and Louisiana filed a federal lawsuit against the Biden Administration, including CISA, alleging government-induced viewpoint-based censorship.¹³⁸ This lawsuit would soon reveal, among other things, direct pressure from the Biden White House to social media companies to censor vaccine-skeptical content.¹³⁹

Meeting notes of the MDM Subcommittee from this period demonstrate that its members and CISA were fully aware of these developments and discussed how CISA could outsource its MDM-related activities to third parties so as to bypass the First Amendment and “avoid the appearance of government propaganda.”¹⁴⁰

A. Fearing public pressure and legal risks, CISA outsourced its censorship operation to the EI-ISAC

In addition to outsourcing its censorship operation to the EI-ISAC, an MDM Subcommittee member and CISA official also suggested laundering its messaging through the EI-ISAC, thereby making the EI-ISAC the mouthpiece for “trusted information.”¹⁴¹ During the April 12, 2022 MDM Subcommittee meeting, “Subcommittee members . . . discussed designating a point of contact as a clearing house for trusted information. Ms. Spaulding and Mr. Hale suggested designating the ISACs as the clearing house for information to avoid the appearance of government propaganda.”¹⁴²



On July 26, 2022, CISA’s Kim Wyman made a particularly forthright admission about CISA’s attempts to launder its censorship operation to outside parties. According to the meeting notes, Wyman was discussing CISA’s “switchboard function to alert a media platform if a mis-

¹³⁵ Beitsch, *supra* note 103.

¹³⁶ Dep’t of Homeland Sec., *supra* note 103.

¹³⁷ Sganga, *supra* note 103.

¹³⁸ Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 1 (Complaint).


¹³⁹ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Robert Flaherty (Jun. 23, 2023).

¹⁴⁰ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING APRIL 12, 2022, at 2 (on file with the Comm.).

¹⁴¹ *Id.*

¹⁴² *Id.*

or dis-information post is identified by another user.”¹⁴³ In that discussion, Wyman indicated that “CISA is currently transferring this work to the Information and Sharing and Analysis Centers (ISACs). She noted the concern over CISA operating this function given the current lawsuit filed by Louisiana and Missouri against CISA over perceived suppression of free speech.”¹⁴⁴




July 26, 2022

- Ms. Wyman shared concerns expressed by the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) since they were not consulted when the Subcommittee was drafting recommendations. She reviewed a sample of CISA’s work to deliver products to the elections community to include operating a switchboard function to alert a media platform if a mis- or dis-information post is identified by another user. CISA is currently transferring this work to the Information Sharing and Analysis Centers (ISACs). She noted the concern over CISA operating this function given the current lawsuit filed by Louisiana and Missouri against CISA over perceived suppression of free speech.

B. The MDM Subcommittee tried to disguise its recommendations by removing references to surveillance and censorship

Both CISA and its advisory subcommittee were keenly aware of and concerned about the political environment and legal risks that accompanied its surveillance and censorship activities. During the May 10, 2022 meeting of the MDM Subcommittee, “Dr. Starbird suggested refining the name of the subcommittee to ‘Informational Threats to Critical Infrastructure’ or ‘Informational Threats to Election Security’ so as not to conflate the group’s efforts with the work of the DHS Disinformation Governance Board.”¹⁴⁵ Twitter’s Gadde then “affirmed this [suggestion] and cautioned the group against pursuing any social listening recommendations for the CSAC June Quarterly Meeting.”¹⁴⁶



May 10, 2022

- Dr. Kate Starbird, Associate Professor, Human Centered Design & Engineering, University of Washington, MDM Subcommittee Chair, began the meeting by asking subcommittee members to discuss the announcement of the new DHS Disinformation Governance Board and the broader implications for this subcommittee.
 - Ms. Kim Wyman, Senior Election Security Lead, CISA, stressed that misinformation and disinformation are elevated to national awareness due to this board. Dr. Starbird suggested refining the name of the subcommittee to “Informational Threats to Critical Infrastructure” or “Informational Threats to Election Security” so as not to conflate the group’s efforts with the work of the DHS Disinformation Governance Board. Ms. Vijaya Gadde, Legal, Public Policy, and Trust and Safety Lead, Twitter, affirmed this and cautioned the group against pursuing any social listening recommendations for the CSAC June Quarterly Meeting.

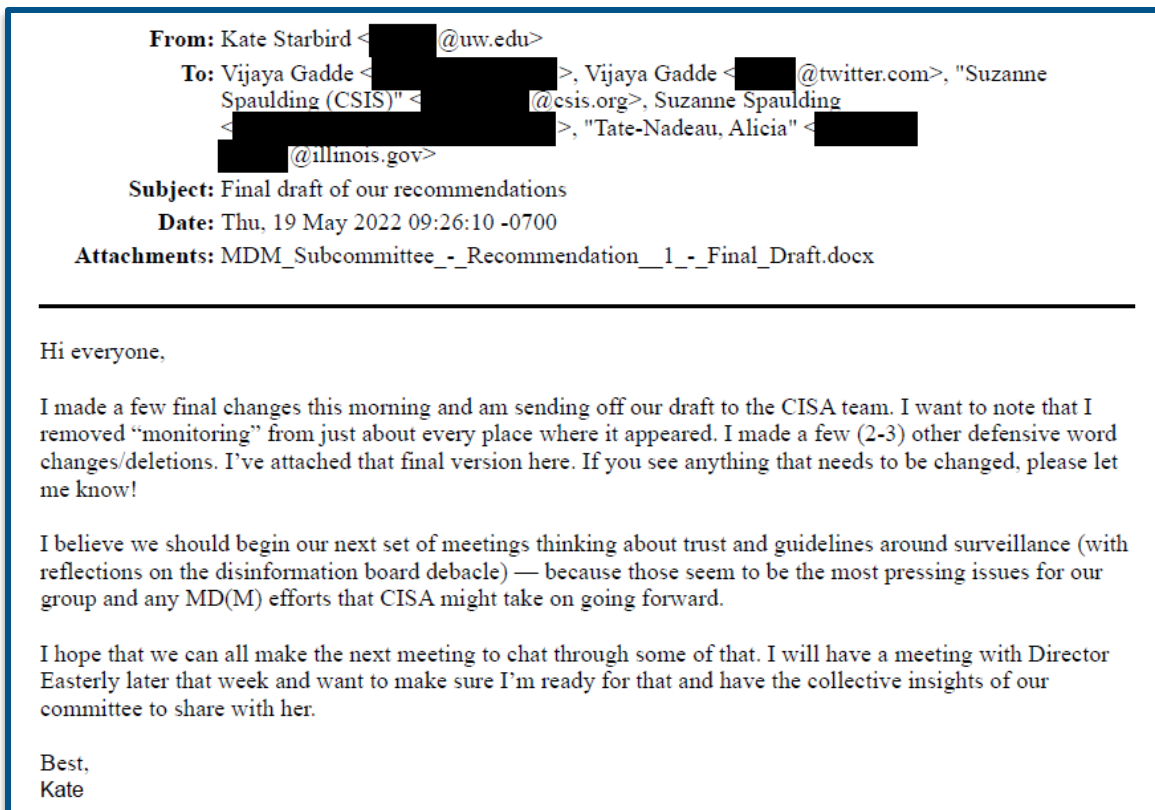
¹⁴³ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JULY 26, 2022, at 1 (on file with the Comm.).

¹⁴⁴ *Id.*

¹⁴⁵ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MAY 10, 2022, at 1 (on file with the Comm.).

¹⁴⁶ *Id.*

A little over a week later, on May 19, Starbird sent an e-mail to the other members of the MDM Subcommittee, writing: “I made a few final changes this morning and am sending off our draft [of the MDM Subcommittee’s June 2022 recommendations] to the CISA team. I want to note that I removed ‘monitoring’ from just about every place where it appeared.”¹⁴⁷



These attempts to disguise the true nature of counter-MDM work are emblematic of the tactics employed by academics “studying” disinformation. According to recent reporting by the *Washington Post*, in response to the Committee’s request for documents from Stanford University, “lawyers at the institution warned researchers to be more thoughtful about what they said in emails. ‘It makes me more careful in my communications with colleagues and collaborators,’ said professor Jeff Hancock, the faculty director of the Stanford Internet Observatory.”¹⁴⁸

C. CISA’s MDM advisors fretted that it was “only a matter of time before someone realizes we exist and starts asking about our work.”

On May 20, Spaulding sent an e-mail to Starbird expressing her concerns about growing public attention. In an e-mail, Spaulding wrote: “It’s only a matter of time before someone

¹⁴⁷ E-mail from Kate Starbird to Vijaya Gadde, Suzanne Spaulding, and Alicia Tate-Nadeau (May 19, 2022, 9:26 AM) (on file with the Comm.).

¹⁴⁸ Naomi Nix and Joseph Menn, *These academics studied falsehoods spread by Trump. Now the GOP wants answers*, WASHINGTON POST (Jun. 6, 2023).

realizes we exist and starts asking about our work. . . . I’m not sure this keeps until our public meeting in June.”¹⁴⁹

On May 20, 2022, at 7:27 AM, Suzanne Spaulding <[REDACTED]> wrote:

Kate,
 It's only a matter of time before someone realizes we exist and starts asking about our work. You may have already discussed this with Jen, but I'm wondering if we should try to find time to talk with CISA's comms and legislative folks about how we socialize what we're doing. It would be good to be proactive in telling our story rather than reacting to how someone else decides to portray it, right? And I'm not sure this keeps until our public meeting in June. I know neither of us has time for this, but I am telling myself that it might save us time in the long run!

best,
 Suzanne

Starbird responded to Spaulding, writing, “Yes. I agree. We have a couple of pretty obvious vulnerabilities.”¹⁵⁰


From: Kate Starbird [REDACTED]@uw.edu
Subject: Re: CSAC MDM Subcommittee Meeting
Date: May 20, 2022 at 7:37 AM
To: Suzanne Spaulding suzannespaulding10@gmail.com

KS

Yes. I agree. We have a couple of pretty obvious vulnerabilities. Do we want to meet prior to our Tues meeting or use that to start this conversation and make a plan? This is currently our singular topic for Tues. I'm supposed to meet with Jen later next week, but we haven't touched base on this yet.

Kate

During a May 24 meeting of the MDM Subcommittee, Starbird “restated the Subcommittee’s commitment to transparency but expressed concern for the Subcommittee’s efforts and cautioned the group on how to communicate their ongoing work.”¹⁵¹



May 24, 2022

- Dr. Kate Starbird, Associate Professor, Human Centered Design & Engineering, University of Washington, MDM Subcommittee Chair, discussed the Subcommittee’s recommendations to present during the CSAC June Quarterly Meeting and the path forward to strategically approach MDM in the government during the current discourse. Dr. Starbird restated the Subcommittee’s commitment to transparency but expressed concern for the Subcommittee’s efforts and cautioned the group on how to communicate their ongoing work.

¹⁴⁹ E-mail from Suzanne Spaulding to Kate Starbird (May 20, 2022, 7:27 AM) (on file with the Comm.).

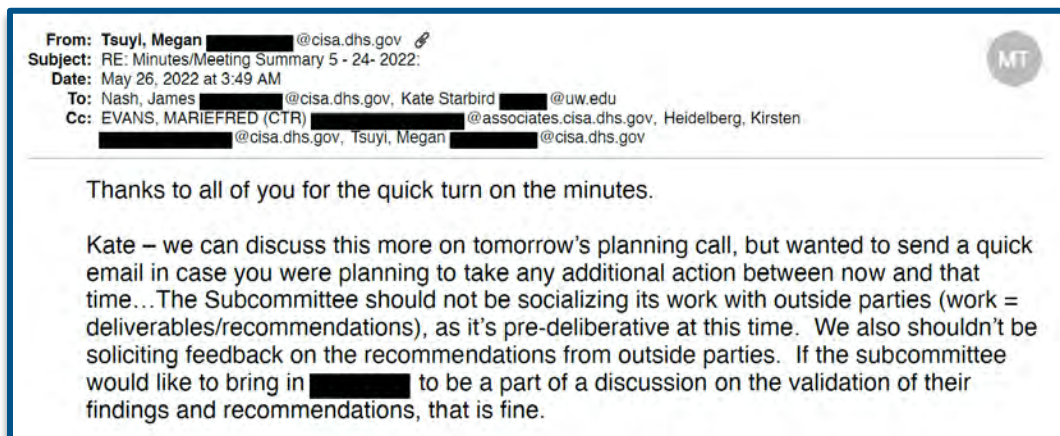
¹⁵⁰ E-mail from Kate Starbird to Suzanne Spaulding (May 20, 2022, 7:37 AM) (on file with the Comm.).

¹⁵¹ CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MAY 24, 2022, at 1 (on file with the Comm.).

In an apparent effort to conceal the full scope of CISA’s MDM-related efforts, Spaulding then “stressed that CISA should examine MDM beyond elections but suggested including in the recommendations that the Subcommittee is scoping their work around elections given the approaching election cycle.”¹⁵²

- Ms. Suzanne Spaulding, Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), suggested that the group recruit subject matter experts (SMEs) to support the Subcommittee’s efforts, solicit different perspectives, and apply credibility to the Subcommittee’s work with a broader audience. Ms. Spaulding offered an additional suggestion of asking Director Easterly for her perspective of socializing this Subcommittee’s work with Congress to prevent outside parties from being blindsided by their efforts. She further suggested the Subcommittee re-read and refine the recommendations and stressed that the safest ground in election is the recommendation for CISA to 1) point individuals to an authoritative source and 2) utilize their convening power. She stressed that CISA should examine MDM beyond elections, but suggested including in the recommendations that the Subcommittee is scoping their work around elections given the approaching election cycle. Ms. Spaulding offered an additional recommendation for CISA to scope their mission space to MDM that poses significant risk to national critical functions (NCFs).

Spaulding’s and others’ proposal to “socialize” the MDM Subcommittee’s work was met with resistance from CISA’s Megan Tsuyi, who told Starbird that “[t]he Subcommittee should not be socializing its work with outside parties . . . as it’s pre-deliberative at this time. We also shouldn’t be soliciting feedback on the recommendations from outside parties.”¹⁵³



D. CISA purged its website of references to domestic MDM and its First Amendment violations in response to public pressure

Following increased public awareness of CISA’s role in government-induced censorship and the Committee’s issuance of subpoenas to Alphabet, Amazon, Apple, Microsoft, and Meta in February 2023, CISA scrubbed its website of references to domestic MDM. Prior to the cleansing, the domain “CISA.gov/mdm” was associated with a webpage titled “Mis, Dis,

¹⁵² *Id.*

¹⁵³ E-mail from Megan Tsuyi to Kate Starbird and James Nash (May 26, 2022, 3:49 AM) (on file with the Comm.).

Malinformation,” as seen in the screenshot below, which shows the website as it appeared on February 12, 2023.¹⁵⁴

The screenshot shows the CISA website's 'MIS, DIS, MALINFORMATION' page. The header includes the CISA logo and navigation links for 'cisa.gov/uscert', 'Report Cyber Issue', and 'Subscribe to Alerts'. The main navigation bar lists categories: CYBERSECURITY, INFRASTRUCTURE SECURITY, EMERGENCY COMMUNICATIONS, NATIONAL RISK MANAGEMENT, ABOUT CISA, and MEDIA. The breadcrumb trail reads 'National Risk Management > Election Security > MDM'. The page title is 'MIS, DIS, MALINFORMATION'. A left sidebar under 'Election Security' lists: Election Cybersecurity Toolkit, Crossfeed, Election Risk Profile Tool, Election Security Library, MDM Resource Library, Mis-, Dis-, Malinformation (highlighted), Resilience Series Graphic Novels, and Rumor Control. The main content area includes a paragraph about CISA's MDM team, an 'ANNOUNCEMENT' section with expandable items like 'MDM Overview' and 'What is MDM?', and a search bar.

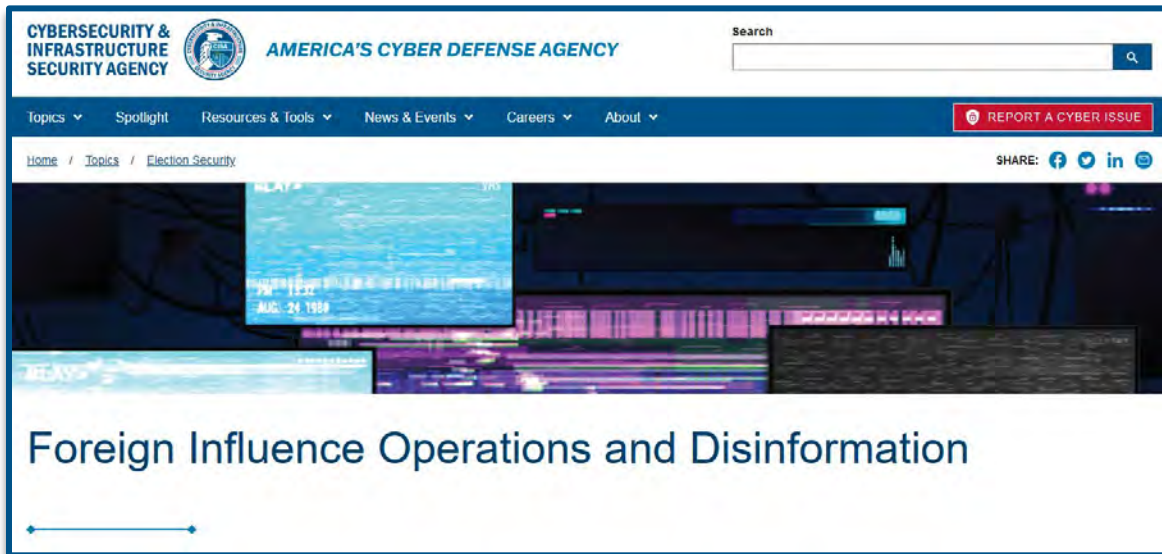
The website previously described the threats posed by both foreign and domestic MDM. For example, the section titled “What is MDM?” read, “Foreign *and domestic* threat actors use MDM campaigns to cause chaos, confusion, and division. These malign actors are seeking to interfere with and undermine our democratic institutions and national cohesiveness.”¹⁵⁵

The screenshot shows the 'What is MDM?' section. It defines Misinformation, Disinformation, and Malinformation. Misinformation is false but not intended to cause harm. Disinformation is deliberately created to mislead, harm, or manipulate. Malinformation is based on fact but used out of context to mislead, harm, or manipulate. The text states that foreign and domestic threat actors use MDM campaigns to cause chaos, confusion, and division, and that resources at the bottom of the page provide examples and more information.

¹⁵⁴ *Mis, Dis, Malinformation*, Cybersecurity and Infrastructure Sec. Agency, <https://cisa.gov/mdm> [<https://web.archive.org/web/20230215235115/https://www.cisa.gov/mdm>].

¹⁵⁵ *Id.* (emphasis added).

Now, the same URL redirects to a different page titled “Foreign Influence Operations and Disinformation,” which omits any reference to “domestic” MDM.¹⁵⁶



As reported by the Foundation for Freedom Online, “between Friday, Feb. 24 at 4:37 p.m. and Sunday, Feb. 26 at 5:55 am., CISA’s once loud-and-proud declaration of long-arm jurisdiction over domestic opinions online seems to have been walked back.”¹⁵⁷

E. The Biden Justice Department interfered with public records requests in order to shield CISA from public scrutiny of its unconstitutional practices

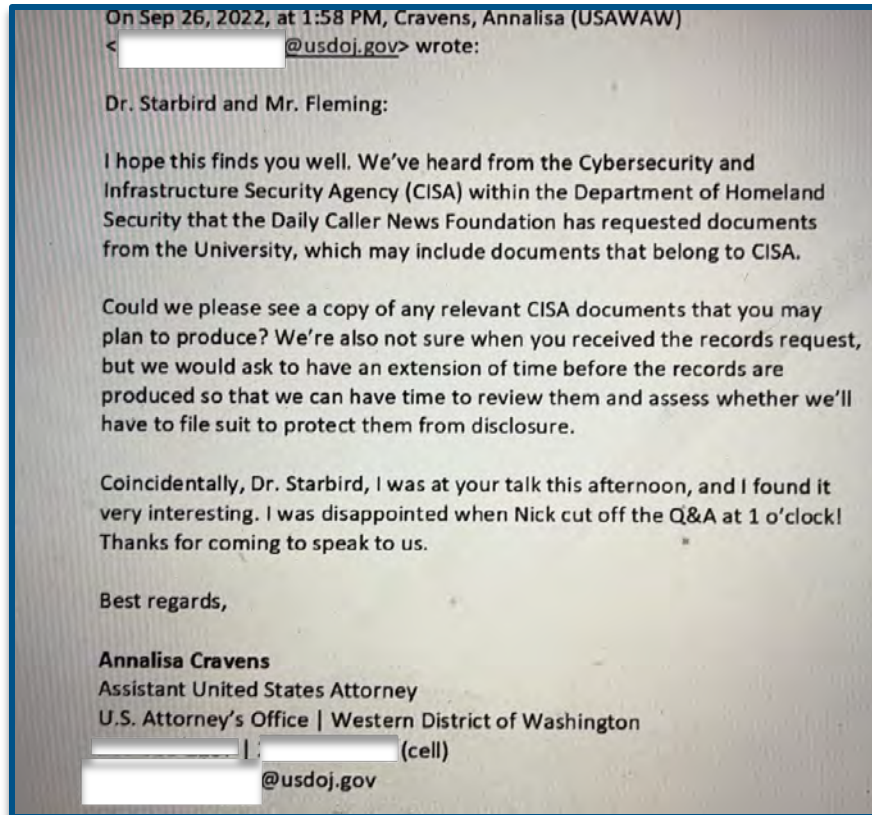
The effort to cover up CISA’s malfeasance appears to be a joint effort across the Biden Administration, according to recent reporting by journalist Lee Fang. In the fall of 2022, several non-profits and journalists, including Fang, individually submitted record requests to the University of Washington for material about Starbird’s work with CISA.¹⁵⁸ On September 26, 2022, Annalisa Cravens, an Assistant United States Attorney with the Department of Justice (DOJ), sent an e-mail to Starbird, writing, “Could we please see a copy of any relevant CISA documents that you may plan to produce? We’re also not sure when you received the records request, but we would ask to have an extension of time to review them and assess whether we’ll have to file suit to protect them from disclosure.”¹⁵⁹

¹⁵⁶ *Foreign Influence Operations and Disinformation*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation> (last visited Jun. 23, 2023).

¹⁵⁷ Mike Benz, *DHS Quietly Purges CISA “Mis, Dis and Malinformation” Website To Remove Domestic Censorship References*, FOUNDATION FOR FREEDOM ONLINE (Mar. 16, 2023), <https://foundationforfreedomonline.com/wp-content/uploads/2023/03/FFO-FLASH-REPORT.pdf>.

¹⁵⁸ Lee Fang, *Biden Justice Dept. Intervened to Block Release of Social Media Censorship Docs*, SUBSTACK (Jun. 6, 2023), <https://www.leefang.com/p/biden-justice-dept-intervened-to>.

¹⁵⁹ *Id.*



As Fang subsequently explained, “[t]he stalling effort highlights not only the broad authority that the federal government has to shape the political content available to the public, but also the toolkit that it relies upon to limit scrutiny of its involvement in the regulation of speech.”¹⁶⁰

¹⁶⁰ *Id.*

CONCLUSION

“Silencing those who disagree with us is a sign of weakness, not strength, and it won’t lead to progress.”
– former President Barack Obama, April 6, 2023.¹⁶¹

In 2019, CISA’s Chief Counsel claimed: “We are not law enforcement and we’re not the intelligence community.”¹⁶² In theory, the statement is accurate. CISA is not a law enforcement agency and is not authorized to act as an intelligence agency. But, in practice, that is how CISA has behaved, arrogating to itself the authority to conduct surveillance of Americans on social media. CISA expanded its unconstitutional practice by developing an elaborate social media censorship apparatus spanning multiple organizations, in order to facilitate the censorship of Americans’ political speech both directly and by proxy. There is no constitutionally viable legal authority that allows CISA to engage in this or any other kind of censorship. Thus, not only does CISA’s conduct violate the First Amendment, it also disregards the basic principle of the separation of powers, which prohibits agencies from acting outside of their congressionally delegated sphere.¹⁶³

As Suzanne Spaulding, the former CIA legal advisor and MDM Subcommittee member, presaged, it was “only a matter of time before someone realizes we exist and starts asking about”¹⁶⁴ CISA’s repeated violations of the First Amendment. CISA’s attempts to cover up its surveillance and censorship operations will not rectify the damage inflicted on the American people by government-induced censorship. Neither CISA’s scrubbing of its website, nor the Biden Administration’s stalling of records requests can conceal the true nature of CISA’s work in “combating MDM.”

CISA must be reined in, as must the Biden Administration’s “whole-of-government” approach to social media censorship. Every American has the right to express his or her opinion online, and to receive information from others. Government classifications of opinions as “misinformation” or “disinformation” do not nullify the First Amendment’s guarantees. A free and democratic society is impossible under a government that acts as the ultimate arbiter of truth in political discourse. To better inform legislative efforts to end government censorship on the Internet and protect Americans’ rights guaranteed by the First Amendment, the Committee and Select Subcommittee will continue to investigate the extent of CISA’s and other Executive Branch agencies’ interactions with social media platforms.

¹⁶¹ Barack Obama (@BarackObama), TWITTER (Apr. 6, 2023, 10:20 PM), <https://twitter.com/BarackObama/status/1644163255189774337>.

¹⁶² *CISA and Cyber Threats: How Government and Private Sector Secure Our Networks and Infrastructure*, *supra* note 28.

¹⁶³ *Am. Hosp. Ass’n v. Azar*, 410 F. Supp. 3d 142, 151 (D.D.C. 2019) (“[A]gency actions beyond delegated authority are *ultra vires* and should be invalidated.”).

¹⁶⁴ E-mail from Suzanne Spaulding to Kate Starbird (May 20, 2022, 7:27 AM) (on file with the Comm.).



**THE WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION:
HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO
CENSOR ONLINE SPEECH “AT SCALE” AND TRYING TO COVER UP ITS
ACTIONS**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



February 5, 2024

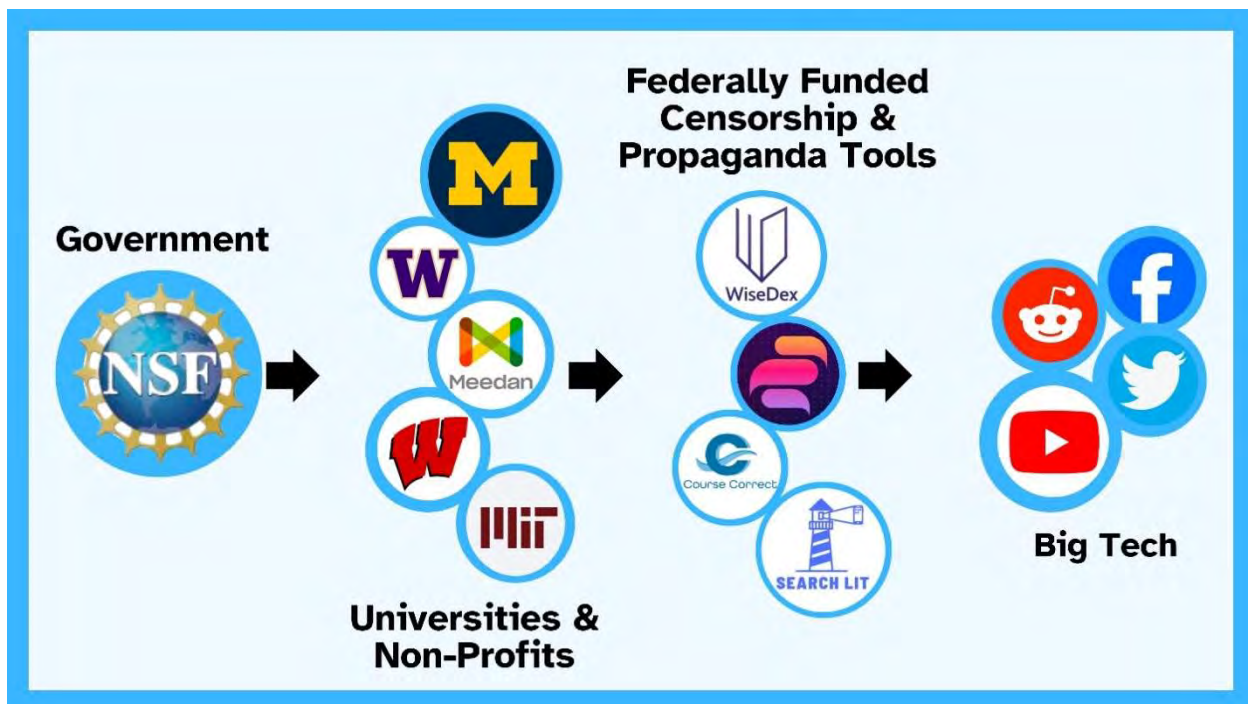
EXECUTIVE SUMMARY

“Our misinformation service helps policy makers at platforms who want to . . . push responsibility for difficult judgments to someone outside the company . . . by *externalizing the difficult responsibility of censorship.*”

– Speaker’s notes from the University of Michigan’s first pitch to the National Science Foundation (NSF) about its NSF-funded, AI-powered WiseDex tool.¹

This interim report details the National Science Foundation’s (NSF) funding of AI-powered censorship and propaganda tools, and its repeated efforts to hide its actions and avoid political and media scrutiny.

In the name of combatting alleged misinformation regarding COVID-19 and the 2020 election, NSF has been issuing multi-million-dollar grants to university and non-profit research teams. The purpose of these taxpayer-funded projects is to develop artificial intelligence (AI)-powered censorship and propaganda tools that can be used by governments and Big Tech to shape public opinion by restricting certain viewpoints or promoting others.



Non-public documents obtained by the House Judiciary Committee and the Select Subcommittee on the Weaponization of the Federal Government demonstrate that these federal bureaucrats, “disinformation” researchers, and non-profit groups understood that their actions—

¹ The University of Michigan’s WiseDex First Pitch Slide Deck entitled “Team469_First Pitch_10.27.2021.pptx” attached to an email from James Park to Michael Pozmantier (Oct. 26, 2021, 10:38 PM), at 1 (on file with the Comm.) (emphasis added).

“content moderation” and combatting so-called misinformation—amounted to “censorship.”² And yet, NSF forged ahead, supporting new technologies that would essentially enable the censorship of online speech “at scale.”

But NSF’s taxpayer funding for this potential automated censorship is only half of the story. The Committee and the Select Subcommittee have also obtained, via document requests and subpoenas, nonpublic emails and other documents that reveal a years-long, intentional effort by NSF to hide its role in funding these censorship and propaganda tools from media and political scrutiny. From legal scholars, such as Jonathan Turley, to conservative journalists, NSF tracked public criticisms of its work in funding these projects. NSF went so far as to develop a media strategy that considered blacklisting certain American media outlets because they were scrutinizing NSF’s funding of censorship and propaganda tools.

The First Amendment prohibits the government from “*abridging* the freedom of speech.”³ Thus, “any law or government policy that reduces that freedom on the [social media] platforms . . . violates the First Amendment.”⁴ To inform potential legislation, the Committee and Select Subcommittee have been investigating the Executive Branch’s collusion with third-party intermediaries, including universities, non-profits, and businesses, to censor protected speech on social media. The Committee and Subcommittee have uncovered serious violations of the First Amendment throughout the Executive Branch, including:

- The Biden White House directly coercing large social media companies, such as Facebook, to censor true information, memes, and satire, eventually leading Facebook to change its content moderation policies;⁵
- Stanford’s Election Integrity Partnership (EIP)—created at the request of the Department of Homeland Security’s (DHS) Cybersecurity & Infrastructure Security Agency (CISA)—working with the federal government to flag thousands of links and submit recommendations directly to large social media platforms to censor Americans’ online speech in the lead-up to the 2020 U.S. election;⁶ and

² *Id.*

³ U.S. Const. amend. I (emphasis added).

⁴ Philip Hamburger, *How the Government Justifies Its Social-Media Censorship*, WALL ST. J. (June 9, 2023); see *Smith v. California*, 361 U.S. 147, 157 (1959) (Black, J., concurring) (“Certainly the First Amendment’s language leaves no room for inference that abridgments of speech and press can be made just because they are slight.”).

⁵ See Jim Jordan (@Jim_Jordan), X, (July 27, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684595375875760128; Jim Jordan (@Jim_Jordan), X, (July 28, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684957660515328001; Jim Jordan (@Jim_Jordan), X, (Aug. 3, 2023, 11:00 AM), https://twitter.com/Jim_Jordan/status/1687116316073930752; Jim Jordan (@Jim_Jordan), X, (Sept. 5, 2023, 6:17 PM), https://twitter.com/Jim_Jordan/status/1699184930331267539; Jim Jordan (@Jim_Jordan), X, (Nov. 30, 2023, 8:44 AM), https://twitter.com/Jim_Jordan/status/1730221179632226337; Jim Jordan (@Jim_Jordan), X, (Dec. 1, 2023, 2:26 PM) https://twitter.com/Jim_Jordan/status/1730669728002142706; see also Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

⁶ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023); see also STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

- The Federal Trade Commission (FTC) harassing Elon Musk’s Twitter (now X) because of Musk’s commitment to free speech, even going so far as to target certain journalists by name.⁷

As egregious as these violations of the First Amendment are, each still faced the same limitation: the censors were *human*. Senior Biden White House officials had to spend time personally berating the social media companies into changing their content moderation policies. Social media executives expended considerable time and effort responding to the White House’s threats and evaluating the flagged content. Stanford had nearly a hundred people working for the EIP in shifts flagging thousands of posts, which was only a fraction of the number of election-related posts made in the fall of 2020.⁸

But what happens if the censorship is automated and the censors are machines? There is no need for shifts or huge teams of people to identify and flag problematic online speech. AI-driven tools can monitor online speech at a scale that would far outmatch even the largest team of “disinformation” bureaucrats and researchers. This interim report reveals how NSF is using American taxpayer dollars to fund the tools that could usher in an even greater threat to online speech than the original efforts to censor speech on social media. The NSF-funded projects threaten to help create a censorship regime that could significantly impede the fundamental First Amendment rights of millions of Americans, and potentially do so in a manner that is instantaneous and largely invisible to its victims.

The Committee and the Select Subcommittee are responsible for investigating “violation[s] of the civil liberties of citizens of the United States.”⁹ In accordance with this mandate, this interim staff report on NSF’s violations of the First Amendment and other unconstitutional activities fulfills the obligation to identify and report on the weaponization of the federal government against American citizens. The Committee’s and Select Subcommittee’s investigation remains ongoing. NSF still has not adequately complied with a request for relevant documents, and more fact-finding is necessary. In order to better inform the Committee’s legislative efforts, the Committee and Select Subcommittee will continue to investigate how the Executive Branch worked with social media platforms and other intermediaries to censor disfavored viewpoints in violation of the U.S. Constitution.

⁷ Ryan Tracy, *FTC Twitter Investigation Sought Elon Musk’s Internal Communications, Journalist Names*, WALL ST. J. (Mar. 8, 2023); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *FIGHTING THE WEAPONIZATION OF THE INTERNAL REVENUE SERVICE: THE END OF ABUSIVE UNANNOUNCED FIELD VISITS* (Comm. Print Oct. 27, 2023).

⁸ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH* (Comm. Print Nov. 6, 2023), at 39.

⁹ H. Res. 12 § 1(b)(E).

 TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS	4
I. THE HISTORICAL LIMITS OF HUMAN CENSORSHIP	5
II. THE FEDERAL GOVERNMENT IS FUNDING AI-POWERED CENSORSHIP TOOLS	7
A. Government Censorship Has Extended to the West, including the United States.....	8
B. Free Speech Advocates Have Sounded the Alarm Regarding How Artificial Intelligence Can Lead to Censorship “At Scale”	9
C. The National Science Foundation’s Funding of Censorship Tools	10
1. The National Science Foundation.....	10
2. NSF’s Convergence Accelerator Program.....	11
3. NSF’s Track F: The Censorship Program.....	11
D. Censorship and Propaganda in Action: Universities and Non-Profits Develop AI Tools and Other New Technologies to Censor at Scale with Help of Federal Funding	13
1. The University of Michigan: WiseDex.....	14
2. Meedan: Co-Insights.....	16
3. The University of Wisconsin: CourseCorrect.....	21
4. MIT: Search Lit.....	21
III. THE FEDERALLY FUNDED CENSORS: PARTISAN AND CONDESCENDING.....	22
A. In Their Own Words, “Disinformation” Pseudo-Scientists Describe Their Work As “Political” and “Censorship”	23
B. NSF-Funded Researchers Believe the American Public is Not Smart Enough to Discern Fact from Fiction, Especially Conservatives, Minorities, and Veterans.....	25
C. NSF-Funded Researchers Understand the Leverage They Have Over Social Media Companies to Ensure the Platforms Bow to Their Demands	26
IV. NSF IS TRYING TO COVER UP ITS FUNDING OF AI CENSORSHIP.....	28
A. NSF Developed an Official Media Strategy to Hide its Track F Censorship Program from the American People.....	28
B. NSF Considered Blacklisting Conservative Media Outlets.....	32
C. NSF Attempted to Hide Additional Funding to Its Track F Censorship Program.....	33
D. NSF Continues to Try to Cover Up Its Funding of Censorship Tools.....	34
E. NSF Is Attempting to Stonewall Congressional Investigations.....	38
V. The Role of Congress: Defund the Censorship-Industrial Complex and Fight the Next Battle to Defend Free Speech	38
APPENDIX A: LETTER FROM THE NATIONAL SCIENCE FOUNDATION DIRECTOR SETHURAMAN PANCHANATHAN TO REP. JIM JORDAN, CHAIRMAN OF HOUSE COMM. ON JUDICIARY COMMITTEE (JUNE 13, 2023).	
APPENDIX B: NSF’S “TRACK F MEDIA STRATEGY” DOCUMENT (NOV. 22, 2021).	
APPENDIX C: THE UNIVERSITY OF MICHIGAN’S WISEDEX FIRST PITCH SLIDE DECK (OCT. 26, 2021).	
APPENDIX D: MIT’S SEARCH LIT PHASE I PROPOSAL TO NSF (2021).	

I. THE HISTORICAL LIMITS OF HUMAN CENSORSHIP

“For if Men are to be precluded from offering their Sentiments on a matter, which may involve the most serious and alarming consequences, that can invite the consideration of Mankind, reason is of no use to us; the freedom of Speech may be taken away, and, dumb and silent we may be led, like sheep, to the Slaughter.”

– George Washington’s *Newburg Address to Officers of the Army*, March 15, 1783

The Committee and Select Subcommittee are investigating how and to what extent the federal government coerced or colluded with social media companies and other third parties to censor Americans’ speech online. Although the medium—social media—is relatively new, the broader fight against government-issued or -directed restrictions on speech is not.

New technologies, from the printing press to the Internet, enabled more people to share their views more widely. These developments hindered governments’ ability to restrict the flow of new ideas, including those that criticize the government. The promise of the Internet, and social media in particular, was to democratize speech at an unprecedented scale. More recently, social media has been credited—or blamed—with political outcomes that reflected the will of the public, rather than the establishment, such as the election of President Donald Trump in 2016 and the “Brexit” vote in 2017.¹⁰

The backlash from the establishment against social media was quick, severe, and thorough. In the United States, Democrats threatened repeatedly to break up American social media companies.¹¹ Federal law enforcement, intelligence, and other agencies all began creating and expanding offices, task forces, and boards designed to fight against so-called mis-, dis-, and malinformation.¹² The last of these—“malinformation”—is particularly pernicious and paternalistic: the U.S. government uses this term to refer to information that is true, but lacks adequate context, at least according to the government.¹³ Academics across the country, often

¹⁰ See, e.g., Issie Lapowsky, *Here's How Facebook Actually Won Trump the Presidency*, WIRED (Nov. 15, 2016); Maya Kosoff, *How Facebook and Twitter Quietly Helped Trump Win*, VANITY FAIR (Oct. 26, 2017); Dr. Richard Fletcher and Meera Selva, *How Brexit referendum voters use news*, REUTERS INSTITUTE (Nov. 25, 2019).

¹¹ See, e.g., Marcy Gordon, *Democrats call for Congress to rein in, break up Big Tech*, AP (Oct. 6, 2020); see also *Missouri v. Biden*, 2023 WL 4335270, at *4, *47 (W.D. La. July 4, 2023); House Judiciary Committee’s Transcribed Interview of Alex Stamos (June 23, 2023), at 187-188 (on file with the Comm.).

¹² See Ken Klippenstein, *The Government Created A New Disinformation Office to Oversee All the Other Ones*, THE INTERCEPT (May 5, 2023) (“Within the federal government, offices dedicated to fighting foreign disinformation are springing up like daisies, from the Pentagon’s new Influence and Perception Management Office to at least four organizations inside the Department of Homeland Security alone, as well as ones inside the FBI and State Department. To oversee the growing efforts — which arose in response to concerns about the impact of Russian meddling in the 2016 election but have now expanded — the director of national intelligence has created a new office.”); see also STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023).

¹³ CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *MIS-, DIS-, AND MALINFORMATION PLANNING AND INCIDENT RESPONSE GUIDE FOR ELECTION OFFICIALS*, at 1 (2022), https://www.cisa.gov/sites/default/files/2022-11/mdm-incident-response-guide_508.pdf; see also STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE

with taxpayer dollars, began researching the pseudo-science of “disinformation.”¹⁴ The zealous overreaction in America to the dangers of “unfettered speech” online is to say nothing of what happened in Europe and elsewhere.¹⁵

Though these developments were expansive and troubling, there was an inherent constraint on all of them: manpower. To be sure, there has been no shortage of bureaucrats, massive “trust and safety” teams at Big Tech, and countless researchers and academics looking to cash in on the growing “censorship industrial complex.”¹⁶ But each of these segments in the censorship regime lamented the shortcomings they faced with the enormous scale of speech that is shared on social media.

For example, Brian Scully, the head of the Cybersecurity and Infrastructure Security Agency’s (CISA) “Mis-, Dis-, and Malinformation” team testified that CISA’s “switchboarding” process—whereby CISA officials received alleged “misinformation” reports from election officials and transmitted those reports to social media companies so that they could take enforcement measures against the reported content—was “resource intensive.”¹⁷ After engaging in the effort for the 2018 and 2020 election cycles, CISA discontinued the practice in 2022.¹⁸

In a similar vein, the Twitter Files revealed that the people on the receiving end of these requests—the various “trust and safety teams” at Big Tech—often felt overwhelmed. For example, in the days leading up to the 2020 U.S. election, Twitter personnel had discussions about how to handle the “backlog” of incoming requests and how to best “prioritize” them.¹⁹ Government-funded third parties, such as the Center for Internet Security (CIS), offered to create “misinformation portals” for social media companies to better facilitate these types of requests.²⁰

FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS, at 10 (Comm. Print June 26, 2023).

¹⁴ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023); *but see* Naomi Nix et al., *Misinformation research is buckling under GOP legal attacks*, WASH. POST (Sept. 23, 2023).

¹⁵ *See Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (statement of Rupa Subramanya); *see also* Dave Davies, *Unfettered Free Speech Is A Threat To Democracy, Journalist Says*, NPR (Oct. 20, 2020).

¹⁶ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 9, 2023) (statements of Matt Taibbi and Michael Shellenberger).

¹⁷ Scully Dep. 17:1–18:1, *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 209.

¹⁸ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

¹⁹ *See, e.g.*, Matt Taibbi (@mtaibbi) X, (Dec. 24, 2022, 12:20 PM) <https://twitter.com/mtaibbi/status/160670144899333253>.

²⁰ *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

Likewise, academics, even when supported by the federal government, could only monitor and report so much content at a time. For example, the Election Integrity Partnership (EIP) had nearly 100 people (plus over a dozen external stakeholders), working in shifts to monitor and report thousands of social media posts by Americans in the lead-up to the 2020 election.²¹ All told, the EIP submitted over 400 misinformation reports, flagging thousands of posts with specific recommendations sent directly to Facebook, Twitter, YouTube, TikTok, and other social media platforms.²² Although any violation of the First Amendment is alarming, the EIP’s efforts led to only *thousands* of Americans’ posts being targeted; new technologies could enable a much smaller team to accomplish the same task for *millions* of posts, if not entire narratives.

II. THE FEDERAL GOVERNMENT IS FUNDING AI-POWERED CENSORSHIP TOOLS

“Across the world right now, governments, in the name of the good, are considering or adopting measures like we have in Canada. In Dublin, they’re about to enact a draconian hate-crime bill that poses a dire threat to free speech. In Paris, President Emanuel Macron has called for censoring online speech. In Brussels, the EU’s Internal Market Commissioner is calling for a crackdown on “illegal content.” In Brasilia, they’re fighting “fake news” and “disinformation” by clamping down on legitimate online speech. To say nothing of Russia and China and Iran. America is so exceptional—indispensable really. Please do not succumb to the same illiberal, the same authoritarianism. Please keep fighting for what you know is right. Canada is watching. The *whole world* is watching.”²³

– Rupa Subramanya, Canadian journalist, testifying before the Select Subcommittee, November 30, 2023

With the development of artificial intelligence and machine learning, governments are recognizing that censorship of speech online has the potential to be automated. Already, authoritarian governments such as China and Russia have used AI tools to surveil their citizens’ speech on the Internet.²⁴ In the West, including the United States, government, researchers, and non-profits are seeking to develop similar tools to monitor and censor speech “at scale” in the name of combatting so-called misinformation.

²¹ *Id.*

²² *Id.*; see also *id.* App’x II.

²³ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (statement of Rupa Subramanya).

²⁴ See, e.g., Dasha Litvinova, *The Cyber Gulag: How Russia Tracks, Censor and Controls its Citizens*, AP (May 23, 2023); Sarah Cook, *China’s Censors Could Shape the Future of AI-Generated Content*, THE JAPAN TIMES (Feb. 27, 2023); Eduardo Baptista, *China Deletes 1.4 Million Social Media Posts in Crackdown on ‘Self-Media’ Accounts*, REUTERS (May 27, 2023).

A. Government Censorship Has Extended to the West, including the United States

The Internet, and later social media, came with the promise of democratizing speech. However, authoritarian governments quickly showed that the Internet does not prevent powerful governments from censoring disfavored viewpoints. For example, citizens in China and Vietnam have been criminally convicted for criticizing how their country handled the COVID-19 pandemic.²⁵

Anti-free speech legislation has since spread to the Western world as well. As the Canadian journalist Rupa Subramanya testified before the Select Subcommittee on the Weaponization of the Federal Government in November 2023, Canada, the United Kingdom, Ireland, and other Western liberal democracies have been enacting measures that crack down on speech.²⁶ In the United Kingdom, a man went to jail for tweeting a joke in poor taste.²⁷ In Canada, doctors face persecution if they question the country's response to the COVID lockdowns or disagree about the safety of COVID vaccines.²⁸

The censorship of speech has extended into financial surveillance and de-banking. The Canadian government froze Canadian citizens' bank accounts simply for protesting vaccine mandates and draconian lockdowns.²⁹ A federal court in Canada recently found the government's invocation of emergency powers to crack down on these protestors to be unreasonable, but the chilling effect of this government overreach remains.³⁰

The Committee and Select Subcommittee have revealed how, in the United States, the federal government solicited banks to turn over information on their customers about whether they shopped at stores such as Bass Pro Shops or purchased firearms.³¹ Documents obtained by the Committee and Select Subcommittee suggest that after January 6, 2021, the Treasury Department's Office of Stakeholder Integration and Engagement in the Strategic Operations of the Financial Crimes Enforcement Network (FinCEN) provided banks with "suggested search terms and Merchant Category Codes for identifying transactions on behalf of federal law enforcement."³²

²⁵ See, e.g., Jason Nguyen, *How Vietnam Utilizes "Fake News" Accusations To Justify Digital Repression*, THE VIETNAMESE (Sept. 20, 2022); *China Jails Citizen Journalists who Reported on COVID-19*, INTERNATIONAL PRESS INSTITUTE (Dec. 28, 2020).

²⁶ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (statement of Rupa Subramanya).

²⁷ See, e.g., Owen Bowcott, *Twitter Joke Trial Became Confrontation with Judicial Establishment*, THE GUARDIAN (July 27, 2012).

²⁸ Sharon Kirkey, *Ontario Doctors Give Up Licences After Complaints Over COVID Vaccine Exemptions, Misinformation*, NATIONAL POST (Apr. 18, 2023); see also Shawn Knox, *10/3 podcast: Jordan Peterson Willing to Risk License Over Social Media Training*, NATIONAL POST (Jan. 24, 2024).

²⁹ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (statement of Rupa Subramanya).

³⁰ Rob Gillies, *Judge says Canada's use of Emergencies Act to quell truckers' protests over COVID was unreasonable*, AP (Jan. 23, 2024).

³¹ Brooke Singman, *'Alarming' Surveillance: Feds Asked Banks to Search Private Transactions for Terms Like 'MAGA,' 'Trump'*, H. JUD. COMM. (Jan. 17, 2024).

³² *Id.*

B. Free Speech Advocates Have Sounded the Alarm Regarding How Artificial Intelligence Can Lead to Censorship “At Scale”

As artificial intelligence has grown and developed, so too have concerns about its impact on free expression. Today, a growing number of voices are sounding the alarm on AI’s potential to infringe on Americans’ civil liberties.

Authoritarian governments, such as China and Russia, restrict what their citizens can say and what journalists can report.³³ But more alarmingly, the threats to free speech have extended to Western liberal democracies as well.

In July 2023, tech billionaire and AI entrepreneur Elon Musk founded “xAI” and, in November 2023, unveiled “Grok,” an AI chatbot trained using real-time data from the social media platform X, which Musk now owns.³⁴ Musk introduced Grok as an alternative to OpenAI’s “woke” ChatGPT and has been outspoken about the risks associated with AI’s development and the need for AI regulation.³⁵ He has also expressed concern over President Biden’s October 2023 AI executive order that pushes the Administration’s radical social “equity” agenda in the name of addressing “algorithmic discrimination.”³⁶

In December 2022, Marc Andreessen, a co-author of Mosaic and co-founder of Netscape, warned that the “level of censorship pressure that’s coming for AI and the resulting backlash will define the next century of civilization.”³⁷ In June 2023, Andreessen wrote, “Why AI Will Save the World,” declaring that AI could be “a way to make everything we care about better,” but also advised that the AI censorship fight is “more important – by a *lot*” than the fight against censorship on social media.³⁸ He explained:

AI is highly likely to be the control layer for everything in the world. How it is allowed to operate is going to matter perhaps more than anything else has ever mattered. You should be aware of how a small and isolated coterie of partisan social engineers are trying to determine that right now, under cover of the age-old claim that they are protecting you.³⁹

³³ See, e.g., Sarah Cook, *China’s Censors Could Shape the Future of AI-Generated Content*, THE JAPAN TIMES (Feb. 27, 2023); Eduardo Baptista, *China Deletes 1.4 Million Social Media Posts in Crackdown on ‘Self-Media’ Accounts*, REUTERS (May 27, 2023); Dasha Litvinova, *The Cyber Gulag: How Russia Tracks, Censor and Controls its Citizens*, AP (May 23, 2023).

³⁴ Jay Peters and Emma Roth, *Elon Musk’s new xAI company launches to ‘understand the true nature of the universe’*, THE VERGE (July 12, 2023).

³⁵ Kelby Vera, *Elon Musk Unveils ‘Grok’ AI Chatbot As Alternative To ‘Woke’ Rivals Like ChatGPT*, HUFF. POST (Nov. 6, 2023); Aaron Kliegman, *Biden administration pushing to make AI woke, adhere to far-left agenda: watchdog*, FOX NEWS (July 3, 2023); James Clayton, *‘Overwhelming consensus’ on AI regulation – Musk*, BBC (Sept. 13, 2023).

³⁶ Rounak Jain, *‘Uh Oh’, Says Elon Musk On President Biden Requiring AI Companies To ‘Address Algorithmic Discrimination’*, BENZINGA (Oct. 31, 2023).

³⁷ Marc Andreessen (@pmarca), X (Dec. 4, 2022, 7:05 PM), <https://twitter.com/pmarca/status/1599555565482823680>.

³⁸ Marc Andreessen, *Why AI Will Save the World*, ANDREESEN HOROWITZ (June 6, 2023).

³⁹ *Id.*

Legal scholars have been warning of the First Amendment implications of AI-powered content moderation.⁴⁰ Legislators have been considering and introducing legislation that would protect against AI-driven censorship of online speech, such as bills that would prevent taxpayer dollars from going to programs using AI to “help label, suppress, and censor speech online.”⁴¹

C. The National Science Foundation’s Funding of Censorship Tools

As the distributor of multi-million-dollar grants, the National Science Foundation (NSF) is a key player in the “censorship industrial complex.” In recent years, under the guise of combatting so-called misinformation, NSF has been funding AI-driven tools and other new technologies that can be used to censor or propagandize online speech.

1. The National Science Foundation

In 1950, Congress established NSF as an independent federal agency tasked with “keeping the U.S. at the leading edge of discovery in science and engineering,” primarily by making grants.⁴² Today, NSF has an annual budget of nearly \$10 billion, over 1,500 federal employees, and 200 scientists from research institutions, issuing, on average, 12,000 awards to 2,000 grantees per year and providing about 25 percent of federal funding to America’s colleges and universities for basic research.⁴³ Over the past two fiscal years, NSF has allocated approximately \$8 billion each in both FY 2021 and FY 2022.⁴⁴

The scope of NSF’s mission has shifted over the years to encompass social and behavioral sciences. For example, NSF used to fund political science projects from the 1960s until 2012, when Congress banned such research from receiving NSF funding.⁴⁵ However, in recent years, and after the academic outcry that Americans elected President Trump only because of “Russian disinformation,” NSF has spent millions of taxpayer dollars funding projects to combat alleged mis- and disinformation.⁴⁶

⁴⁰ See, e.g., Jonathan Turley, *Bill Gates, elites want to use AI to censor political opponents*, N.Y. POST (Feb. 14, 2023); *Artificial intelligence, free speech, and the First Amendment*, FIRE, <https://www.thefire.org/research-learn/artificial-intelligence-free-speech-and-first-amendment> (last visited Feb. 4, 2024).

⁴¹ Elizabeth Elkind, *GOP lawmaker aims to cut US taxpayer dollars from United Nations 'censorship' program*, FOX NEWS (Sept. 18, 2023); see also Chris Pandolfo and Houston Keene, *Josh Hawley says tech CEOs will 'absolutely' use AI to censor conservatives, interfere in elections*, FOX NEWS (Sept. 13, 2023).

⁴² *About NSF*, NAT. SCI. FOUND., <https://new.nsf.gov/about#who-we-are-ff8> (last visited Feb. 4, 2024).

⁴³ *Id.*; *Budget, Performance and Financial Reporting*, NAT. SCI. FOUND., <https://new.nsf.gov/about/budget> (last visited Feb. 4, 2024).

⁴⁴ *NSF FY 2023 Budget Request to Congress*, NAT. SCI. FOUND., https://nsf-gov-resources.nsf.gov/about/budget/fy2023/pdf/01_fy2023.pdf (last visited Feb. 3, 2024); *FY 2024 Budget Request to Congress*, NAT. SCI. FOUND., https://nsf-gov-resources.nsf.gov/2023-08/NSF%20FY24%20CJ_Entire%20Rollup_web_%28ERRATA%20v4%29.pdf (last visited Feb. 3, 2024).

⁴⁵ Charles Lane, *Congress should cut funding for political science research*, THE WASH. POST (June 4, 2012); *Congress Limits NSF Funding for Political Science*, SCIENCE MAG. Vol. 339 (Mar. 29, 2013), https://uh.edu/hobby/_docs/science-political-science.pdf.

⁴⁶ See, e.g., *NSF 21-500: Secure and Trustworthy Cyberspace (SaTC) Program Solicitation*, NAT. SCI. FOUND. (Oct. 2, 2020), <https://www.nsf.gov/pubs/2021/nsf21500/nsf21500.htm>.

2. NSF’s Convergence Accelerator Program

In 2019, NSF launched its Convergence Accelerator grant program seeking to bring together multiple disciplines, ideas, approaches, and technologies to solve “national-scale societal challenges” aligned with specific research “tracks” that “have the potential for significant national impact.”⁴⁷ This two-phase program funds research teams and places them into collaborative cohorts, which work “convergently” to solve issues relevant to their track and “impact society at scale.”⁴⁸

The Convergence Accelerator grant program currently has thirteen tracks:

- Track A (2019): Open Knowledge Networks
- Track B (2019): AI and the Future of Work
- Track C (2020): Quantum Technology
- Track D (2020): AI-Innovation Data Sharing & Modeling
- Track E (2021): Networked Blue Economy
- Track F (2021): Trust & Authenticity in Communication Systems
- Track G (2021): Securely Operating Through 5G Infrastructure
- Track H (2022): Enhancing Opportunities for Persons with Disabilities
- Track I (2022): Sustainable Materials for Global Challenges
- Track J (2022): Food & Nutrition Security
- Track K (2023): Equitable Water Solutions
- Track L (2023): Real-World Chemical Sensing Applications
- Track M (2023): Bio-Inspired Design Innovations

3. NSF’s Track F: The Censorship Program

In March 2021, NSF introduced Track F: Trust & Authenticity in Communication Systems, allocating \$21 million to the program.⁴⁹ For Track F, NSF solicited proposals to address the manipulation or “unanticipated negative effects” of communication systems—a departure from the Convergence Accelerator program’s other, more concrete research topics.⁵⁰

The euphemistic “trust and authenticity in communication systems,” in fact, means combatting so-called “misinformation,” *i.e.*, censorship. In an early draft solicitation, NSF indicated that Track F projects will “address issues of trust and authenticity in communication systems, including *predicting, preventing, detecting, correcting, and mitigating the spread of inaccurate information* that harms people and society.”⁵¹ As NSF’s Track F program manager,

⁴⁷ *NSF Convergence Accelerator Phases 1 and 2 for the 2023 Cohort - Tracks K, L, M*, NAT. SCI. FOUND. (May 16, 2023), <https://nsf.gov-resources.nsf.gov/solicitations/pubs/2023/nsf23590/nsf23590.pdf>

⁴⁸ *Id.*

⁴⁹ *Convergence Accelerator Portfolio*, NAT. SCI. FOUND., <https://new.nsf.gov/funding/initiatives/convergence-accelerator/portfolio> (last visited Feb. 4, 2024).

⁵⁰ *Funding Opportunity: NSF Convergence Accelerator Phase I and II for the 2021 Cohort*, NAT. SCI. FOUND. (Mar. 18, 2021).

⁵¹ Draft of NSF 2021 Convergence Accelerator Program Solicitation entitled “NSF Convergence Accelerator Phase I and II mgmt plan FY 2021 2021-01-04.docx,” attached to a January 10, 2021 NSF email (emphasis added).

Michael Pozmantier, explained more plainly in a June 2021 email, Track F is the NSF “Accelerator track focused on combatting mis/disinformation.”⁵²

From: Pozmantier, Michael <[REDACTED]@nsf.gov>
Sent: Friday, June 11, 2021 2:23:30 PM
To: Pozmantier, Michael <[REDACTED]@nsf.gov>
Subject: NSF Convergence Accelerator: Trust and Authenticity in Communications Systems

Good afternoon,

I'm contacting you because you have been recommended by my NSF colleagues or your peers to be reviewers for proposals in our Accelerator track focused on combatting mis/disinformation and inauthentic behavior. I believe you would bring valuable expertise and insights to our review panels, as we select projects to address this issue.

On March 18, 2021, NSF issued the funding opportunity for Track F, ultimately asking applicants to propose solutions involving AI-powered tools to help Big Tech combat misinformation as well as provide “education and training materials” for school children and communities that might “exhibit different vulnerabilities to disinformation methods.”⁵³

In September 2021, after receiving dozens of proposals, NSF publicly announced the 24 research teams it had selected for its 2021 cohort (Tracks E and F), awarding twelve Track F teams \$750,000 each (a total of \$9 million) to develop and refine their project ideas and build partnerships in Phase 1.⁵⁴ During this year-long initial planning phase, the teams participated in a nine-month-long NSF program to “advanc[e] their initial idea to a proof of concept” and develop pitch presentations to deliver to “various stakeholders including potential partners, investors and end users” at NSF’s annual Convergence Accelerator Expo.⁵⁵

Ultimately, after the teams made their case for continued funding at NSF’s July 2022 Expo, in September 2022, NSF selected six of the original twelve “Phase 1” Track F teams to move to “Phase 2,” each receiving an additional \$5 million (for a total of \$30 million) over the next two years to further develop, scale, and sustain their projects beyond NSF support.⁵⁶ In all, NSF allocated a total of \$39 million to the various Track F teams.

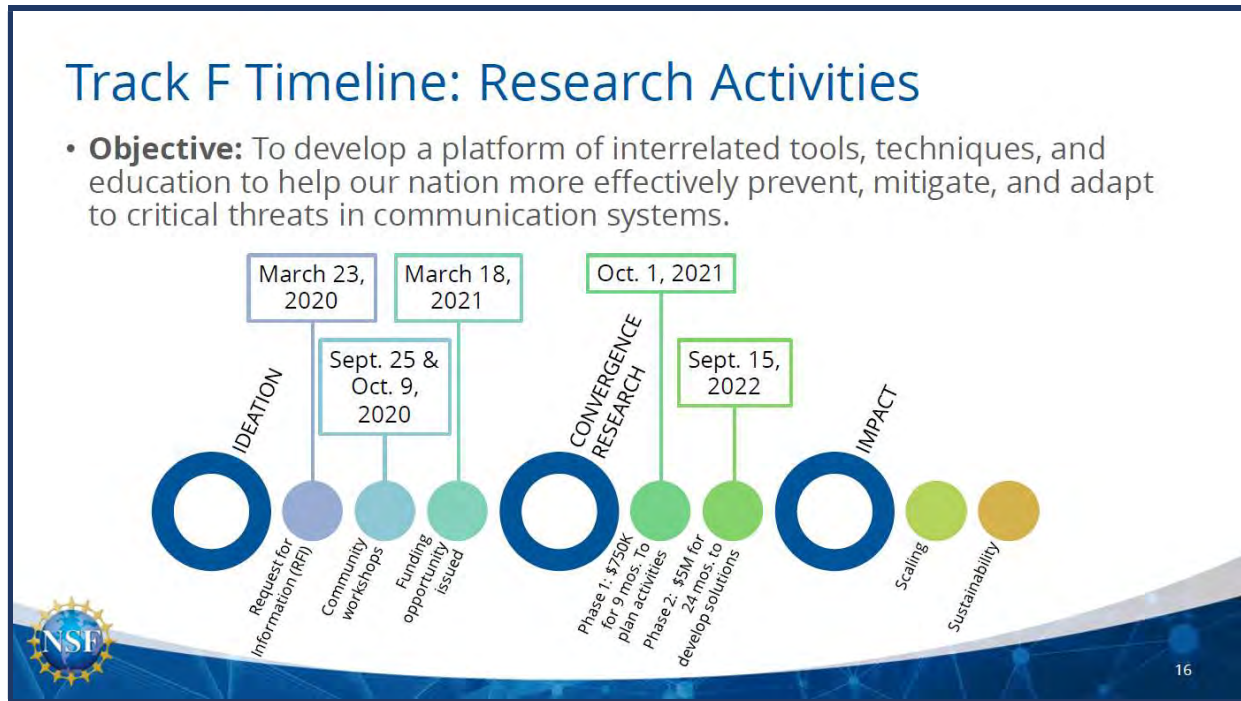
⁵² Email from Michael Pozmantier to Michael Pozmantier (June 11, 2021, 2:23 PM) (on file with the Comm.).

⁵³ See NSF Convergence Accelerator 2021 Cohort Program Solicitation, NAT. SCI. FOUND. (Mar. 18, 2021), <https://nsf-gov-resources.nsf.gov/solicitations/pubs/2021/nsf21572/nsf21572.pdf> (“Projects in Track F will pursue a convergence research agenda and leverage multi-sector partnerships to address issues of trust and authenticity in communication systems, including predicting, preventing, detecting, correcting, and mitigating the spread of *inaccurate information* that harms people and society.”) (emphasis added).

⁵⁴ *NSF invests \$21 million to tackle 2 complex societal challenges: the networked blue economy, and trust and authenticity in communication systems*, NAT. SCI. FOUND. (Sep. 22, 2021), https://www.nsf.gov/news/special_reports/announcements/092221.jsp.

⁵⁵ *Convergence Accelerator Program Model*, NAT. SCI. FOUND., <https://new.nsf.gov/funding/initiatives/convergence-accelerator/program-model>.

⁵⁶ *NSF Convergence Accelerator Phases 1 and 2 for the 2023 Cohort – Tracks K, L, M*, NAT. SCI. FOUND. (May 12, 2023), <https://new.nsf.gov/funding/opportunities/nsf-convergence-accelerator-phases-1-2-2023-cohort>.



This interim report focuses on four of those original twelve Track F recipients and their NSF-funded projects, which received a combined \$13 million in American taxpayer dollars:

- the University of Michigan and its WiseDex tool (\$750,000);
- Meedan and its Co-Insights tool (\$5.75 million);
- the University of Wisconsin-Madison and its CourseCorrect tool (\$5.75 million); and
- Massachusetts Institute of Technology (MIT) and its Search Lit platform (\$750,000).

D. Censorship and Propaganda in Action: Universities and Non-Profits Develop AI Tools and Other New Technologies to Censor at Scale with Help of Federal Funding

Under the guise of addressing critical threats to communications systems and “combatting mis/disinformation,”⁵⁷ NSF has provided millions of taxpayer dollars to university researchers for the development of advanced censorship tools. One research team, led by researchers at the University of Michigan, used the \$750,000 it received from NSF to examine how AI could help Big Tech handle and outsource the “responsibility of censorship” on social media.

⁵⁷ See email from Michael Pozmantier to Michael Pozmantier (June 11, 2021, 2:23 PM) (on file with the Comm.).

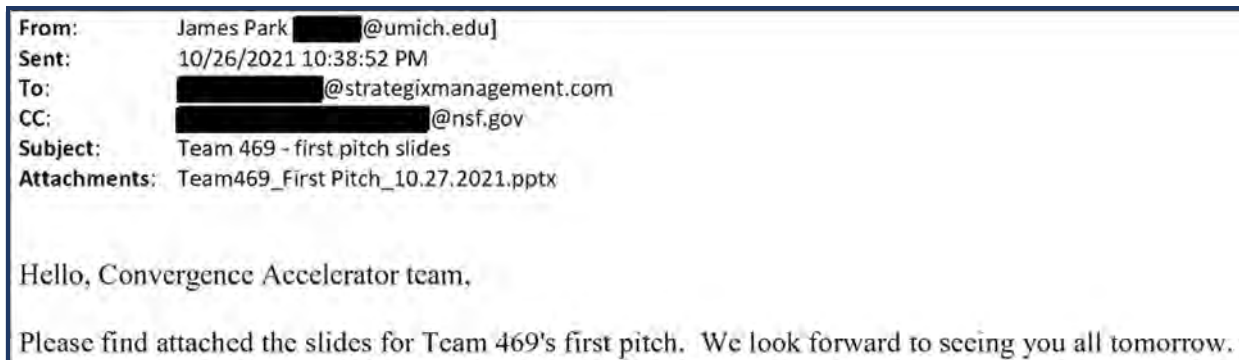
1. The University of Michigan: WiseDex

In September 2021, through its Track F program, NSF awarded a group of researchers at the University of Michigan \$750,000 to develop two services:

1. A “golden set” service that determines what content is misinformation “that deserves enforcement” each month; and
2. A forecasting application programming interface (API) that can tell a social media platform “for any content item” how true that content is to aid in “a platform’s decision procedures” (*i.e.*, whether the content should be censored).⁵⁸

The University of Michigan intended to use the federal funding to develop its tool “WiseDex,” which could use AI technology to assess the veracity of content on social media and assist large social media platforms with what content should be removed or otherwise censored.⁵⁹ As noted by the team’s head researcher, “The original goal of the project was to develop processes that would have public legitimacy, which social media platforms could use for taking enforcement action against misinformation.”⁶⁰

Documents show that NSF was aware that federal tax dollars would be supporting a tool used for censorship.



The Committee and Select Subcommittee have obtained October 2021 presentation slides with speaker’s notes that shed light on this point. In the University of Michigan’s “first pitch”⁶¹

⁵⁸ Award Abstract # 2137469: NSF Convergence Accelerator Track F: Misinformation Judgments with Public Legitimacy, NAT. SCI. FOUND., (last updated Jan. 30, 2024), https://www.nsf.gov/awardsearch/showAward?AWD_ID=2137469.

⁵⁹ *Id.*

⁶⁰ *Id.*


⁶¹ Email from James Park to NSF Convergence Accelerator team (October 26, 2021, 10:38 PM) (on file with the Comm.).

to the NSF Convergence Accelerator, the researchers marketed WiseDex as a way for “policy makers at platforms” to “externaliz[e] the difficult responsibility of censorship.”⁶²

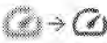
Team F-469

Overview

Our misinformation service






helps **policy makers at platforms** 

get good PR for their actions on misinformation

by having a **clear benchmark for outcomes** 

and eliminating the need to defend internal procedures.

Misinformation Judgments with Public Legitimacy

 Paul Resnick Lead PI University of Michigan	 David Jurgens Co-PI University of Michigan	 Amy Zhang Co-PI University of Washington
 Adam Berinsky Senior Personnel MIT	 David Rand Senior Personnel MIT	 James Park Project Manager University of Michigan

NSF Convergence Accelerator

NSF Convergence Accelerator

Substituted clear benchmark for: “externalizing responsibility for assessing the validity of particular actions”
Our misinformation service helps policy makers at platforms who want to

- Get people off our backs for how we act on misinfo
- Do the things we know work without backlash
- Push responsibility for difficult judgments to someone outside the company
- Feel good about how they are acting on misinfo
- legitimate way to act on misinformation ,

By

Externalizing the difficult responsibility of censorship

Measuring/defending outcomes instead of procedures
and Eliminating the need to defend specific procedures.

The speaker’s notes also reveal how federal bureaucrats and “disinformation” pseudo-scientists talk about their work in private. Although these statements plainly violate the First Amendment, NSF continued to fund the University of Michigan’s \$750,000 project directed toward “censorship.” In fact, these candid remarks were made to NSF just one month after NSF awarded the University of Michigan \$750,000 in Phase 1 funding in late September 2021.⁶³

About six months later, in July 2022, the WiseDex team made a presentation at NSF’s annual “Convergence Accelerator Expo” to an audience that included interested parties in the public and private sector as well as other research teams that had received NSF funding. In advance of the 2022 Expo, the University of Michigan team emailed representatives at major social media platforms, inviting them to the Expo and describing WiseDex as a tool that

⁶² The University of Michigan’s WiseDex First Pitch Slide Deck entitled “Team469_First Pitch_10.27.2021.pptx” attached to an email from James Park to Michael Pozmantier (Oct. 26, 2021, 10:38 PM), at 1 (on file with the Comm.) (emphasis added).

⁶³ *Award Abstract # 2137469: NSF Convergence Accelerator Track F: Misinformation Judgments with Public Legitimacy*, NAT. SCI. FOUND. (last updated Jan. 30, 2024).

“harnesses the wisdom of crowds and AI techniques to help flag more posts.”⁶⁴ The University of Michigan team explained further that the “result is more comprehensive, equitable, and consistent enforcement, significantly reducing the spread of misinformation.”⁶⁵ In its agenda presentation notes for the Expo, the Michigan team explained that the WiseDex tool will enable the “scaling-up enforcement of misinformation policies” on social media.⁶⁶ Put more plainly, WiseDex would facilitate the censorship of speech online at a speed and in a manner that human censors are not capable.

2. Meedan: Co-Insights

Meedan is a non-profit that, among other things, builds software to combat alleged misinformation online.⁶⁷ In May 2020, Scott Hale, Meedan’s Director of Research, contacted NSF about Meedan’s interest in the Convergence Accelerator program, noting in an email that Meedan’s vision was to build software and run training and programs “to counter misinformation online” and “advance the state-of-art in misinformation research.”⁶⁸ On May 5, 2021, Meedan sent NSF an official letter expressing its intent to apply for NSF’s Track F.⁶⁹ If it were to receive taxpayer dollars, Meedan would leverage its “relationships and experience” with WhatsApp, Telegram, and Signal to develop approaches that proactively “identify and limit susceptibility to misinformation” and “pseudoscientific information online.”⁷⁰ This included “[o]pen-web crawling and controversy detection identifying possibly [*sic*] content for fact-checking.”⁷¹ Ultimately, NSF awarded Meedan’s project \$5.75 million through its Track F program.⁷²

Meedan’s project went through multiple name changes, including “FACT CHAMP”: “Fact-checker, Academic, and Community Collaboration Tools: Combating Hate, Abuse, and Misinformation with Minority-led Partnerships.”⁷³ By the summer of 2022, it had the name that it has today: Co-Insights. The project’s purpose is to use “data and machine learning” to “identify, preempt, and respond to misinformation in minoritized [*sic*] communities.”⁷⁴



⁶⁴ Email from WiseDex team to multiple recipients, including representatives from major social media platforms (July 13, 2022, 10:23 PM) (on file with the Comm.).

⁶⁵ *Id.*

⁶⁶ WiseDex team’s agenda presentation notes for 2022 Expo (Feb. 2022), at 2 (on file with the Comm.).

⁶⁷ *Mission*, MEEDAN, <https://meedan.com/mission>; *see also Check*, MEEDAN, <https://meedan.com/check>.

⁶⁸ Email from Scott Hale to NSF personnel (May 5, 2020, 2:41 AM) (on file with the Comm.).

⁶⁹ Meedan’s Letter of Intent to Propose to NSF’s Convergence Accelerator Track F program (May 5, 2021), at 1 (on file with the Comm.).

⁷⁰ *Id.*

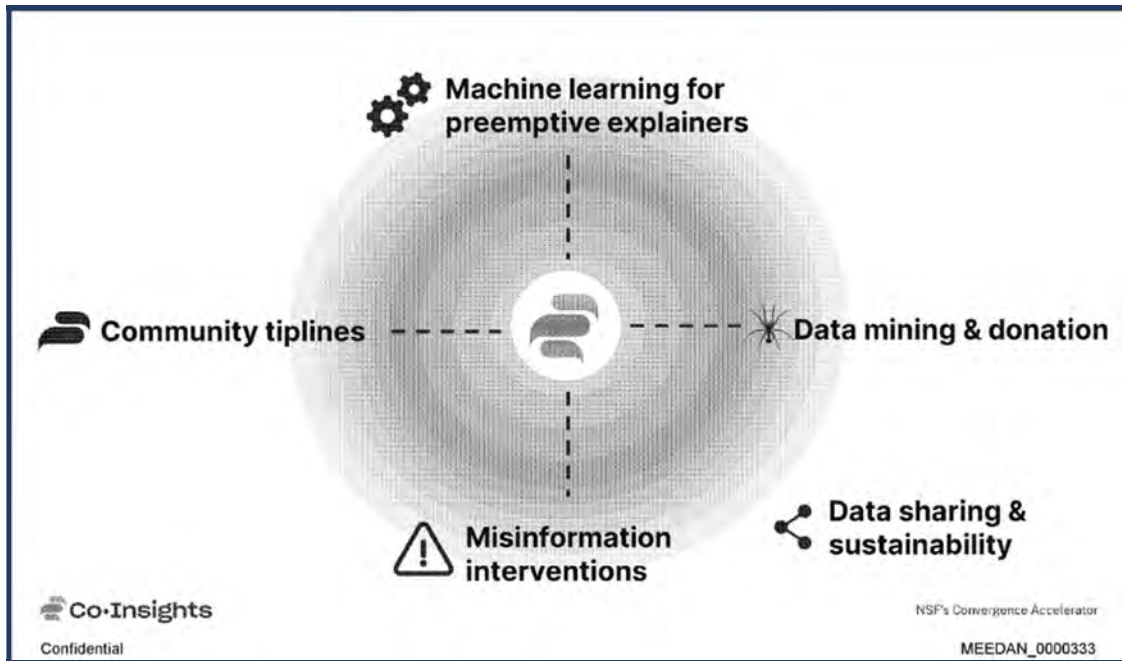
⁷¹ Email from Meedan to NSF personnel (Aug. 30, 2021, 8:54 AM) (on file with the Comm.).

⁷² *FACT CHAMP: New project to increase collaboration between fact-checkers, academics, and community leaders to counter misinformation online*, MEEDAN (Sept. 27, 2021); *Co-Insights wins \$5m from the National Science Foundation*, MEEDAN (Oct. 17, 2022).

⁷³ Email from Scott Hale to NSF personnel (Sept. 7, 2021, 4:13 PM) (on file with the Comm.).

⁷⁴ Meedan’s Oral Pitch Slide Deck entitled “F032-Co-Insights-Slides-v2.pdf” attached to an email from Scott Hale to Michael Pozmantier (June 27, 2022, 7:33 PM), at 6 (on file with the Comm.).

In its pitch to NSF for an additional \$5 million in Phase 2 funding, Meedan’s Co-Insights team again explained how its project used a variety of advanced tools to inform “misinformation interventions.”⁷⁵



For example, in one slide, the team boasted that it was using AI to monitor 750,000 blogs and media articles daily as well as mine data from the major social media platforms.⁷⁶

Prof. Ethan Zuckerman
University of Massachusetts Amherst

Dr. Keen Sung
AuCoDe
Amherst University of Massachusetts

MEDIA CLOUD

750,000
blogs and media articles crawled daily

Data mining

Instagram, Twitter, YouTube, TikTok, Facebook, Reddit

Co-Insights
Confidential

NSF's Convergence Accelerator
MEEDAN_0000312

⁷⁵ *Id.*, at 8.
⁷⁶ *Id.*, at 18.

In another presentation slide, the Co-Insights team declared that it had the “world’s best system for matching social media posts to fact-checks.”⁷⁷

Prof. Shiri Dori-Hacohen
UNCONN UNIVERSITY OF CONNECTICUT

Prof. Brendan O'Connor
University of Massachusetts Amherst

Competition

CLEF2022 CheckThat! Lab - Task 2

CLEF

1st

Hugging Face

World's best system for matching social media posts to fact-checks.

Co-Insights

Confidential

NSF's Convergence Accelerator

MEEDAN_0000338

As part of its presentation to NSF, Co-Insights emphasized that it would monitor and respond to “common misinformation narratives,” such as:

- “Fearmongering and anti-Black narratives,” such as criticizing the *New York Times* for “ignoring Black-on-Asian hate crimes,” and
- “Undermining trust in mainstream media.”⁷⁸

Prof. Jonathan Ong
University of Massachusetts Amherst

Prof. Natasha Shrikant
University of Colorado Boulder

Common misinformation narratives

- Fearmongering and anti-Black narratives
- Undermining trust in mainstream media
- Glorifying vigilantism
- Weakening political participation

ASIAN DAWN

CRITICS SLAM THE NY TIMES FOR IGNORING BLACK-ON-ASIAN HATE CRIMES

Co-Insights

Confidential

NSF's Convergence Accelerator

MEEDAN_0000339

⁷⁷ *Id.*, at 13.

⁷⁸ *Id.*, at 14.

The project would also operate “tiplines to source potentially problematic content and return misinformation interventions.”⁷⁹

Ongoing project activities	
	Overall project management; monitoring & evaluation; quarterly logframe updates & advisory board meetings ¹
⚠	Creation of misinformation interventions (e.g., conversation guides, explainers, fact-checks) ^{5, 2, 4, 8} ; Taxonomy development, training, resources to support interventions ²
🔍	Identification and monitoring of key mainstream misinformation spreaders ²
🔗	Operation of tiplines to source potentially problematic content and return misinformation interventions ^{5, 1, 2, 4, 8}
🔍	Ongoing identification of new narratives through quantitative and qualitative data analysis ^{8, 2, 4, 5}

These efforts by Meedan, funded by NSF, were part of a much larger, long-term goal by the non-profit. As Hale, the Director of Research at Meedan, explained in an email to NSF, in his “dream world,” Big Tech would collect all of the censored content to enable “disinformation” researchers to use that data to create “automated detection” to censor any similar speech automatically.⁸⁰

From: Scott Hale [REDACTED]@meedan.com
Sent: 11/17/2022 9:31:39 PM
To: Pozmantier, Michael [REDACTED]@nsf.gov
Subject: Re: FW: [EXTERNAL] - NSF Award Search: Award # 2131929 - Mid-scale RI-1 (M1:IP); Observatory for Online Human and Platform Behavior

Hi Mike,

Great to talk earlier. In addition to Rehul's work ("Data Station"), the discussion about research infrastructure made me think of the work Christopher Guess is doing at Duke Reporter's Lab. They've been working on a dataset of fact-checks and the original media connected to those fact-checks. I believe that work is nearly complete and will be public soon, but I'm sure there are elements that will benefit teams in our track and ways it could be expanded.

The term I couldn't think of before was "data enclaves." I think we'd benefit from ways to run code on remote datasets without having access to the data (i.e., everything in and out has a minimum level of aggregation/anonymization). This applies to mis/disinformation given how it may involve personal data and the potential for misuse by malicious actors. It applies even more to hate speech, radicalization, etc. In my dream world, social media platforms would put all the content they take down into a data enclave that researchers could run code against to produce aggregate analyses and benchmark different automated detection approaches without ever having direct access to the data. There's nothing more frustrating than, for example, finding out half the tweet ids (or urls) in a dataset of high-quality human labels are now inaccessible.

The millions of taxpayer-funding notwithstanding, NSF considered whether it could recruit other, existing, successful AI companies and persuade them to wield their tools for purposes of “content moderation.” For example, in January 2023, Pozmantier, the NSF Track F project manager, emailed Meedan’s Hale about NSF’s interactions with “Storytell,” which is a Chrome extension that uses AI to “automatically” summarize any page, including YouTube

⁷⁹ *Id.*, at 28.

⁸⁰ Email from Scott Hale to Michael Pozmantier (Nov. 17, 2022, 9:31 PM) (on file with the Comm.).

videos.⁸¹ According to Pozmantier, NSF had been engaging with Storytell, and the company had “been open to listening to content moderation as a use case,” *i.e.*, Storytell would consider NSF’s idea of repurposing its AI technology to be used for content moderation.⁸²

From: Scott Hale [REDACTED]@meedan.com]
Sent: 1/19/2023 11:13:01 PM
To: Pozmantier, Michael [REDACTED]@nsf.gov]
Subject: Re: [EXTERNAL] - Fwd: Mike - RE: Storytell Chrome Extension; beta release. Interested?

Cool. I don't know the business model they're wanting to pursue, but I'd certainly be open to talking with them and seeing if there was some proof of concept we could help them do to demonstrate the value to fact-checkers. The amount of video we see coming to fact-checking tiplines on WhatsApp is continually increasing. We probably see the most video in Brazil right now, although I realize their tech might be English only at the moment.

On Thu, Jan 19, 2023 at 6:09 PM Pozmantier, Michael <[REDACTED]@nsf.gov> wrote:
 I've been asking them if they plan to have this tool in a format that can be used at a greater scale, they've said they want to have something like that down the line. But specific feedback like yours will help drive them that way, they've been open to listening to content moderation as a use case.

From: Scott Hale [REDACTED]@meedan.com>
Date: Thursday, January 19, 2023 at 6:07 PM
To: "Pozmantier, Michael" <[REDACTED]@nsf.gov>
Subject: Re: FW: [EXTERNAL] - Fwd: Mike - RE: Storytell Chrome Extension; beta release. Interested?

Thanks, Mike,

This looks like nice technology, but I'm not sold on the Chrome extension format. For me, this would be much better as an API that could be used in one of two ways:

- 1) summarizing videos and breaking out key segments could be very useful for fact-checkers assessing video content. One of the annoying things about fact-checking YouTube, TikTok, etc. is that fact-checkers generally have to watch the video before knowing what claims are being made and determining whether it's worth fact-checking those
- 2) summarizing larger datasets to spot patterns and trends - there's reference to this feature in the video, but I don't see how that currently works with the Chrome extension format. Ideally, I'd point it at a dataset of content, and it would be able to generate a report, summarize themes from multiple pieces of content, identify key pieces of content, etc. to help me make sense of that large dataset. For us, this would be spotting trends and longer-term themes in social media content that might benefit from pre-emptive explainers. For others, I could imagine it summarizing free-text responses to surveys, etc.

Best wishes,
 Scott

On Thu, Jan 19, 2023 at 5:50 PM Pozmantier, Michael <[REDACTED]@nsf.gov> wrote:
 Love to hear what you all think about this tool. Appears to work pretty well at pulling information from videos, but currently doesn't do much at scale.

⁸¹ Email from Michael Pozmantier to Scott Hale (Jan. 19, 2023, 5:50 PM) (on file with the Comm.); *see also* *Storytell.ai: ChatGPT with your Content*, CHROME WEB STORE, <https://chromewebstore.google.com/detail/storytellai-chatgpt-with/khggjnjoomjjihbjkpbhmpelgcdodjpi> (last visited Feb. 4, 2024).

⁸² Email from Michael Pozmantier to Scott Hale (Jan. 19, 2023, 6:09 PM) (on file with the Comm.).

3. The University of Wisconsin: CourseCorrect

Beginning in September 2021, through its Track F program, NSF awarded a group of researchers at the University of Wisconsin-Madison a total of \$5.75 million to develop a tool to “empower efforts by journalists, developers, and citizens to fact-check” “delegitimizing information” about “election integrity and vaccine efficacy” on social media.⁸³ UW-Madison’s CourseCorrect tool would allow “fact-checkers to perform rapid-cycle testing of fact-checking messages and monitor their real-time performance among online communities at-risk of misinformation exposure.”⁸⁴

Like Michigan’s WiseDex, the University of Wisconsin-Madison’s CourseCorrect project harnessed AI and machine learning techniques to address misinformation on social media.⁸⁵ Unlike WiseDex, the University of Wisconsin-Madison researchers made clear that their project was specifically focused on “address[ing] two democratic and public health crises facing the U.S.: skepticism regarding the integrity of U.S. elections and hesitancy related to COVID-19 vaccines.”⁸⁶ To do so, CourseCorrect spent over \$5 million in taxpayer money working to “identify, test, and correct real-world instances” of COVID-19, election-related, and other forms of “dangerous misinformation” on social media and scale and sustain the project beyond NSF support.⁸⁷

4. MIT: Search Lit

In September 2021, through its Track F program, NSF awarded \$750,000 to a group of researchers at the Massachusetts Institute of Technology (MIT) to develop “effective interventions” to educate Americans—specifically, those that the MIT researchers alleged “may be more vulnerable to misinformation campaigns”—on how to discern fact from fiction online.⁸⁸ In particular, the MIT team believed that conservatives, minorities, and veterans were uniquely incapable of assessing the veracity of content online.⁸⁹

⁸³ *Award Abstract # 2137724: NSF Convergence Accelerator Track F: How Large-Scale Identification and Intervention Can Empower Professional Fact-Checkers to Improve Democracy and Public Health*, NAT. SCI. FOUND. (last updated Sep. 20, 2021), https://www.nsf.gov/awardsearch/showAward?AWD_ID=2137724.

⁸⁴ *Id.*

⁸⁵ CourseCorrect Slide Deck entitled “Intervention_July_v3.pptx” (created July 20, 2023, 11:59 AM), at 2, 3, 10-12 (on file with the Comm.).

⁸⁶ *Award Abstract # 2137724: NSF Convergence Accelerator Track F: How Large-Scale Identification and Intervention Can Empower Professional Fact-Checkers to Improve Democracy and Public Health*, NAT. SCI. FOUND. (last updated Sep. 20, 2021), https://www.nsf.gov/awardsearch/showAward?AWD_ID=2137724.

⁸⁷ *Id.*

⁸⁸ *Award Abstract # 2137530: NSF Convergence Accelerator Track F: Adapting and Scaling Existing Educational Programs to Combat Inauthenticity and Instill Trust in Information*, NAT. SCI. FOUND. (last updated Dec. 7, 2023), https://www.nsf.gov/awardsearch/showAward?AWD_ID=2137530.

⁸⁹ *Id.*

The MIT project targeted individual groups and designed propaganda tools aimed at “educating” rural and indigenous communities, military veterans, older adults, and military families—all of whom the researchers claimed were unusually susceptible to “misinformation campaigns” online.⁹⁰

In one project proposal document to NSF, the researchers explained the need for “a *proactive* suite of human technologies” to assist these groups with “dangerous digital content” because “*reactive*” content moderation is too slow and ineffective.⁹¹ In order to build “a more digitally discerning public,” the Search Lit team proposed developing tools that could support the government’s viewpoint on COVID-19 public health measures and the 2020 election.⁹²

III. THE FEDERALLY FUNDED CENSORS: PARTISAN AND CONDESCENDING

In her ethnographic study of two conservative groups, Tripodi (2018) found that information-seekers engage in a distinct set of media practices tied to the way they see the world. One practice centered around the close reading of textual documents deemed sacred (e.g. the Bible or the Constitution). By inverting traditional assumptions that truth is only curated at the top, this media practice allows for everyday people to act as subject matter experts. These practices, which developed and emerged in a print era, have been adapted to online search practices. Because interviewees distrusted both journalists and academics, they drew on this practice to fact check how media outlets reported the news.

* * *

While lateral readers try to find secondary sources that reliably summarize expert consensus on sources and claims (Wineburg & McGrew, 2017; Caulfield, 2017), respondents often focused on reading a wide array of *primary* sources, and performing their own synthesis (Tripodi, 2018).

– MIT’s 2021 Proposal to NSF (\$750,000 ultimately awarded)

The nonpublic communications and documents obtained by the Committee and Select Subcommittee demonstrate that (1) the “disinformation” academics understood their work as part of a partisan project; and (2) the bureaucrats and so-called “experts” in this space have complete disdain for most of the American population.

⁹⁰ *Id.*

⁹¹ *Id.*; MIT’s summary of its Search Lit proposal to NSF, at 2 (on file with the Comm.) (emphasis in original).

⁹² MIT Search Lit team’s annual report to NSF (Dec. 1, 2022), at 20-23 (on file with the Comm.).

A. In Their Own Words, “Disinformation” Pseudo-Scientists Describe Their Work As “Political” and “Censorship”

In response to the Committee and Select Subcommittee’s investigation into government-directed censorship, mainstream media outlets have largely characterized “mis- and disinformation” researchers as apolitical academics pursuing serious research free of political biases or agendas.⁹³ But the very same disinformation “experts” making these public claims, such as the University of Washington’s Dr. Kate Starbird, have acknowledged privately that working to counter disinformation is “inherently political”⁹⁴ and is itself a form of “censorship.”⁹⁵



The NSF-funded researchers at the University of Michigan, University of Washington, and MIT privately explained that their work is involved with the “difficult *responsibility* of censorship,” a statement that implies these “experts” bear the burden of determining for everyone

⁹³ See, e.g., Naomi Nix, et al., *Misinformation research is buckling under GOP legal attacks*, THE WASH. POST (Sept. 23, 2023); Kate Starbird, *UW misinformation researchers will not buckle under political attacks*, SEATTLE TIMES (Oct. 6, 2023).

⁹⁴ Email from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.); see also Kate Starbird et al., Proposal to the National Science Foundation for “Collaborative Research: SaTC: Core: Large: Building Rapid-Response Frameworks to Support Multi-Stakeholder Collaborations for Mitigating Online Disinformation” (Jan. 29, 2021) (unpublished proposal) (on file with the Comm.) (“The study of disinformation today invariably includes elements of politics.”).

⁹⁵ The University of Michigan’s WiseDex First Pitch Slide Deck entitled “Team469_First Pitch_10.27.2021.pptx” attached to an email from James Park to Michael Pozmancier (Oct. 26, 2021, 10:38 PM), at 1 (on file with the Comm.) (emphasis added).

else what is good information and what is not.⁹⁶ Even if this statement was not so remarkably paternalistic, it would still be an unconstitutional use of federal taxpayer dollars.

Team F-469

Overview

Our misinformation service

helps **policy makers at platforms** ...

get good PR for their actions on misinformation

by having **a clear benchmark for outcomes** →

and eliminating the need to defend internal procedures.

Misinformation Judgments with Public Legitimacy

		
Paul Resnick Lead PI University of Michigan	David Jurgens Co-PI University of Michigan	Amy Zhang Co-PI University of Washington
		
Adam Berinsky Senior Personnel MIT	David Rand Senior Personnel MIT	James Park Project Manager University of Michigan

Substituted clear benchmark for: “externalizing responsibility for assessing the validity of particular actions”

Our misinformation service helps policy makers at platforms who want to

- Get people off our backs for how we act on misinfo
- Do the things we know work without backlash
- Push responsibility for difficult judgments to someone outside the company
- Feel good about how they are acting on misinfo

legitimate way to act on misinformation ,

By

Externalizing the difficult responsibility of censorship

Measuring/defending outcomes instead of procedures

and Eliminating the need to defend specific procedures.

Renée DiResta, another prominent disinformation researcher at the Stanford Internet Observatory (SIO), disclosed in her notes for a fall 2021 presentation at an annual CISA Summit that the EIP was designed to fill the “gap” that the federal government could not fill. Her presentation notes state that there were “[u]nclear legal authorities including *very real 1st amendment questions*.”⁹⁷

⁹⁶ See *id.*

⁹⁷ “CISA keynote.pptx” attach. to email from Renée DiResta to Kenneth Bradley and Amanda Glenn (Oct. 6, 2021, 3:58 PM) (on file with the Comm.); see also email from Renée DiResta to Kenneth Bradley and Amanda Glenn (Oct. 6, 2021, 3:58 PM) (on file with the Comm.) (DiResta writes, “I was just writing out the full script into the speaker notes in case the teleprompter was the best bet.”); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

As the Committee and Select Subcommittee have detailed in earlier reports, a full accounting of the content that the EIP flagged for social media platforms reveals the political leanings of the academics; though Americans on both sides of the political spectrum were censored, conservatives were targeted disproportionately.⁹⁸ Similarly, the Twitter Files revealed that Republicans were censored at a rate of at least “ten-to-one” as Democrats.⁹⁹ And the lead litigator in *Missouri v. Biden* testified to the Select Subcommittee that “the vast majority” of examples of censorship uncovered in discovery in that case were of conservative speech.¹⁰⁰

B. NSF-Funded Researchers Believe the American Public is Not Smart Enough to Discern Fact from Fiction, Especially Conservatives, Minorities, and Veterans

Littered throughout these researchers’ federally funded projects is the paternalistic assumption that particular groups of American citizens are uniquely unable to differentiate between truth and falsehood online. As the MIT-led researchers explained in a summary of their project proposal to NSF, “broad swaths of the public cannot effectively sort truth from fiction online.”¹⁰¹ In particular, the Search Lit team singled out the following demographics:

- “rural and indigenous communities;”
- “military veterans, older adults, and military families;” and
- “older adults.”¹⁰²

As part of their efforts to target military families, NSF proposed working “with educators in the Department of Defense Education Activity (DoDEA) group, the organization that runs [Defense Department] schools on military bases, to adapt our innovations to both directly serve children in military families and *then have students share their new learning with their families.*”¹⁰³ Put plainly, Search Lit sought to help train the children of military families to help influence the beliefs of military families. When Search Lit “discussed these ideas with DoDEA stakeholders, they immediately brought up concerns about military personnel involvement in the January 6 assault on the Capitol and the subsequent anti-extremism training that is a military priority.”¹⁰⁴

In support of their case for NSF funding, the MIT-led researchers cited a study “of two conservative groups” performed by a Search Lit team member, Francesca Tripodi, examining the “online search practices” of Americans who hold “the Bible or the Constitution” as “sacred” and

⁹⁸ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

⁹⁹ Kaitlin Lewis, *Musk Tells Rogan Twitter ‘Suppressed’ Republicans ‘10 Times’ More Than Dems*, NEWSWEEK (Oct. 31, 2023).

¹⁰⁰ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong., at 48 (Mar. 30, 2023).

¹⁰¹ MIT’s Search Lit “Project Description” in its formal Phase II proposal to NSF, at 2. (on file with the Comm.).

¹⁰² MIT’s Search Lit “Project Summary” in its formal Phase I proposal to NSF, at 1 (on file with the Comm.); *see also* App’x D, at 1.

¹⁰³ *Id.*, at 8 (emphasis added).

¹⁰⁴ MIT’s Search Lit “Project Summary” in its formal Phase I proposal to NSF, at 8 (on file with the Comm.); *see also* App’x D.

“distrust[] journalists and academics.”¹⁰⁵ The summary also derisively noted that the approach that “everyday people” typically use to get their news and information allows them “to act as subject matter experts,” rather than “truth [being] only curated at the top.”¹⁰⁶

In her ethnographic study of two conservative groups, Tripodi (2018) found that information-seekers engage in a distinct set of media practices tied to the way they see the world. One practice centered around the close reading of textual documents deemed sacred (e.g. the Bible or the Constitution). By inverting traditional assumptions that truth is only curated at the top, this media practice allows for everyday people to act as subject matter experts. These practices, which developed and emerged in a print era, have been adapted to online search practices. Because interviewees distrusted both journalists and academics, they drew on this practice to fact check how media outlets reported the news.

According to the researchers, Tripodi’s study found that many conservative respondents “may have believed they were [] ‘doing the research’” but were in fact only “focused on the top results of Google, seldom scrolling down or looking at subsequent paged results.”¹⁰⁷ As evidence, the researchers point out that the conservative “respondents often focused on reading a wide array of *primary* sources, and performing their own synthesis,” further alleging that, “unlike expert lateral readers,” the conservative respondents made “no such effort” to “eliminate bias that might skew results from search terms.”¹⁰⁸

In fact, many respondents may have believed they were engaging in “lateral reading” (e.g. “doing the research” using Google). However, their approach differed in crucial respects. Unlike professional fact checkers, who practice “click restraint” (Wineburg & McGrew, 2017), users focused on the top results of Google, seldom scrolling down or looking at subsequent paged results (Tripodi, 2018). While lateral readers try to find secondary sources that reliably summarize expert consensus on sources and claims (Wineburg & McGrew, 2017; Caulfield, 2017), respondents often focused on reading a wide array of *primary* sources, and performing their own synthesis (Tripodi, 2018). While lateral readers seek to eliminate bias that might skew results from search terms (Caulfield, 2017), respondents made no such effort. Finally, unlike expert lateral readers, respondents evaluated search terms based on the nature of the results returned. One participant saw the fact that most results presented a similar story as evidence of a “rigged” media, rather than a heuristic of expert or professional consensus — and re-ran the search with new terms (Tripodi, 2018).

To summarize, the researchers’ concern is that there are Americans who deem the Constitution and the Bible “sacred,” and therefore dare to conduct their own research of “primary sources” rather than trust the “professional consensus.”

C. NSF-Funded Researchers Understand the Leverage They Have Over Social Media Companies to Ensure the Platforms Bow to Their Demands

NSF funding dictates who can survive in the pseudo-science world of studying so-called “disinformation.” With this role comes tremendous leverage for NSF to determine who to elevate within the censorship-industrial complex.

¹⁰⁵ *Id.*, at 7.

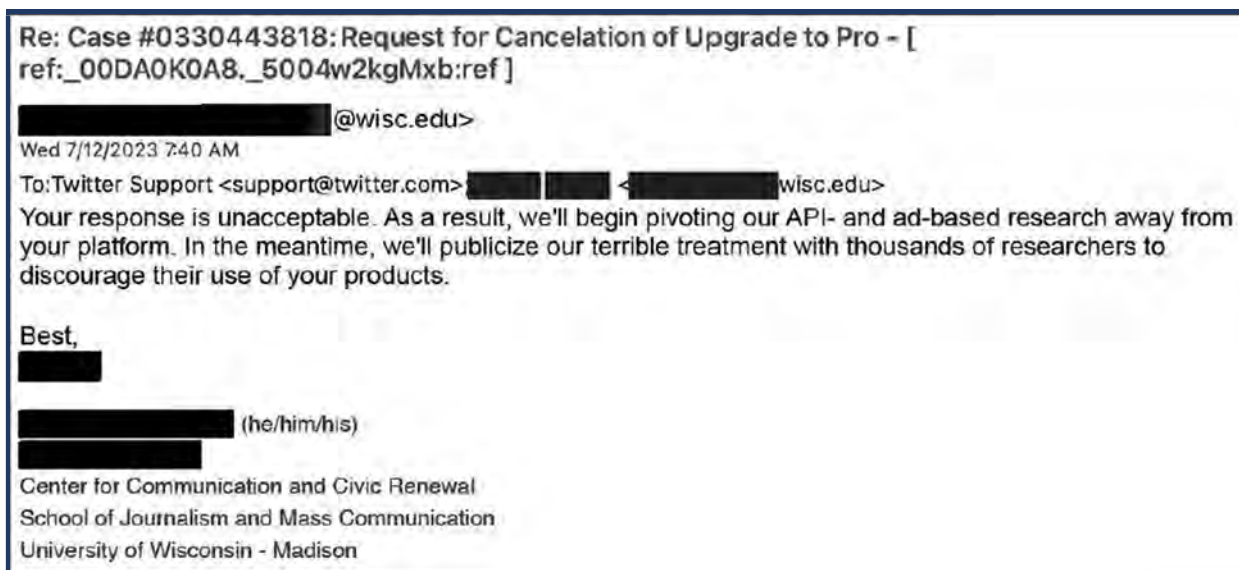
¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

Once empowered with taxpayer dollars, the pseudo-science researchers wield the resources and prestige bestowed upon them by the federal government against any entities that resist their censorship projects. In some instances, if a social media company fails to act fast enough to change a policy or remove what the researchers perceive to be misinformation on its platform, disinformation researchers will issue blogposts or formal papers to “generate a communications moment” (*i.e.*, negative press coverage) for the platform, seeking to coerce it into compliance with their demands.¹⁰⁹

Other times, the pseudo-scientists use their leverage for petty grievance. For example, on July 12, 2023, when an employee at Twitter refused to issue a refund to a Wisconsin CourseCorrect researcher based on his request to cancel a service upgrade on Twitter, the Wisconsin researcher sent an email threatening to publicize “our terrible treatment with thousands of researchers to discourage their use of your products.”¹¹⁰



Examples like these illustrate the tremendous sway these so-called “disinformation” researchers hold over social media platforms and why the federal government often turns to these unaccountable academics when seeking a proxy for their censorship activities.¹¹¹

¹⁰⁹ See House Judiciary Committee’s Transcribed Interview of Alex Stamos (June 23, 2023), at 183-184 (on file with the Comm.); see also House Judiciary Committee’s Transcribed Interview of Kate Starbird (June 6, 2023), at 153 (on file with the Comm.).

¹¹⁰ Email from UW-Madison researcher to Twitter support team (July 12, 2023, 7:40 AM) (on file with the Comm.).

¹¹¹ See STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

IV. NSF IS TRYING TO COVER UP ITS FUNDING OF AI CENSORSHIP

Following congressional oversight and media scrutiny, Executive Branch agencies in the censorship-industrial complex often try to hide their involvement. For example, in early 2023, CISA scrubbed its website of mentions to “domestic actors” on its mis-, dis-, malinformation page.¹¹² In 2022, CISA considered using third parties to avoid the scrutiny that followed the public backlash to the Disinformation Governance Board.¹¹³

Throughout the entire Track F funding process, NSF has been closely tracking any signs of political or media attention on its misconduct. NSF developed an extensive “media strategy” and instructed the Track F teams on what they could or should say about their censorship projects. At one point, NSF considered blacklisting certain conservative media outlets that were covering NSF.

A. NSF Developed an Official Media Strategy to Hide its Track F Censorship Program from the American People

In the fall of 2021, various media outlets began reporting on NSF-funded Track F projects, sounding the alarm about how American taxpayer money might be funding the development of tools to censor and indoctrinate Americans.¹¹⁴

On September 27, 2021, one week after NSF started issuing Track F awards, Katelynn Richardson, then at *Campus Reform*, reported on how NSF was providing millions to universities to develop tools and techniques to address alleged misinformation. Her reporting highlighted multiple Track F projects, including Wisconsin’s CourseCorrect and Michigan’s WiseDex, and cited comments made by the head researchers explaining how they would design and test the propaganda and censorship tools.¹¹⁵

The following month, on October 22, 2021, *Campus Reform* published another article on Track F, this time highlighting a project led by researchers at Temple University. The article cited an interview in which Eduard Dragut, the lead Temple University researcher on the \$750,000 project, admitted that his team planned to “use natural language processing algorithms along with social networking tools to mine the communities where [misinformation] may happen.”¹¹⁶

¹¹² See STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023), at 32-34.

¹¹³ *Id.* at 27.

¹¹⁴ See Katelynn Richardson, *NSF grants nearly \$7.5 million to universities developing anti-'misinformation' tools*, CAMPUS REFORM (Sept. 27, 2021); Katelynn Richardson, *Federal Gov Pays University \$750K to Create Tool That Warns Journalists Against Publishing 'Polarizing' Content*, CAMPUS REFORM (Oct. 22, 2021); see also Reclaim The Net, *University Receives \$750k of Federal Funds to Stop Reporters From Creating "Negative Unintended Outcomes"*, INFOWARS (Oct. 25, 2021).

¹¹⁵ Katelynn Richardson, *NSF grants nearly \$7.5 million to universities developing anti-'misinformation' tools*, CAMPUS REFORM (Sept. 27, 2021).

¹¹⁶ Katelynn Richardson, *Federal Gov Pays University \$750K to Create Tool That Warns Journalists Against Publishing 'Polarizing' Content*, CAMPUS REFORM (Oct. 22, 2021).

A few days later, on October 26, Michael Pozmantier, NSF’s Track F program manager, began emailing the head researchers about the need to devise a Track F-specific “media/outreach strategy” to inform how NSF and the research teams would handle the media going forward.¹¹⁷

From: "Pozmantier, Michael" <[REDACTED]@nsf.gov>
Date: Tuesday, October 26, 2021 at 3:17 PM
To: [REDACTED]@mit.edu, [REDACTED]@uw.edu, [REDACTED]
 [REDACTED]@hackshackers.com, [REDACTED]@email.gwu.edu, [REDACTED]
 [REDACTED]@buffalo.edu, Paul Resnick <[REDACTED]@umich.edu>, [REDACTED]@cse.ohio-
 state.edu, [REDACTED]@temple.edu, [REDACTED]@uci.edu, Michael Wagner
 <[REDACTED]@wisc.edu>, [REDACTED]@uw.edu, Scott Hale <[REDACTED]@meedan.com>
Subject: Media/Outreach Strategy

In his email, Pozmantier referred to the *Campus Reform* article as the latest example of “misinfo and attacks” against “researchers in this space,” adding that “NSF leadership and public affairs” needs to be “better equipped to deal with what’s coming.”¹¹⁸

Pls,

As you all know and have likely dealt with for quite a while, researchers in this space are subject to misinfo and attacks. An article was just released about one of the projects in the track and it has ginned up the usual joyful response, it makes sense for us to discuss how we (NSF) should handle this going forward. Given that there are no better people anywhere to help us with this, I’d like to schedule a meeting with all of you to discuss. You each can include one other person from your team who has experience with this if you’d like but I’d prefer that we keep this meeting reasonably sized, so it is manageable. Plus, the more people, the harder it is to schedule.

This discussion will lead to others, I plan to engage NSF leadership and public affairs soon after our conversation so that they can be better equipped to deal with what’s coming and try to find ways to avoid issues where possible based on your input and guidance. By NSF doing a better job, hopefully we can avoid causing any new issues for you as well.

Shortly thereafter, Pozmantier emailed Michael Wagner, the head researcher for Wisconsin’s CourseCorrect team, saying, “I knew [blowback] was a possibility, just a question of who is actually paying attention to what we’re doing.”¹¹⁹

From: "Pozmantier, Michael" <[REDACTED]@nsf.gov>
Subject: Re: [EXTERNAL] - Re: Media/Outreach Strategy
To: Michael Wagner <[REDACTED]@wisc.edu>
Date: October 26, 2021 3:56:21 PM CDT

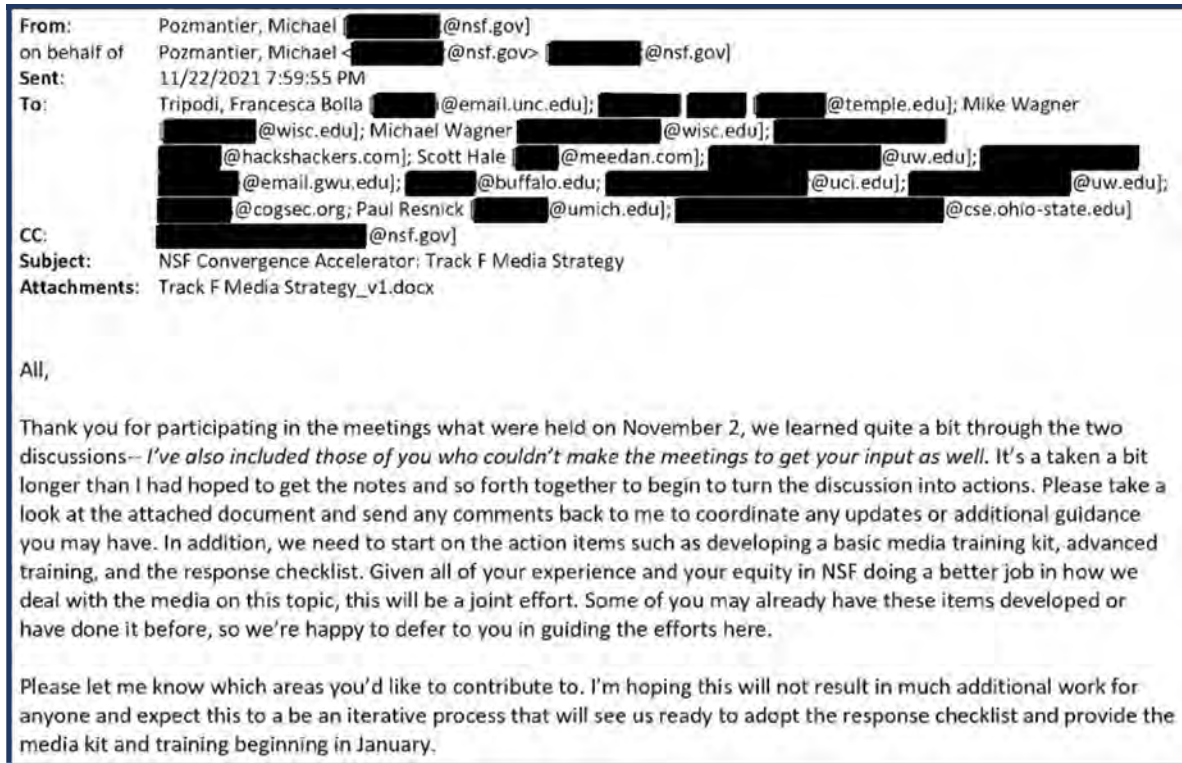
I knew it was a possibility, just a question of who is actually paying attention to what we’re doing. It’s amazing how few people know what NSF, so I thought any blowback would come from other places.

¹¹⁷ Email from Michael Pozmantier to NSF Track F grantees (Oct. 26, 2021, 3:17 PM) (on file with the Comm.).

¹¹⁸ *Id.*

¹¹⁹ Email from Michael Pozmantier to Michael Wagner (Oct. 26, 2021, 3:56 PM) (on file with the Comm.).

On November 2, 2021, NSF held two meetings with the research teams to develop an official “Track F Media Strategy.” In a November 22, 2021 email attaching a first draft of NSF’s Track F media strategy, Pozmantier emphasized that “a joint effort” would be required for NSF to do “a better job in how we deal with the media on this topic,” including “training” for the researchers “beginning in January.”¹²⁰



The Track F Media Strategy document begins by noting that because Track F “is a controversial topic, it’s important for NSF to proactively develop a strategy to enable the Foundation and funded researchers to be in sync,” adding that “many” of the Track F researchers “have extensive experience dealing with this issue.”¹²¹

Knowing that Track F is a controversial topic, it’s important for NSF to proactively develop a strategy to enable the Foundation and funded researchers to be in sync. Additionally, many of the PIs, Co-PIs, and Sr. Personnel working on Track F projects have extensive experience dealing with this issue. Two meetings were organized by the Convergence Accelerator to draw upon this expertise, to develop the strategy to help prevent or lessen opportunities for the spreading of misinformation about the Track.

The result of these meetings was a set of recommended activities and artifacts to be developed by NSF, the Convergence Accelerator, and the teams to be used to assist in minimizing and responding to issues. The information would also be shared with NSF’s Office of Legislative and Public Affairs and other relevant parties.

¹²⁰ Email from Michael Pozmantier to NSF Track F grantees, attaching “Track F Media Strategy” document (Nov. 22, 2021, 7:59 PM) (on file with the Comm.).

¹²¹ First Draft of NSF’s Track F Media Strategy entitled “Track F Media Strategy_v1.docx,” at 1 (on file with the Comm.); *see also* App’x B.

The strategy then provides specific recommendations for the Track F research teams when dealing with the media, such as “always highlight the pro-democracy nature of the Track and each project” and “if possible, focus on the non-ideological nature of work”—even if, as NSF privately acknowledged, showing “both sides can distort” who is really being censored.¹²²

Recommendations

Messaging:

- Always highlight the pro-democracy nature of the Track and each project
- Always be accurate, any inaccuracies can be a hanging thread to be pulled
- If possible, focus on the non-ideological nature of work
 - Give examples of both sides ******(I’m not a fan of always trying to show both sides because they are not always equal in impact and showing both sides can distort)
 - When it’s possible, use sports metaphors
- Focus on the scientific process

Protective Measures:

- Subscribe to monitoring service(s) to proactively help manage when project information is published and possibly miscommunicated.
- Subscribe to scrubbing services, such as DeleteMe

The media strategy document also reveals how NSF developed and required the Track F research teams to receive “media training” with “key messaging about the NSF Convergence Accelerator, Track F, [and] each funded project.”¹²³

Media Training:

Develop and provide media training to NSF Convergence Accelerator staff and funded researchers understand media engagement best practices, internal communication processes, and standard messaging. The multi-level training will include basic training and an advanced training.

- Multi-level
 - Basic training
 - Media engagement best practices
 - Interview requests (e.g., Who to involve, when to provide a written statement or have a live interview, etc.)
 - Speaking in plain language
 - Highlighting the scientific strategy, value and impact
 - Reporter terminology (e.g., What does it mean to be ‘On the record’, ‘Off the record, or ‘On background’?)
 - Standard key messaging about the NSF Convergence Accelerator, Track F, each funded project

¹²² *Id.*

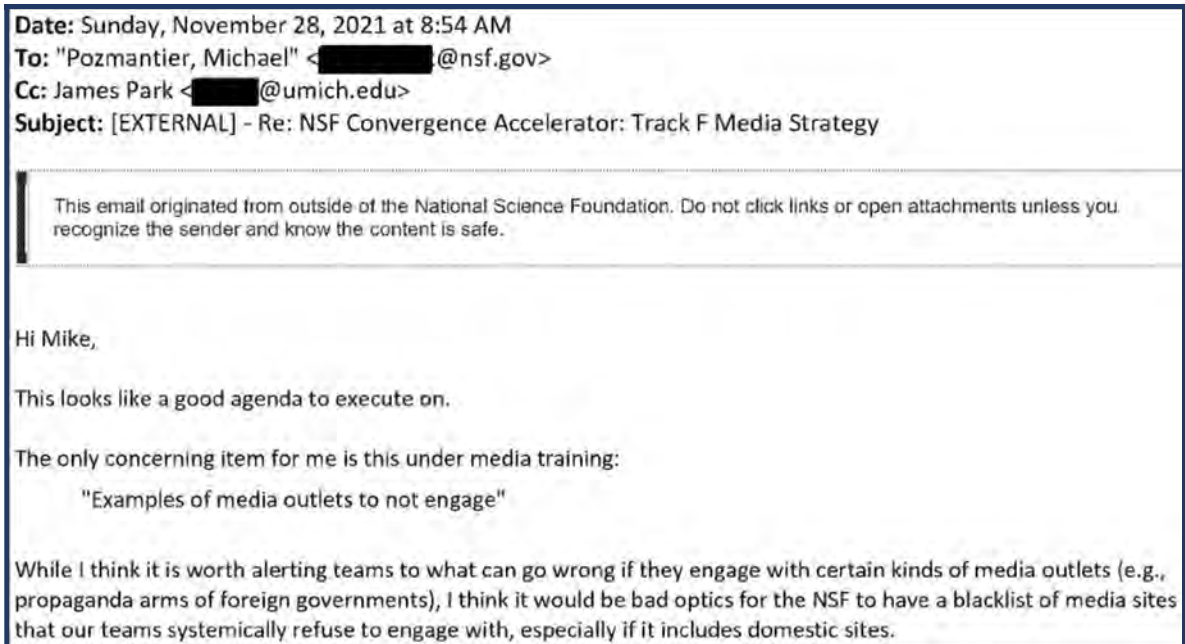
¹²³ First Draft of NSF’s Track F Media Strategy entitled “Track F Media Strategy_v1.docx,” at 2 (on file with the Comm.); *see also* App’x B.

B. NSF Considered Blacklisting Conservative Media Outlets

The Track F “Media Strategy” memo reveals that NSF initially planned to instruct the Track F teams—groups that received federal taxpayer dollars—about which “media outlets to not engage” as part of its “basic training.”¹²⁴

- Examples of media outlets to not engage
- Processes: Notifying your organization of the media request, when to notify NSF
- Advanced
 - Harassment:
 - How to respond to harassment (accompanied by Checklist)
 - Who to notify if harassment is received

After reviewing the media strategy, the head researcher for Michigan’s WiseDex project expressed his concerns to Pozmantier that a media blacklist “would be bad optics,” noting that, “[w]hile I think it is worth alerting teams to what can go wrong if they engage with certain kinds of media outlets . . . , I think it would be bad optics for the NSF to have a blacklist of media sites that our teams systemically refuse to engage with, especially if it includes domestic sites.”¹²⁵



Pozmantier replied, “I agree 100%, that shouldn’t be in there. I’ll remove it.”¹²⁶

¹²⁴ *Id.*

¹²⁵ Email from Paul Resnick to Michael Pozmantier (Nov. 28, 2021, 8:54 AM) (on file with the Comm.) (emphases added).

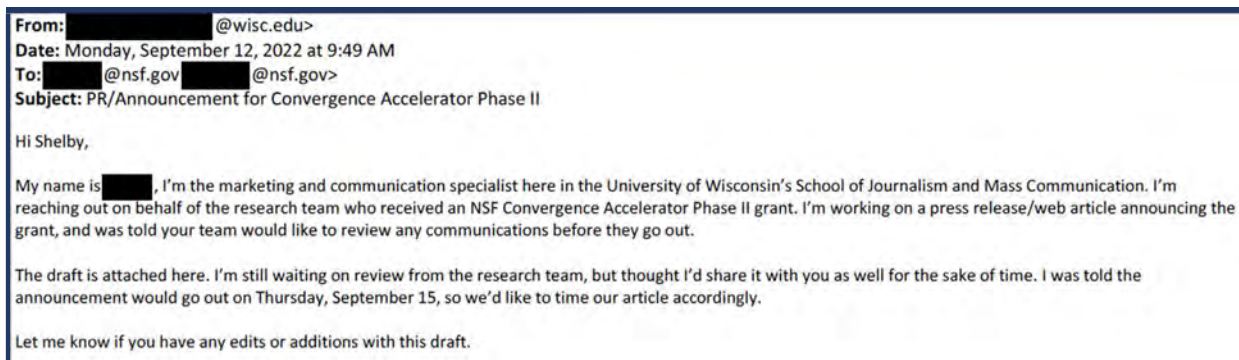
¹²⁶ Email from Michael Pozmantier to Paul Resnick (Nov. 29, 2021, 2:12 PM) (on file with the Comm.).

C. NSF Attempted to Hide Additional Funding to Its Track F Censorship Program

In August 2022, when the time came for NSF to announce which Track F projects would receive an additional \$5 million in Phase 2 funding, NSF quietly decided to not issue a press release, although its typical practice was to do so.¹²⁷ When NSF announced the \$30 million that Track E recipients would be receiving in Phase 2, a similar announcement of the equal amount of taxpayer dollars being provided to Track F recipients was conspicuously absent.¹²⁸

Rather, NSF maintained a tight hold on the information, providing clear instructions to any Track F teams who might be interested in announcing their Phase 2 awards. In an August 19, 2022 email to the six Track F teams selected for Phase 2 funding, Pozmantier explained that “NSF will not be including this track in the Phase 2 press release, only Track E will be announced,” adding that any research teams interested in announcing their Phase 2 awards should coordinate with NSF to do so.¹²⁹

It also appears that NSF asked the Track F teams to get formal approval from NSF before issuing press releases, publishing articles, or responding to media inquiries relating to the program, and that the researchers complied, checking with NSF before responding to media inquiries.¹³⁰ For example, on September 12, 2022, a University of Wisconsin public relations employee emailed Shelby Smith, the communications and outreach director for NSF’s Convergence Accelerator, writing, “I’m working on a press release/web article announcing the [Phase 2] grant, and was told your team would like to review any communications before they go out.”¹³¹



To date, NSF continues to maintain an announcement on its website for the Phase 2 recipients of *every* track except for Track F.¹³² To be clear, this is *not* because the Track F

¹²⁷ Email from Michael Pozmantier to NSF Track F “Phase 2 Cohort” (Aug. 19, 2022, 12:13 PM) (on file with the Comm.).

¹²⁸ See *Convergence Accelerator Portfolio*, NAT. SCI. FOUND., <https://new.nsf.gov/funding/initiatives/convergence-accelerator/portfolio>.

¹²⁹ Email from Michael Pozmantier to NSF Track F “Phase 2 Cohort” (Aug. 19, 2022, 12:13 PM) (on file with the Comm.).

¹³⁰ See, e.g., email from Paul Resnick to Michael Pozmantier (Jan. 31, 2023, 5:02 PM) (on file with the Comm.).

¹³¹ Email from Wisconsin marketing and communication specialist to NSF personnel (Sept. 12, 2022, 9:49 AM) (on file with the Comm.).

¹³² See *Convergence Accelerator Portfolio*, NAT. SCI. FOUND., <https://new.nsf.gov/funding/initiatives/convergence-accelerator/portfolio>.

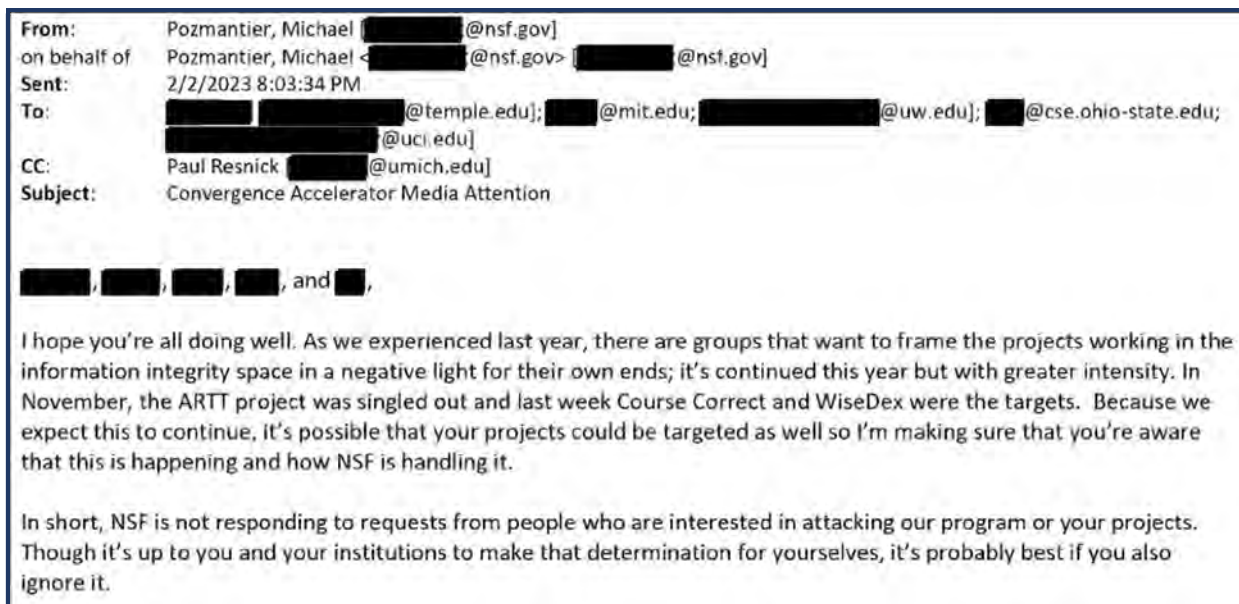
program ended or because no teams were selected to receive further funding. Rather, it appears that NSF recognized that the American people would not respond kindly to the announcement that an additional \$30 million was being allocated to projects aimed at indoctrinating and silencing them.

D. NSF Continues to Try to Cover Up Its Funding of Censorship Tools

In 2022, NSF created an official media strategy and made the calculated decision to not announce Track F’s Phase 2 recipients. NSF’s cover up of its censorship program continued into at least 2023.

For example, on January 31, 2023, a few days after Pozmantier advised Paul Resnick, the head researcher for Michigan’s WiseDex team, to not respond to media inquiries, Resnick followed up again with another “reporter inquiry” about whether “Twitter use[s] WiseDex as a vendor,” noting that he wanted to check with Pozmantier “before responding.”¹³³ Pozmantier ultimately replied: “NSF would probably stay away.”¹³⁴

Days later, on February 2, 2023, Pozmantier emailed the Track F teams, outlining the various Track F projects receiving media attention, including WiseDex and CourseCorrect, and explaining “how NSF is handling it.”¹³⁵ “In short, NSF is not responding to requests from people who are interested in attacking our programs or your projects,” Pozmantier wrote, adding “it’s probably best if you also ignore it.”¹³⁶



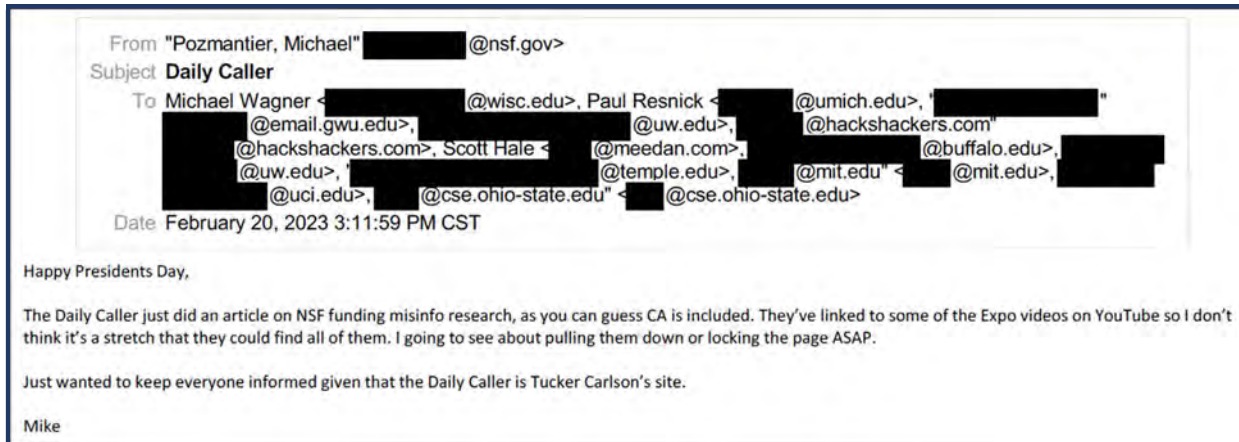
¹³³ Email from Paul Resnick to Michael Pozmantier (Jan. 31, 2023, 5:02 PM) (on file with the Comm.).

¹³⁴ Email from Michael Pozmantier to Paul Resnick (Jan. 31, 2023, 10:10 PM) (on file with the Comm.).

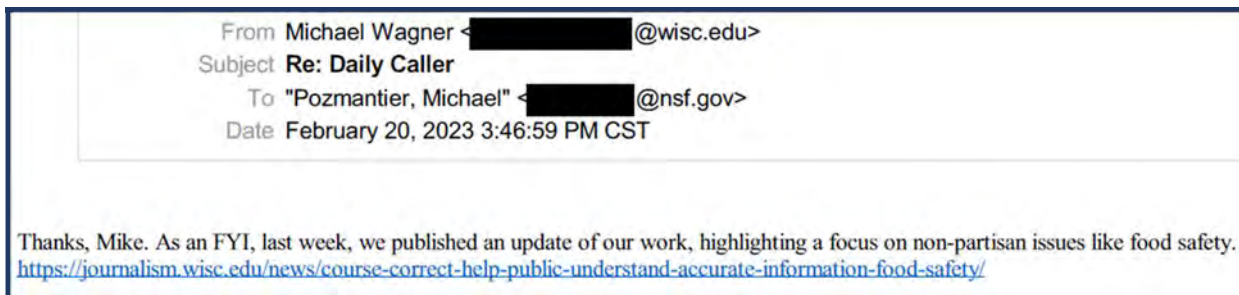
¹³⁵ Email from Michael Pozmantier to the head researchers of the Phase 2 Track F teams (Feb. 2, 2023, 8:03 PM) (on file with the Comm.).

¹³⁶ *Id.*

A couple weeks later, in late February 2023, when Katelynn Richardson, now at the *Daily Caller*, published an article on “NSF funding misinfo research,” and “linked to some of the Expo videos on YouTube,” Pozmantier quickly emailed the heads of each of the research teams, warning them of the article.¹³⁷ He also noted that he was “going to see about pulling [the Track F Expo videos on YouTube] down or locking the page ASAP.”¹³⁸



In response to this email, Michael Wagner, the head researcher for Wisconsin's CourseCorrect team, assured Pozmantier that his team had recently issued a statement emphasizing that CourseCorrect is focused on “non-partisan issues like food safety.”¹³⁹

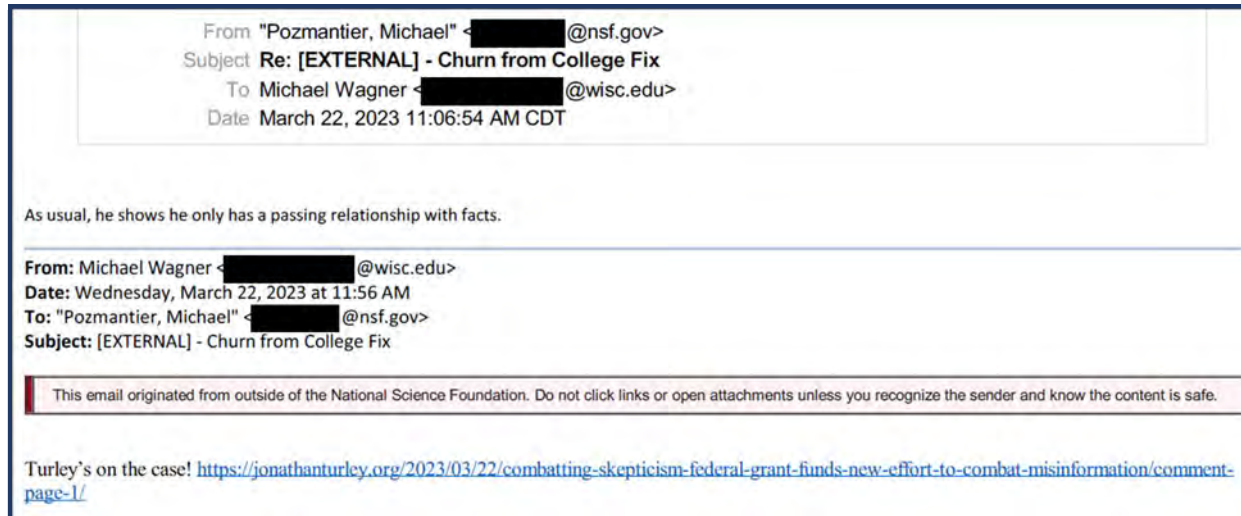


¹³⁷ Email from Michael Pozmantier to the head researchers of each the twelve Track F grants (Feb. 20, 2023, 3:12 PM) (on file with the Comm.).

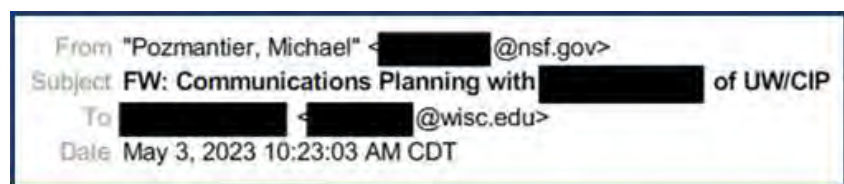
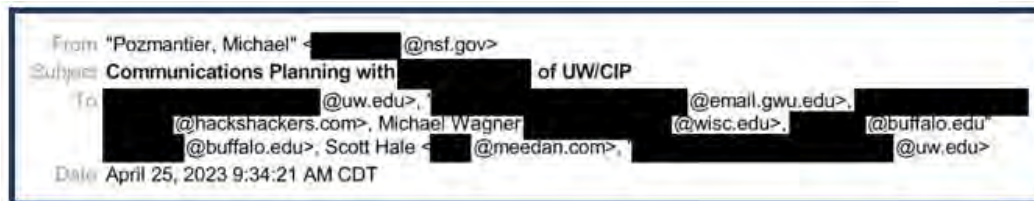
¹³⁸ *Id.*

¹³⁹ Email from Michael Wagner to Michael Pozmantier (Feb. 20, 2023, 3:46 PM) (on file with the Comm.).

In March 2023, Wagner flagged for Pozmantier a recent article from legal scholar Jonathan Turley about the projects NSF had been funding, writing mockingly that “Turley’s on the case!”¹⁴⁰ Pozmantier revealed his contempt for the legal scholar, writing “[a]s usual, he shows he only has a passing relationship with the facts,” without identifying any shortcomings in Turley’s article.¹⁴¹



In April 2023, the situation had progressed such that Pozmantier started organizing “communications planning” meetings for the Track F teams,¹⁴² which continued into May.¹⁴³



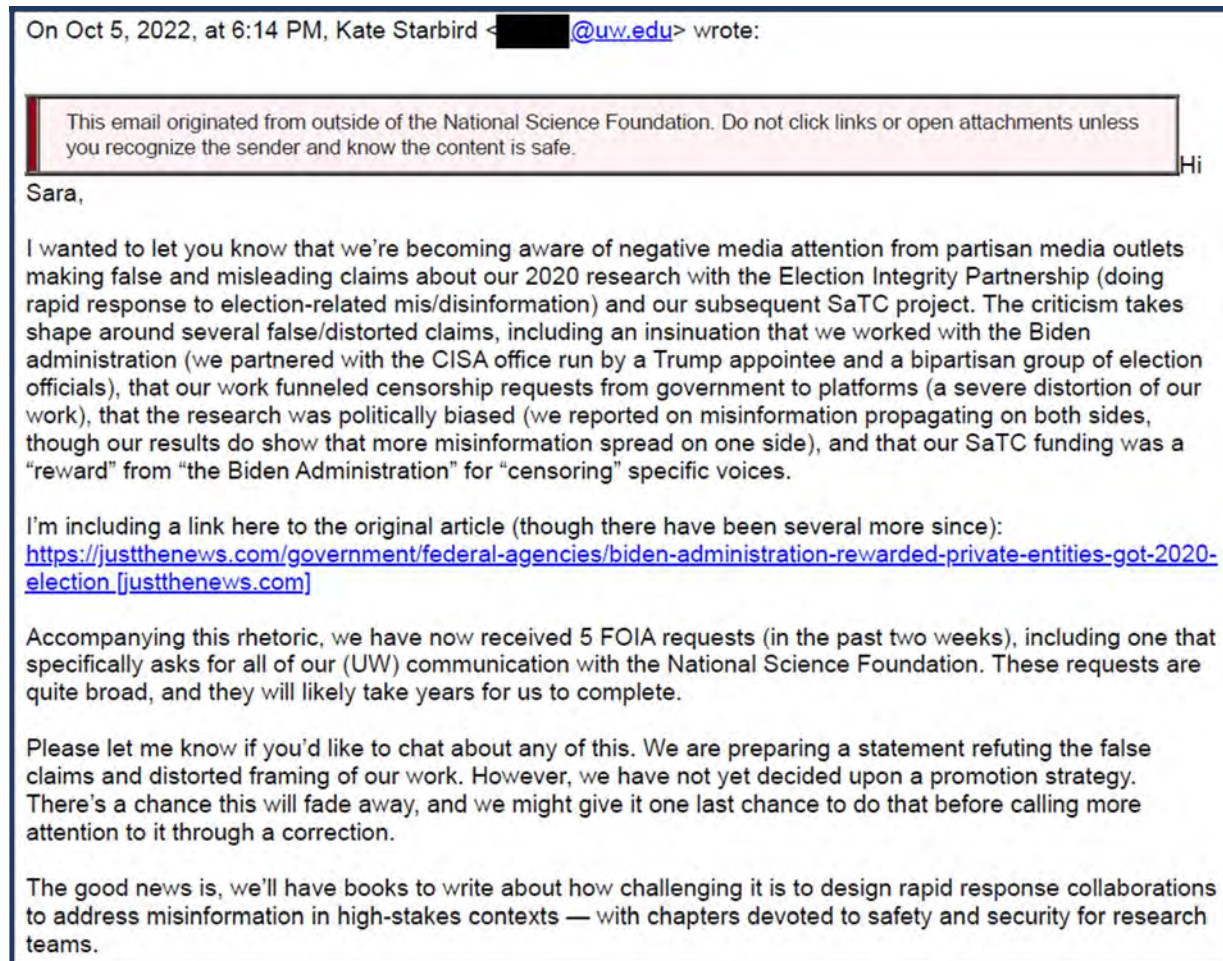
¹⁴⁰ Email from Michael Wagner to Michael Pozmantier (March 22, 2023, 11:56 AM) (on file with the Comm.).

¹⁴¹ Email from Michael Pozmantier to Michael Wagner (March 22, 2023, 11:06 AM) (on file with the Comm.).

¹⁴² Email from Michael Pozmantier to Track F Recipients (Apr. 25, 2023, 9:34 AM) (on file with the Comm.).

¹⁴³ Email from Michael Pozmantier to Track F Recipients (May 3, 2023, 10:23 AM) (on file with the Comm.).

NSF and researchers receiving taxpayer-funded NSF grants coordinated their responses to media coverage of other NSF fundings as well. For example, on September 29, 2022, *Just the News* wrote an article on NSF’s multi-million-dollar grants to Stanford and the University of Washington through its Secure and Trustworthy Cyberspace (SaTC) program.¹⁴⁴ Like the Track F projects, the projects funded through NSF’s SaTC were also focused on countering so-called “(mis/dis)information online.”¹⁴⁵ In response, on October 5, 2022, Dr. Kate Starbird, the head of the University of Washington’s Center for an Informed Public, emailed Sara Kiesler, an NSF official, warning that “partisan media outlets [are] making false and misleading claims” about her work.¹⁴⁶ Linking to the *Just the News* article, Dr. Starbird criticized the claim that her “SaTC funding was a ‘reward’ from ‘the Biden Administration’ for ‘censoring’ specific voices.”¹⁴⁷



¹⁴⁴ Greg Piper and John Solomon, *Outsourced censorship: Feds used private entity to target millions of social posts in 2020*, JUST THE NEWS (Sept. 29, 2022).

¹⁴⁵ *Id.* (quoting UW’s press release: Michael Grass, *\$2.25 Million in NSF Funding Will Support Center for an Informed Public Research*, UNIVERSITY OF WASHINGTON INFORMATION SCHOOL (Aug. 17, 2021). Stanford and UW were two key personnel in the EIP. See STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH* (Comm. Print Nov. 6, 2023).

¹⁴⁶ Email from Dr. Kate Starbird to NSF personnel (Oct. 5, 2022, 6:14 PM) (on file with the Comm.).

¹⁴⁷ *Id.*

E. NSF Is Attempting to Stonewall Congressional Investigations

On January 24, 2023, Pozmantier emailed Paul Resnick, the head researcher for Michigan’s WiseDex project, mentioning that Senator Joni Ernst wrote NSF a “letter of inquiry” in November 2022 regarding a particular Track F project that had gained media attention.¹⁴⁸ However, just a few days later, in a February 2, 2023 email, Pozmantier noted that “NSF is not responding to requests from people who are interested in attacking our program.”¹⁴⁹ Taken together, these emails raise questions as to whether NSF’s lack of transparency on Track F would extend to openly defying information requests from Congress.

These emails may also help explain why NSF has failed to provide the Committee and Select Subcommittee with an appreciable volume of documents and information responsive to the requests sent more than nine months ago in May 2023 pursuant to the Committee’s ongoing investigation.¹⁵⁰ To date, NSF has produced a mere 294 pages to the Committee in response to requests for documents and information relating to its Track F program, maintaining an iron grip on much of the substantially relevant information in its possession and obstructing the Committee and Select Subcommittee’s investigation for over half a year.¹⁵¹

Time and again, NSF engaged in efforts to hide its Track F censorship program from the American people, training the research teams on how to avoid media scrutiny and refusing to respond substantively to congressional requests itself. The extent to which NSF has gone to shield its taxpayer-funded censorship research raises serious concerns that NSF knows its research activities violate the Constitution and fundamental civil liberties.

V. THE ROLE OF CONGRESS: DEFUND THE CENSORSHIP-INDUSTRIAL COMPLEX AND FIGHT THE NEXT BATTLE TO DEFEND FREE SPEECH

If you *don’t* agree with the prevailing niche morality that is being imposed on both social media and AI via ever-intensifying speech codes, you should also realize that the fight over what AI is allowed to say/generate will be even more important – by a *lot* – than the fight over social media censorship. AI is highly likely to be the control layer for everything in the world. How it is allowed to operate is going to matter perhaps more than anything else has ever mattered. You should be aware of how a small and isolated coterie of partisan social engineers are trying to determine that right now, under cover of the age-old claim that they are protecting you.

In short, don’t let the thought police suppress AI.¹⁵²

– Marc Andreessen, June 6, 2023

¹⁴⁸ Email from Michael Pozmantier to Paul Resnick (Jan. 24, 2023, 9:53 PM) (on file with the Comm.).

¹⁴⁹ Email from Michael Pozmantier to researchers, copying Paul Resnick (Feb. 2, 2023) (on file with the Comm).

¹⁵⁰ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Dr. Sethuraman Panchanathan, Dir., Nat. Sci. Found. (May 1, 2023) (on file with the Comm.).

¹⁵¹ NSF Production to the House Judiciary Committee (Aug. 25, 2023) (on file with Comm.); NSF Production to the House Judiciary Committee (Dec. 15, 2023) (on file with Comm.); NSF Production to the House Judiciary Committee (Feb. 5, 2024) (on file with Comm.).

¹⁵² See Marc Andreessen, *Why AI Will Save the World*, ANDREESEN HOROWITZ (June 6, 2023) (emphases in original).

The Committee and the Select Subcommittee will continue their investigation to understand the full threat to free speech in order to inform legislative solutions, such as prohibiting NSF from funding projects used to monitor speech. Matt Taibbi and Michael Shellenberger, two of the journalists at the forefront of this issue, have testified before the Select Subcommittee on the intersection of government, Big Tech, universities, and other third parties, dubbing the enterprise the “censorship-industrial complex.”¹⁵³ But just how big is the censorship-industrial complex? One of the key players, Meedan, estimated that market in 2022 for “content moderation solutions” was \$10 billion.¹⁵⁴



With the power of the purse, the House of Representatives is uniquely positioned to legislate to protect fundamental First Amendment rights and end the censorship-industrial complex by draining it of its key resource: American taxpayer dollars. To be sure, other legislative solutions have been, and will continue to be, considered. Moreover, mainstream outlets are reporting that universities in the censorship-industrial complex are “ending” their disinformation programs because of civil liberties concerns identified by the Committee’s and Select Subcommittee’s investigation.¹⁵⁵

These successes notwithstanding, the urgency of the situation cannot be overstated. New technologies are being developed that represent a threat of a different magnitude to online speech, and with it, the modern town square. At a minimum, American taxpayers should not be funding the tools that may take away one of their most important and fundamental rights. The Committee and Select Subcommittee will continue to investigate and legislate to protect Americans’ freedom of speech against threats old and new.

¹⁵³ See *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 9, 2023) (statements of Matt Taibbi and Michael Shellenberger).

¹⁵⁴ Meedan’s Oral Pitch Slide Deck, *supra* note 74, at 24.

¹⁵⁵ Naomi Nix et al., *Misinformation research is buckling under GOP legal attacks*, WASH. POST (Sept. 23, 2023).

Appendix A



National Science Foundation
Office of the Director

June 13, 2023

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Jordan:

Thank you for your letter regarding content moderation on technology and social media platforms. The U.S. National Science Foundation (NSF) takes very seriously our responsibilities to the public, and strong oversight and stewardship of taxpayer dollars are vital to NSF's ability to deliver on its mission to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense. I appreciate the opportunity to respond to your questions and NSF staff are working diligently to identify all responsive records.

For more than seven decades, NSF has been a critical component in powering the United States economy, transforming American lives, and securing the national defense. NSF advances research and innovation and American competitiveness by investing in foundational, curiosity-driven, discovery research, as well as use-inspired, solution-oriented innovations to advance key technologies and address societal and economic challenges. Many of the technological advances we are benefiting from today such as Artificial Intelligence, Quantum Information Science, and Biotechnology are rooted in sustained investment over many decades. However, we currently face intense global competition in the race to develop these technologies and the workforce needed to secure the future of innovation. Our success in unlocking the promise of these and other technological developments and scientific breakthroughs will determine our continued global leadership and are central to our economic and national security.

Among the areas in which NSF is a leader on behalf of the U.S. Government is next-generation communication networks and systems. For example, NSF investments over the last two decades have led to millimeter wave technologies, dynamic spectrum sharing, and open radio access networks (OpenRAN), which are enabling the fifth, sixth, and future generations of wireless networks ("5G" and "6G"). As part of this mission, it is critical that NSF also invests in tools, technologies, and approaches to prevent, mitigate and adapt to critical threats to communication systems and assist end users with knowledge to make informed decisions.

NSF uses a rigorous [merit review process](#) to ensure funding decisions are based on a fair, competitive, and transparent process, consistent with NSF's broad mission as well as specific direction from Congress. Each proposal submitted to NSF is reviewed by science and engineering experts well-versed in their particular discipline or field of expertise. Further, All each proposal submitted to NSF is reviewed according to two merit review criteria: Intellectual

Merit and Broader Impacts. NSF's merit review process is widely considered to be the "gold standard" of scientific review. Perhaps the best evidence of NSF's success is the repeated replication of its merit review model for discovery, education and innovation around the globe. The Internet, 3D printing, the economic theory underpinning spectrum auctioning and kidney exchanges, and the first image of a black hole are all examples of the power of NSF investments in innovations and innovators.

In recent years, Congress has called on NSF to engage the research community to identify and address issues of safety, ethics and adversarial influence online. Examples of this Congressional direction include:

House Report 117-395, as referenced by the joint explanatory statement accompanying Division B, the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2023, of the FY2023 Consolidated Appropriations Act (P.L. 117-328):

Trustworthy Algorithmic Research.—The Committee urges NSF to increase support for research into the safety and ethical effects of content moderation and recommendation algorithms that will advance new technical methods to reduce the likelihood of unexpected negative effects from these algorithms. The Foundation shall further consider using the special authority provided under Section 5401 (f) of the National Artificial Intelligence Initiative Act, Public Law 116–283, to carry out this research. No later than 180 days after the enactment of this Act, NSF shall provide the Committee with a report on its efforts to prioritize such research.

The joint explanatory statement accompanying Division B, the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2022, of the FY2022 Consolidated Appropriations Act (P.L. 117-103):

Online Influence. —NSF is encouraged to consider additional research efforts that will help counter influence from foreign adversaries on the Internet and social media platforms designed to influence U.S. perspectives, sow discord during times of pandemic and other emergencies, and undermine confidence in U.S. elections and institutions. To the extent practicable, NSF should foster collaboration among scientists from disparate scientific fields and engage other Federal agencies and NAS to help identify areas of research that will provide insight that can mitigate adversarial online influence, including by helping the public become more resilient to undue influence.

The Identifying Outputs of Generative Adversarial Networks (IOGAN) Act (P.L. 116-258):

Sec. 3. NSF support of research on manipulated or synthesized content and information security.

The Director of the National Science Foundation, in consultation with other relevant Federal agencies, shall support merit-reviewed and competitively awarded research on manipulated or synthesized content and information authenticity, which may include—

- (1) fundamental research on digital forensic tools or other technologies for verifying the authenticity of information and detection of manipulated or synthesized content, including content generated by generative adversarial networks;
- (2) fundamental research on technical tools for identifying manipulated or synthesized content, such as watermarking systems for generated media;
- (3) social and behavioral research related to manipulated or synthesized content, including human engagement with the content;
- (4) research on public understanding and awareness of manipulated and synthesized content, including research on best practices for educating the public to discern authenticity of digital content; and
- (5) research awards coordinated with other federal agencies and programs, including the Defense Advanced Research Projects Agency and the Intelligence Advanced Research Projects Agency, with coordination enabled by the Networking and Information Technology Research and Development Program.

NSF has a long history of addressing these types of priority research areas through special-emphasis programs and public-private partnership to address potential biases in AI systems, with the goal of contributing to the trustworthiness of such systems. For example, the NSF Program on Fairness in AI in Collaboration with Amazon supports building trustworthy AI systems to tackle grand challenges facing society. Specific topics of interest include transparency, explainability, accountability, integrity, mitigation strategies, validation, and inclusivity. NSF's independent merit review process ensures projects funded through this collaboration enable broadened acceptance of AI systems, helping the U.S. further capitalize on the potential of AI technologies. NSF also joined with the Partnership on AI (PAI), a multistakeholder organization that brings together academic researchers, industry, civil society organizations, and other groups working together to better understand AI's impact on society, to support projects exploring the social challenges arising from AI technology and enabling scientific contributions to overcome them.

NSF's investments also aim to enhance authentic and trustworthy information and dissemination in cyberspace. For example, NSF's Secure and Trustworthy Cyberspace (SaTC) program includes, among its research topics of interest, information integrity, and particularly emerging threat models stemming from unverifiable information provenance. This includes adversarial machine learning threats in model training, deployment, and reuse; privacy risks, including model inversion and risks to individuals such as re-identification, and de-anonymization; and forensic and formal methods for analyzing, auditing, and verifying security- and privacy-related issues of AI components.

A key element of strengthening resilience against information manipulation is to empower individuals through education on how to recognize, create, consume, and propagate trustworthy information and to identify corrupted information. NSF investments support research to develop effective educational and digital literacy pathways for all age levels, demographics, and

technological experiences. The SaTC program also supports evidence-based and evidence-generating methods to improve cybersecurity education and workforce development at the K-12, undergraduate, graduate, and professional education levels. This includes approaches to improve cybersecurity learning and learning environments, new educational materials and methods of instruction, and assessment tools to measure student learning.

In your letter, you requested information specifically about NSF's Convergence Accelerator Track F: Trust & Authenticity in Communications Systems. The NSF Convergence Accelerator supports the development of new technologies that address pressing societal and economic challenges for the Nation. This particular Convergence Accelerator track is addressing the urgent need for tools and techniques that help the Nation more effectively prevent, mitigate, and adapt to critical risks to the trust and authenticity in communication systems.

The NSF Convergence Accelerator follows an ideation process for selecting convergent research topics, or "tracks," for the program's yearly cohort. The ideation process involves gathering ideas and insights from the research and innovation community to include community workshops and findings. Selected ideas must also be grounded in scientific research, suitable for a convergent approach, advance key technologies, and address a societal or economic challenge.

The selection process for Track F began in March 2020 by issuing a Dear Colleague Letter, Request for Information on Future Topics (NSF-20-061). Based on the community input, two workshop topics were chosen for the 2021 cohort track topics, one being Track F: Trust & Authenticity in Communication Systems. The selection of the topic and the subsequent workshop occurred in 2020, during the Trump Administration. The subsequent funding opportunity was released in early 2021. Track F: Trust & Authenticity in Communication Systems was selected to assist the Nation with effectively preventing, mitigating, and adapting to critical threats to national security in the form of communication systems that our adversaries seek to disrupt or exploit to negatively impact U.S. businesses, platforms, networks and more. We continue to believe it is vital for the U.S. to understand how to be resilient to these types of attacks and has the tools to do so.

In September 2021, NSF awarded up to \$750,000 per team and \$9 million total to twelve Track F Phase 1 teams. At the end of Phase 1, teams competed to advance to Phase 2, as envisioned in the original solicitation and consistent with all Convergence Accelerator tracks. NSF selected six Track F teams for Phase 2, awarding up to \$5 million per team or \$30 million total over 24 months. Please find below all the awards made through the Track F program with links that will take you to the award summaries and additional information.

[NSF Convergence Accelerator Track F: America's Fourth Estate at Risk: A System for Mapping the \(Local\) Journalism Life Cycle to Rebuild the Nation's News Trust](#)

Award Number:2137846; Organization: Temple University; Start Date:10/01/2021; Award Amount: \$750,000.00.

NSF Convergence Accelerator Track F: An Algorithmic Observatory to Address Financial Misinformation and Disinformation in Minoritized Communities (LOI ID: L02616265)

Award Number:2137567; Organization: University of California-Irvine; Start Date: 10/01/2021; Award Amount: \$750,000.00.

NSF Convergence Accelerator Track F: Adapting and Scaling Existing Educational Programs to Combat Inauthenticity and Instill Trust in Information

Award Number:2137530; Organization: Massachusetts Institute of Technology; Start Date: 10/01/2021; Award Amount: \$750,000.00.

NSF Convergence Accelerator Track F: Building Trust in Communication Systems by Addressing Misinformation-Driven Online Abuse and Harassment

Award Number:2137448; Organization: George Washington University; Start Date: 10/01/2021; Award Amount: \$749,222.00.

NSF Convergence Accelerator Track F: Co-designing for Trust: Reimagining Online Information Literacies with Underserved Communities

Award Number:2230616; Organization: University of Washington; Date: 10/01/2022; Award Amount: \$2,611,462.00.

NSF Convergence Accelerator Track F: Expert Voices Together: Building Trust in Communication Systems by Addressing Online Abuse and Harassment

Award Number:2230683; Organization: George Washington University; Start Date: 09/15/2022; Award Amount: \$2,691,316.00.

NSF Convergence Accelerator Track F: Course Correct: Precision Guidance Against Misinformation

Award Number:2230692; Organization: University of Wisconsin-Madison; Start Date: 09/15/2022; Award Amount: \$2,370,316.00.

NSF Convergence Accelerator Track F: How Large-Scale Identification and Intervention Can Empower Professional Fact-Checkers to Improve Democracy and Public Health

Award Number:2137724; Organization: University of Wisconsin-Madison; Start Date: 10/01/2021; Award Amount: \$750,000.00.

NSF Convergence Accelerator Track F: Misinformation Judgments with Public Legitimacy

Award Number:2137469; Organization: Regents of the University of Michigan - Ann Arbor; Start Date:10/01/2021; Award Amount: \$750,000.00.

NSF Convergence Accelerator Track F: Online Deception Awareness and Resilience Training (DART)

Award Number:2230494; Organization: SUNY at Buffalo; Start Date:09/15/2022; Award Amount: \$2,500,000.00.

NSF Convergence Accelerator Track F: A Disinformation Range to Improve User Awareness and Resilience to Online Disinformation

Award Number:2137871; Organization: SUNY at Buffalo; Start Date:10/01/2021;
Award Amount: \$750,000.00.

NSF Convergence Accelerator Track F: Actionable Sensemaking Tools for Curating and Authenticating Information in the Presence of Misinformation during Crises

Award Number:2137806; Organization: Ohio State University; Start Date:10/01/2021;
Award Amount: \$749,999.00.

Through the programs mentioned above and other funding opportunities, as well as the specific funded projects, NSF seeks to invest in research, innovation, and workforce development that will benefit society by deepening our understanding of a changing technological information environment and provide the public with tools to safely navigate it.

NSF is working to identify and produce other documents responsive to your request. We appreciate your patience and will follow up with the Committee staff in the near future to coordinate further productions. Please feel free to contact [REDACTED], Head of the Office of Legislative and Public Affairs, at [REDACTED] if you have any additional questions.

Sincerely,



Sethuraman Panchanathan
Director

Cc: The Honorable Jerrold Nadler
Ranking Member
Committee on the Judiciary
U.S. House of Representatives

Appendix B

Message

From: Pozmantier, Michael [REDACTED]@nsf.gov
on behalf of Pozmantier, Michael <[REDACTED]@nsf.gov> [REDACTED]@nsf.gov
Sent: 11/22/2021 7:59:55 PM
To: Tripodi, Francesca Bolla [REDACTED]i@email.unc.edu]; [REDACTED] [REDACTED]@temple.edu]; Mike Wagner [REDACTED]@wisc.edu]; Michael Wagner [REDACTED]@wisc.edu]; [REDACTED] [REDACTED]@hackshackers.com]; Scott Hale [REDACTED]@meedan.com]; [REDACTED]@uw.edu]; [REDACTED] [REDACTED]@email.gwu.edu]; [REDACTED]@buffalo.edu]; [REDACTED]@uci.edu]; [REDACTED]@uw.edu]; [REDACTED]@cogsec.org; Paul Resnick [REDACTED]@umich.edu]; [REDACTED]i@cse.ohio-state.edu]
CC: Smith, Shelby L. [REDACTED]@nsf.gov]
Subject: NSF Convergence Accelerator: Track F Media Strategy
Attachments: Track F Media Strategy_v1.docx

All,

Thank you for participating in the meetings what were held on November 2, we learned quite a bit through the two discussions-- *I've also included those of you who couldn't make the meetings to get your input as well.* It's a taken a bit longer than I had hoped to get the notes and so forth together to begin to turn the discussion into actions. Please take a look at the attached document and send any comments back to me to coordinate any updates or additional guidance you may have. In addition, we need to start on the action items such as developing a basic media training kit, advanced training, and the response checklist. Given all of your experience and your equity in NSF doing a better job in how we deal with the media on this topic, this will be a joint effort. Some of you may already have these items developed or have done it before, so we're happy to defer to you in guiding the efforts here.

Please let me know which areas you'd like to contribute to. I'm hoping this will not result in much additional work for anyone and expect this to a be an iterative process that will see us ready to adopt the response checklist and provide the media kit and training beginning in January.

Feel free to pass this along to anyone on your teams that you feel should be included.

Happy Thanksgiving,

Mike

Media Strategy

Background

Due to the nature of the research/work being conducted by the Track F: Trust and Authenticity in Communication Systems funded projects, it is likely that NSF and the project teams will become a focal point for the various groups including media, non-profit, and other organizations. This is based on the response to reporting on a project focusing on helping local journalists understand how their work might be misused. An article written by an organization that is followed by various groups/publications with extensive reach was republished with the project being mischaracterized in the process, resulting in angry emails to NSF's media external mailbox. This process continued with a mention in another article further mischaracterizing the project in a more mainstream source.

Knowing that Track F is a controversial topic, it's important for NSF to proactively develop a strategy to enable the Foundation and funded researchers to be in sync. Additionally, many of the PIs, Co-PIs, and Sr. Personnel working on Track F projects have extensive experience dealing with this issue. Two meetings were organized by the Convergence Accelerator to draw upon this expertise, to develop the strategy to help prevent or lessen opportunities for the spreading of misinformation about the Track.

The result of these meetings was a set of recommended activities and artifacts to be developed by NSF, the Convergence Accelerator, and the teams to be used to assist in minimizing and responding to issues. The information would also be shared with NSF's Office of Legislative and Public Affairs and other relevant parties.

Recommendations

Messaging:

- Always highlight the pro-democracy nature of the Track and each project
- Always be accurate, any inaccuracies can be a hanging thread to be pulled
- If possible, focus on the non-ideological nature of work
 - Give examples of both sides *(I'm not a fan of always trying to show both sides because they are not always equal in impact and showing both sides can distort)
 - When it's possible, use sports metaphors
- Focus on the scientific process

Protective Measures:

- Subscribe to monitoring service(s) to proactively help manage when project information is published and possibly miscommunicated.
- Subscribe to scrubbing services, such as DeleteMe

Media Training:

Develop and provide media training to NSF Convergence Accelerator staff and funded researchers understand media engagement best practices, internal communication processes, and standard messaging. The multi-level training will include basic training and an advanced training.

- Multi-level
 - Basic training
 - Media engagement best practices
 - Interview requests (e.g., Who to involve, when to provide a written statement or have a live interview, etc.)
 - Speaking in plain language
 - Highlighting the scientific strategy, value and impact
 - Reporter terminology (e.g., What does it mean to be 'On the record', 'Off the record, or 'On background'?)
 - Standard key messaging about the NSF Convergence Accelerator, Track F, each funded project
 - Examples of media outlets to not engage
 - Processes: Notifying your organization of the media request, when to notify NSF
 - Advanced
 - Harassment:
 - How to respond to harassment (accompanied by Checklist)
 - Who to notify if harassment is received

Develop Response Checklist

Actions:

1. Create a talking points document
2. Put together list of scrubbing and monitoring services
 - a. Some may offer free service to researchers, if not this is an allowable project expense
3. Develop Media Basic Training Kit that can be provided without a training session
4. Design a Media Training Session to go over more advanced topics
5. Develop Response Checklist in conjunction with advanced training

Appendix C

Message

From: James Park [REDACTED]@umich.edu]
Sent: 10/26/2021 10:38:52 PM
To: [REDACTED]@strategixmanagement.com
CC: [REDACTED]@nsf.gov
Subject: Team 469 - first pitch slides
Attachments: Team469_First Pitch_10.27.2021.pptx

Hello, Convergence Accelerator team,

Please find attached the slides for Team 469's first pitch. We look forward to seeing you all tomorrow.

Thanks again,
James





--

James C. Park
Assistant Director, Center for Social Media Responsibility
School of Information | University of Michigan



Team F-469

Overview

Our misinformation service

helps **policy makers at platforms**     ...

get good PR for their actions on misinformation

by having a **clear benchmark for outcomes**  → 

and eliminating the need to defend internal procedures.

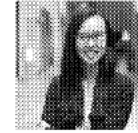
Misinformation Judgments with Public Legitimacy



Paul Resnick
Lead PI
University of Michigan



David Jurgens Co-PI
University of Michigan



Amy Zhang
Co-PI
University of Washington



Adam Berinsky
Senior Personnel
MIT



David Rand
Senior Personnel
MIT



James Park
Project Manager
University of Michigan



NSF's Convergent Accelerator

NSF's Convergent Accelerator Curriculum
Phase I

Substituted clear benchmark for: "externalizing responsibility for assessing the validity of particular actions" Our misinformation service helps policy makers at platforms who want to

Get people off our backs for how we act on misinfo

Do the things we know work without backlash

Push responsibility for difficult judgments to someone outside the company

Feel good about how they are acting on misinfo

legitimate way to act on misinformation ,

By

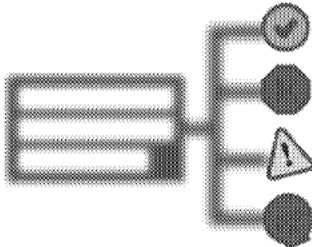
Externalizing the difficult responsibility of censorship

Measuring/defending outcomes instead of procedures

and Eliminating the need to defend specific procedures.


Why


Everyone agrees platforms should slow the spread of misinformation **but** they disagree on which content is misinformation.



Customer Problem Statement

Any action Platform Product Policy owners take will be criticized.
Thus, they are reluctant to innovate and to be transparent.





NSP's Convergence Accelerator

NSP's Convergence Accelerator Curriculum
Phase I

Because there there is no clear benchmark for determining whether a new procedure is more effective and fair...

We can unleash platforms to stop misinformation if society can agree on how to evaluate what is misinformation.

Previous possibilities for why:

There is widespread agreement

Misinformation undermines liberal democracy by eroding the commonly accepted facts that allow society to reach consensus.

The misinformation-informed partisan definitions of facts are increasingly divergent, making efforts to curtail misinformation by social media companies untenably controversial. Thus misinformation is accelerating the fracture of modern society.

Our work reestablishes bipartisan consensus on truth and therefore enables platforms to curtail the spread of misinformation, saving modern democracy.

How

Value Proposition

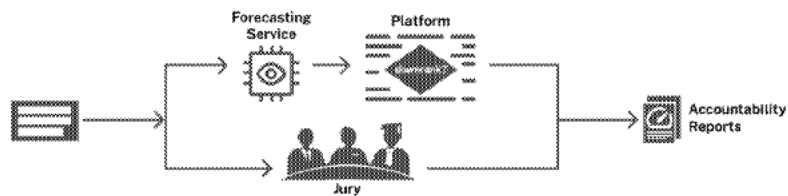
Our external service will provide **publicly legitimate judgments**. Platforms can focus on the engineering challenge of approximating the correct decisions quickly and at large scale.

Deliverables

A **golden set service** will convene juries.

Accountability reports will use the jury judgments.

A **forecasting service** will provide, for any content item, a forecast of jury outcomes.



A major initial project activity will be to determine the conditions of public legitimacy for such jury processes. Alternative design elements include: who would be the jurors; how would case materials be selected; how would juries deliberate? The second service

Appendix D

PROJECT SUMMARY

Overview:

The health of a democracy depends on the public's ability to access reliable information (Hobbs, 2010; Mihailidis & Thevenin, 2013). Learning how to find information and assess its quality is essential to making informed personal and civic decisions (Lynch, 2017; Metzger et al., 2010). On the Internet, traditional gatekeepers and hallmarks of authority are largely absent. Moreover, few understand how search engines work and the role that search terms play in shaping the information returned. If people consume information without the ability to assess its credibility—unable to tell who is behind a cause and what their motives might be—they are easy prey for groups that seek to deceive, mislead, and manipulate. In these ways and others, the toxic effects of disinformation have chipped away at the foundations of democracy the world over (Diamond, 2020; Levitsky & Ziblatt, 2018). Members of our team have developed and evaluated cost-effective interventions that teach K-12 and college students to find trustworthy online sources in a wide variety of domains. Based on research with professional fact checkers (Wineburg & McGrew, 2017, 2019), these interventions teach civic online reasoning—skills that allow Internet users to efficiently evaluate the information that flows across their screens. Rigorous studies conducted in secondary school and college settings show that these interventions improve students' ability to distinguish between quality digital information and sham (Breakstone et al., 2021a; 2021b; Brodsky et al., 2019; McGrew, 2020; McGrew et al., 2018).

In the Convergence Accelerator program, we will shift our attention from public education to education of the public. Through a three-year road map, and with partners in academia, industry, nonprofit, and government, we propose a multidisciplinary human-centered design process for adapting effective interventions to new contexts—based on our expertise in the sociology of information, effective web reading practices, curriculum development, and online delivery at scale. We will disseminate effective approaches through an open software platform that integrates educational interventions and assessment. We will test this approach with populations often excluded from information literacy efforts and who may be more vulnerable to misinformation campaigns, such as rural and indigenous communities with limited access to high-speed internet, military veterans, older adults, and military families.

The project's Phase I output will be to co-design, test, adapt, and scale misinformation interventions that have proven effective within educational settings to the broader public. In Phase I, we will work with Humanities Montana, a convener of libraries and cultural institutions and advocate for engaged citizenship, to adapt proven educational interventions to serve rural, low-income citizens, including indigenous populations, in libraries and other community settings. Such efforts will require expertise in the study of existing media practices of selected sub-groups, experience with developing and assessing civic online reasoning interventions, and a proven track record of designing and delivering educational experiences at scale.

Intellectual Merit:

We will develop a flexible, human-centered design process for adapting existing search literacy interventions to particular contexts. In Phase II, we will use this design process to create targeted interventions for a range of groups outside the formal educational system who are vulnerable to misinformation campaigns, including for military veterans, military families, older adults, immigrant populations, and low-income urban residents.

Broader Impacts:

The broader impacts of our research will be 1) to widely disseminate resources for effective search practices across diverse communities through public media and online learning resources, 2) to publish in journals, conferences, and other venues use-inspired research that provides a road map for understanding the deep stories and search practices of particular communities and using that understanding to adapt existing, effective interventions to new contexts, and 3) to develop an openly-licensed integrated software platform of simulations and assessments that allow for the evaluation of interventions across diverse contexts.

TABLE OF CONTENTS

For font size and page formatting specifications, see PAPPG section II.B.2.

	Total No. of Pages	Page No.* (Optional)*
Cover Sheet for Proposal to the National Science Foundation		
Project Summary (not to exceed 1 page)	1	_____
Table of Contents	1	_____
Project Description (Including Results from Prior NSF Support) (not to exceed 15 pages) (Exceed only if allowed by a specific program announcement/solicitation or if approved in advance by the appropriate NSF Assistant Director or designee)	15	_____
References Cited	5	_____
Biographical Sketches (Not to exceed 2 pages each)	8	_____
Budget (Plus up to 3 pages of budget justification)	18	_____
Current and Pending Support	51	_____
Facilities, Equipment and Other Resources	3	_____
Special Information/Supplementary Documents (Data Management Plan, Mentoring Plan and Other Supplementary Documents)	20	_____
Appendix (List below.) (Include only if allowed by a specific program announcement/ solicitation or if approved in advance by the appropriate NSF Assistant Director or designee)	_____	_____
Appendix Items:		

*Proposers may select any numbering mechanism for the proposal. The entire proposal however, must be paginated. Complete both columns only if the proposal is numbered consecutively.

NSF Convergence Accelerator Track F: Adapting and Scaling Existing Educational Programs to Combat Inauthenticity and Instill Trust in Information¹

Overview

The health of a democracy depends on the public’s ability to access reliable information (Hobbs, 2010; Mihailidis & Thevenin, 2013). Learning how to find information and assess its quality is essential to making informed personal and civic decisions (Lynch, 2017; Metzger et al., 2010). On the Internet, traditional gatekeepers and hallmarks of authority are largely absent. Moreover, few understand how search engines work and the role that search terms play in shaping the information returned. If people consume information without the ability to assess its credibility—unable to tell who is behind a cause and what their motives might be—they are easy prey for groups that seek to deceive, mislead, and manipulate. Just as important, citizens who feel unable to identify misinformation are less likely to engage in sharing *any* information, even when that information may be reliable and socially beneficial (Yang & Horning, 2020). In these ways and others, the toxic effects of disinformation have chipped away at the foundations of democracy the world over (Diamond, 2020; Levitsky & Ziblatt, 2018).

Members of our team have developed and evaluated cost-effective interventions that teach K-12 and college students to find trustworthy online sources in a wide variety of domains. Based on research with professional fact checkers (Wineburg & McGrew, 2017, 2019), these interventions teach a set of skills—*civic online reasoning*—that allow Internet users to efficiently evaluate the information that flows across their screens. Rigorous studies conducted in secondary school and college settings show that these interventions improve students’ ability to distinguish between quality digital information and sham (Breakstone et al., 2021a; 2021b; Brodsky et al., 2019; McGrew, 2020; McGrew et al., 2018).

In the Convergence Accelerator program, we will shift our attention **from public education to education of the public**. Through a three-year road map, we propose **a multidisciplinary human-centered design process for adapting effective interventions to new contexts--based on our expertise in the sociology of information, effective web reading practices, curriculum development, and online delivery at scale. We will disseminate effective approaches through an open software platform that integrates educational interventions and assessment**. We will test this approach with populations often excluded from information literacy efforts and who may be more vulnerable to misinformation campaigns, such as rural and indigenous communities with limited access to high-speed internet (Swire-Thompson & Lazer, 2020), military veterans (House Veterans' Affairs Committee, 2020), older adults (Guess et al., 2019), and military families (Newman, 2021).

The project’s Phase I output will be to **co-design, test, adapt, and scale misinformation interventions** that have proven effective within educational settings to the broader public. In Phase I, we will work with Humanities Montana, a convener of libraries and cultural institutions and advocate for engaged citizenship, to adapt proven educational interventions to serve rural, low-income citizens, including indigenous populations, in libraries and other community settings. If the goal is to educate *every* Internet user, we must develop processes that allow us to adapt and deliver the tools developed by our team to new contexts and populations. Such efforts will require expertise in the study of existing media practices of selected sub-groups, experience with developing and assessing civic online reasoning interventions, and a proven track record of designing and delivering educational experiences at scale.

Educational interventions need to account for the distinct media literacy practices of different communities, including where they go for information they can trust and how they come to trust those sources. We will ground our work in ethnographic methods to understand *existing media literacy practices*. By understanding the “deep stories” (Hochschild, 2016; Tripodi, 2018) that communities bring with them when they search (e.g., Lee et al., 2021), our work will provide more context to how these processes are exploited by media manipulators and foreign governments. This research will inform how we adapt our interventions to help citizens become discerning consumers of digital content.

¹The title has evolved slightly since the Co-PIs submitted the letter of intent with this title: *Lateral Reading for All--Adult Educational Programs for Effective Search Practices to Combat Inauthenticity in Communication*.

In Phase I, through a co-design process, we will develop a searchable library of tasks and curriculum materials with detailed guidance about implementation in diverse contexts. To achieve the goal of adapting, testing, and scaling community-centered misinformation interventions, we will bring together diverse stakeholders to prototype and test a range of interventions that will include workshops and classes, online learning modules, public service announcements (PSAs), posters, and other resources and activities. In developing materials, we will build on extensive experience creating free online curricula, professional development workshops, open online courses, and public media (in partnership with Retro Report, a premier documentary news organization that produces videos for the New York Times and other news organizations). We will evaluate materials using digital clinical simulations (Thompson et al., 2019) and other tested assessment tools (Breakstone et al., 2021a; 2021b; McGrew et al., 2018). We will then disseminate materials through partnerships with organizations like Humanities Montana, as well as develop an online repository of our resources of adapted intervention materials for use in communal settings (e.g., libraries, senior centers, and places of worship). This initial set of materials will be made available through Stanford’s existing Civic Online Reasoning website, a site that has logged 180,000 curriculum downloads in the last 18 months. Above all, we will develop a flexible, human-centered design process for adapting existing interventions to new contexts.

In Phase II, we will extend this human-centered design process **to create and scale targeted interventions for a range of additional groups who are especially vulnerable to misinformation campaigns**, including military veterans, military families, and older adults. We will follow the process developed in Phase I: (1) generate ethnographic understanding of existing information-seeking practices; (2) prototype interventions based on patterns identified during ethnographic research; (3) engage in an iterative prototyping and testing with key community stakeholders; and (4) archive effective approaches, resources, and assessment prompts. To support our work across multiple contexts, **we will develop an integrated learning and assessment platform** that includes digital clinical simulations of challenging tasks in civic online reasoning, diverse assessment items that evaluate intervention effectiveness with distinct populations, and curricular materials for community settings like senior centers.

The multidisciplinary, multi-sector team brings expertise in combating misinformation from a range of disciplines and methodological training including: sociology, education, the learning sciences, information science, civics, adult online and blended learning, personalized learning at scale, and psychometrics. The team includes members from nonprofit, industry, and academia, with proposed partnerships in health care and the military to be developed during Phase I in preparation for Phase II.

A. Objectives and Significance of the Proposed Activity

The overarching goal of this work is to equip the general public with the knowledge and skills needed to find trustworthy information online. Understanding communities’ unique media literacy practices-- where they go for information, how they come to trust that information, and how their orientation to search inputs influences outputs (Tripodi, 2018)-- is crucial to the success of training and intervention delivery. Unlike decontextualized interventions and games, the key to our success is authentic task environments of the live web (Caulfield, 2017; McGrew, 2020; Wineburg & McGrew, 2017). Our three year roadmap **expands our efforts beyond traditional classrooms to generate a software platform for research and interventions that can analyze, identify, and respond to the unique socio-technical features** of the communities we wish to serve. We will adapt and test existing interventions for use with groups at increased risk for falling prey to inauthentic behavior. Through this iterative process, we will create a repository of curriculum and assessment materials that will be made freely available online. Our core objectives for the proposed activities include:

1. **Build a Multi-Sector Partnership:** Establish a collaborative community with partners from academia, non-profits, the military, and industry to build human-centered, use-inspired interventions that foster trust in communication among the public.

2. **Seek Information on Information Seekers:** Assess how groups decide what information they trust, where they go for news and information, and how they understand the algorithms that drive search engines like Google.
3. **Co-Design Prototype Interventions:** Building on existing interventions developed by our team, create co-design tools, media and curricula that meet the needs of the target communities.
4. **Iteratively Evaluate Intervention Effectiveness:** Evaluate implementation and engagement in target communities, and how much new interventions improve civic online reasoning
5. **Disseminate Insights and Tools to the Field:** Distribute resources including a public-facing report, an online repository of free curricular materials, an interactive e-learning tool, a collection of professionally produced videos, assessment items, and digital clinical simulations.

Through a set of tasks described in *D. Coordination Plan* below, including participation in the NSF Innovation Curriculum, the proposed work will address these **guiding questions**:

1. Where do people go for information they can trust and how do they come to rely on this information? To what extent are these practices shaped by community norms and values? How do these practices vary across communities? How well do users understand the technology they use to validate information (e.g., Google or Wikipedia)?
2. Can community-centered education and training materials that result from the convergence approach create more digitally discerning citizens?
3. To what extent should intervention approaches differ across communities and contexts? What parts of effective interventions are most likely to require contextual adaptations, and what aspects typically work across contexts?

From Public Education to *Educating the Public*: Evaluating What Works and For Whom

The baseline of search skills in the U.S. population is dangerously low. People struggle to evaluate online information. Participants who said they would base evaluations on source information rarely did so when observed in real time (Eysenbach & Köhler, 2002; Flanagin & Metzger, 2007; Hargittai et al., 2010). Individuals frequently ignored source information (Bartlett & Miller, 2011; Barzilai & Zohar, 2012), focusing instead on the relevance (rather than quality or accuracy) of the information provided (Walraven et al., 2009) and basing their conclusions on a website’s surface-level features (Coiro et al., 2015; Hargittai & Young, 2012; McGrew et al., 2018). These findings may reflect deficiencies in how people are taught to judge the credibility of Internet sources. Many of the most widely used website evaluation materials—including those appearing on prestigious university websites—feature outdated strategies that can lead students astray (Breakstone et al., 2018; Caulfield, 2017; Sullivan, 2019; Wineburg et al., 2020; Wineburg & Ziv, 2020). In the largest study of its kind (Breakstone et al., 2021a), 3,446 high school students were provided a live Internet connection and tested on a series of tasks. On one, students were shown an anonymously produced video that circulated on Facebook claiming to show ballot stuffing during Democratic primary elections and asked to use Internet-enabled computers to determine whether the video provided strong evidence of voter fraud. Despite access to the Internet’s powerful search capabilities, just three of the study’s more than three thousand participants were able to divine the true source of the video, which actually featured footage of voter fraud in Russia.

The encouraging news is that there are cost-effective solutions for improving digital discernment at scale. Studies conducted in the last few years suggest that it is possible to improve individuals’ digital savvy through focused educational interventions based on research with professional fact checkers (Breakstone et al., 2021a; 2021b; Brodsky et al., 2019, 2021; Kohnen et al., 2020; McGrew, 2020; McGrew et al., 2019). Wineburg and McGrew found substantial differences in how expert fact checkers approached digital content compared with intelligent but less competent searchers (Wineburg & McGrew, 2016a, 2016b, 2017, 2019). While less competent web readers tended to focus on reading the information in front of them, fact checkers did the opposite, opening up new tabs across the horizontal axis of their browsers and searching for information about the organization or individual behind it—a skill we call *lateral reading*. Only after surveying other sites did fact checkers return to the original site. Using this

approach, fact checkers quickly sized up sites that masked their intent and backers. Students and academics, on the other hand, dwelled on the original site, often resulting in confusion about its real agenda or sponsor. Lateral reading allowed fact checkers to quickly answer a crucial question: *Who's behind the information, and what are the strengths and weaknesses of this source?*

Recent lateral reading educational interventions have been conducted in K-12 settings (Kohnen et al., 2020; McGrew, 2020) and college classrooms (Breakstone et al., 2021b; McGrew et al., 2019; Brodsky et al., 2019, 2021) to test whether students can learn and apply these strategies. In work based both on the Stanford History Education Group's (SHEG) Civic Online Reasoning (COR) curriculum and co-PI Caulfield's SIFT model (Stop, Investigate the source, Find better coverage, Trace claims; Caulfield, 2019), instructors provided students with explicit instruction on how to evaluate a range of digital content, and students practiced these skills through engagement with real online sources. Pretest and posttest measures asked students to evaluate the credibility of unfamiliar sources in authentic online environments with live Internet connections. Empirical data shows that students successfully apply lateral reading and identify reputable sources and claims, sometimes with only a few hours of training. In Exhibit 1, we show sample assignment prompts (Caulfield, n.d.) such as twitter posts (Panel A), scam emails (Panel B), sponsored source web pages (Panel C), and altered photographs (Panel D) that the team has used in prior interventions. On the right is a mobile friendly simulation assessment that asks participants to assess the reliability of a website (Panel C). Participants are shown the images and a set of related claims, and they are asked to determine the level of authenticity, trust, and evidence to support those claims. A large-scale practice and assessment bank would allow the team to adapt training materials so they resonate with the user. We will bring this human-centered, use-inspired approach to Phase 1 and Phase 2 deliverables.

Exhibit 1. Sample Assessment Prompts and Evaluation Interface in Online Learning Environment

Sample Assignment Prompts

A. Sample tweet from satire account GOPTeens

C. Web page on CO2 from fossil fuel sponsored organization

B. Sample scam email with tips from "John Hopkins University" on combating cancer

D. An altered image of Einstein fleeing atomic bomb

Digital Clinical Simulation

Here are four student responses you received from your students. These screenshots are representative of how the entire class performed.

Response 1 (Jamie): I think it is reliable because it provides a lot of useful information about the effects of rising CO2. It even has a .org domain, which means it is run by an organization. Plus, the article cites sources to back the claims.

Response 2 (Fatima): Yes, it is reliable because I went to the website's "About" page and I read that they are a charity "dedicated to discovering and disseminating scientific information pertaining to the effects of atmospheric CO2 enrichment on climate and the biosphere."

Response 3 (Pinki): This is not a reliable source for learning about carbon dioxide's environmental effects because the website does not look professionally made and it even asks you to donate money.

Response 4 (Mel): No, according to Wikipedia, they receive funding from Exxon Mobil, a fossil company, which would make them biased toward saying CO2 is good for the environment when it's not.

Which response was the strongest?

Response 1 (Jamie)

Response 2 (Fatima)

Response 3 (Pinki)

Response 4 (Mel)

Explain why you chose this response.

E. Mobile-friendly simulation assessment interface

The SIFT model has been used in the teaching of a wide range of scientific disciplines, and SHEG's work has shown great promise in domain transferability: students who showed digital

discernment in one topical domain (such as nutrition) were able to transfer their strategies to evaluating sources in another domain (Breakstone et al., 2021b). Adoption of these methods has been accelerating in higher education and K-12. Caulfield’s SIFT method is widely disseminated in university library-based information literacy training (Warzel, 2021) and recently, a pilot with CIVIX Canada, involved 3,000 K-12 students in 96 classrooms (CIVIX, n.d.). SHEG’s COR materials, which span multiple topics and disciplines, have been downloaded more than 180,000 times, featured in *TIME Magazine* (Steinmetz, 2018), and integrated into legislation on digital literacy (California SB-135, 2018). Below, we detail our human-centered design process for building the underlying beliefs and cultural norms of non-student populations into a training and delivery system for civic online reasoning.

The Need for a Human-Centered Solution to a Technology Problem: The Role of Context in Misinformation Intervention Efficacy

Investigating how different populations understand information ecosystems, engage in search practices, and respond to misinformation interventions are all critical precursors to adapting proven educational interventions at scale. Research is needed on how different groups assess information and how media literacies vary across groups. Use-inspired research into how people understand algorithms, personalization, and how our information environment is constructed is a necessary precursor to developing effective interventions that serve the needs of diverse populations.

In her ethnographic study of two conservative groups, Tripodi (2018) found that information-seekers engage in a distinct set of media practices tied to the way they see the world. One practice centered around the close reading of textual documents deemed sacred (e.g. the Bible or the Constitution). By inverting traditional assumptions that truth is only curated at the top, this media practice allows for everyday people to act as subject matter experts. These practices, which developed and emerged in a print era, have been adapted to online search practices. Because interviewees distrusted both journalists and academics, they drew on this practice to fact check how media outlets reported the news.

In fact, many respondents may have believed they were engaging in “lateral reading” (e.g. “doing the research” using Google). However, their approach differed in crucial respects. Unlike professional fact checkers, who practice “click restraint” (Wineburg & McGrew, 2017), users focused on the top results of Google, seldom scrolling down or looking at subsequent paged results (Tripodi, 2018). While lateral readers try to find secondary sources that reliably summarize expert consensus on sources and claims (Wineburg & McGrew, 2017; Caulfield, 2017), respondents often focused on reading a wide array of *primary* sources, and performing their own synthesis (Tripodi, 2018). While lateral readers seek to eliminate bias that might skew results from search terms (Caulfield, 2017), respondents made no such effort. Finally, unlike expert lateral readers, respondents evaluated search terms based on the nature of the results returned. One participant saw the fact that most results presented a similar story as evidence of a “rigged” media, rather than a heuristic of expert or professional consensus — and re-ran the search with new terms (Tripodi, 2018).

Findings from this one subpopulation underscore the variations that we expect to find among different groups. On the one hand, respondents lacked key understandings and techniques to search effectively and adhered to deeper narratives that might make them suspicious of any intervention that privileges mainstream sources or recognized experts. On the other hand, the community possessed one of the hardest things to foster in students — the habit, a deep part of their practice, of opening up more than one tab. In a related vein, many conservatives today are concerned about algorithmic bias (Vaidhyanathan, 2019; Tripodi 2019a; Tripodi 2019b) in ways most students are not. Yet, in the context of deeper communal narratives of media conspiracy, this algorithmic awareness may not yield greater search competency and may erode institutional trust.

Communities Disproportionately Targeted. Over the full scope of a three-year project, we propose to use human-centered design processes to adapt search literacy interventions to new contexts and populations. We are particularly interested in developing resources for underserved populations who have complex relationships with institutions designed to instill community trust (e.g., government, health care,

social services). Disinformation works in conjunction with sociopolitical factors to increase the spread of problematic content (Freelon & Wells, 2020). For example, ahead of the 2020 election, a cybersecurity firm found that suspicious accounts targeted indigenous groups by exploiting tensions between indigenous nations and the U.S. government (Groupsense, 2020). Fragile relationships between government health agencies and indigenous groups in Brazil pose similar difficulties when it comes to establishing trust in the COVID-19 vaccine (BBC News, 2021). Strategically targeting groups with curated content that resonates with their audiences makes a misinformation campaign effective (Yin et al., 2018). However, most rigorous interventions regarding media literacy do not take into account the cultural contexts by which various groups decide what information to trust. We propose **in-depth investigation and information literacy interventions** in the following contexts:

- 1) Libraries in rural areas of the United States, especially those serving adults who live in low-income or isolated settings with limited access to high-speed internet
- 2) Military families, veterans, and related groups
- 3) Older adults, especially those facing challenges from cognitive impairment

Preliminary conversations with stakeholders from these groups indicate the diversity of these groups' information needs and of the misinformation threats they face. For instance, active duty military service members, their families, and veterans are all linked by common experiences and service, but their information needs and practices differ by context and by generation. Interventions to serve them will need to differ as well. In developing early partnerships with military groups, we heard different needs from different subpopulations in these groups. We will work with educators in the Department of Defense Education Activity (DoDEA) group, the organization that runs DoD schools on military bases, to adapt our interventions to both directly serve children in military families and then have students share their new learning with their families. When we discussed these ideas with DoDEA stakeholders, they immediately brought up concerns about military personnel involvement in the January 6 assault on the Capitol and the subsequent anti-extremism training that is a military priority (PBS NewsHour, 2021).

By contrast, in developing our partnerships with colleagues who work with older adults in the Veterans Affairs (VA) system, their concerns were more related to financial scams, medical misinformation, and threats that are particular to veterans facing cognitive impairment. Research reveals that patterns of neurocognitive and psychiatric comorbidities of posttraumatic stress disorder make older veterans particularly vulnerable (Kang, Xu, & McConnell, 2018). A core research question of our proposal involves understanding how to efficiently adapt interventions to diverse populations. Effective interventions are contingent on understanding how various groups establish trust. What features of the instructional design, pedagogical approach, examples, delivery mechanism, or assessments of an intervention need to be adapted for rural libraries, veterans, and children and families of active duty soldiers? If we can identify features that work across contexts and those that need to be context-specific, we can more efficiently adapt proven interventions to new populations.

The Opportunity: Building Publicly Accessible, Adaptable, Scalable Interventions to Prepare Digitally Discerning Citizens

Phase I Overview. In Phase I, we will begin our initial work through a partnership with Humanities Montana and their network of rural libraries and cultural institutions. We will target the search literacy learning needs of rural adults and tribal groups, with a focus on patrons who use the library as their primary means of Internet access. We will identify 3-5 institutions to work with closely, and then begin a human-centered design process with the following stages:

- 1) **Ethnographic field work in Montana with library patrons and tribal groups in rural areas:**
We will conduct field interviews, observations, and think aloud protocols with 15-25 library patrons across multiple institutions, settings and cultural contexts to better understand their existing media literacy practices. This preliminary work will identify how patrons decide what information to trust and test their current understanding of search engines, their results, and the Internet context.

- 2) **Co-design of prototype interventions:** Working with Humanities Montana, our team will connect with front-desk librarians, library system leaders, and influencers in tribal groups to conduct a set of human-centered design sessions. These sessions will focus on developing prototype interventions in multiple media—workshops, online learning modules, posters, PSAs, search aides—that help rural and Montanans improve their civic online reasoning.
- 3) **Assess effectiveness:** Using our extensive assessment experience, we will use a combination of digital clinical simulations (described below) and assessment items to evaluate which interventions appear most promising for improving patron searches.
- 4) **Bring promising interventions to scale:** Drawing on the experience of the MIT Teaching Systems Lab and our partners at Retro Report, we will build an online repository of openly licensed versions of our most promising interventions and disseminate with partners.
- 5) **Evaluate the nature and type of adaptations:** We will compare our final set of adapted interventions in the Montana context with the core, proven interventions that we have used widely in K-20 settings to identify the kinds of adaptations necessary. By understanding how we adapt core materials to the cultural needs to rural library patrons and tribal groups we can develop hypotheses for how our team can adapt effective interventions in new contexts (e.g., veterans, military families, older adults) in Phase II and what parts work across contexts.

During Phase I, we will include our partners from DoDEA and affiliates with the VA system so that we begin to engage them in this co-design work. We anticipate substantial logistical challenges in arranging access to work with military populations and patients in Veterans Administration medical care, such as understanding the restricted Internet access in active duty contexts and developing adequate arrangements with human subjects boards (IRB) to study veteran populations. We propose working on these challenges in Phase I, so we are ready in Phase II to begin work in these additional contexts.

Technology Innovations for Simulation and Assessment. A key component in our efforts to prototype, improve and assess our interventions are *digital clinical simulations*. PI Reich and co-PI Wineburg, in a previous collaboration, developed a free open online course called *Sorting Truth from Fiction: Civic Online Reasoning*, which has served thousands of registrants on edX. The course includes digital simulations that allow participants to practice civic online reasoning skills in a partly-controlled environment. We develop these scenarios in our openly licensed digital simulation platform called *Teacher Moments* (Thompson et al., 2019). These simulations typically consist of five components:

- 1) A prompt for civic online reasoning task
- 2) Full access to the internet and/or a set of sample search results from lateral reading
- 3) Assessment items that allow participants to explain their process, findings, and reasoning
- 4) AI coaching agents that provide feedback and scaffolding
- 5) Debriefing videos that show expert search practitioners completing analogous tasks

Typical prompts ask participants to identify the source behind a website or evaluate a claim from a website or social media post. Since research shows that effective fact checkers employ lateral reading and solve information challenges by using the web to evaluate sources, our simulations always allow participants to either fully engage in searching the web, or use a set of simulated search results. We have some criticisms of proposed web literacy tasks or simulations that ask participants to evaluate web sources without access to the open web; expert fact checkers don't rely on their own intuitions as much as they seek out collective judgments found in broader information ecosystems.

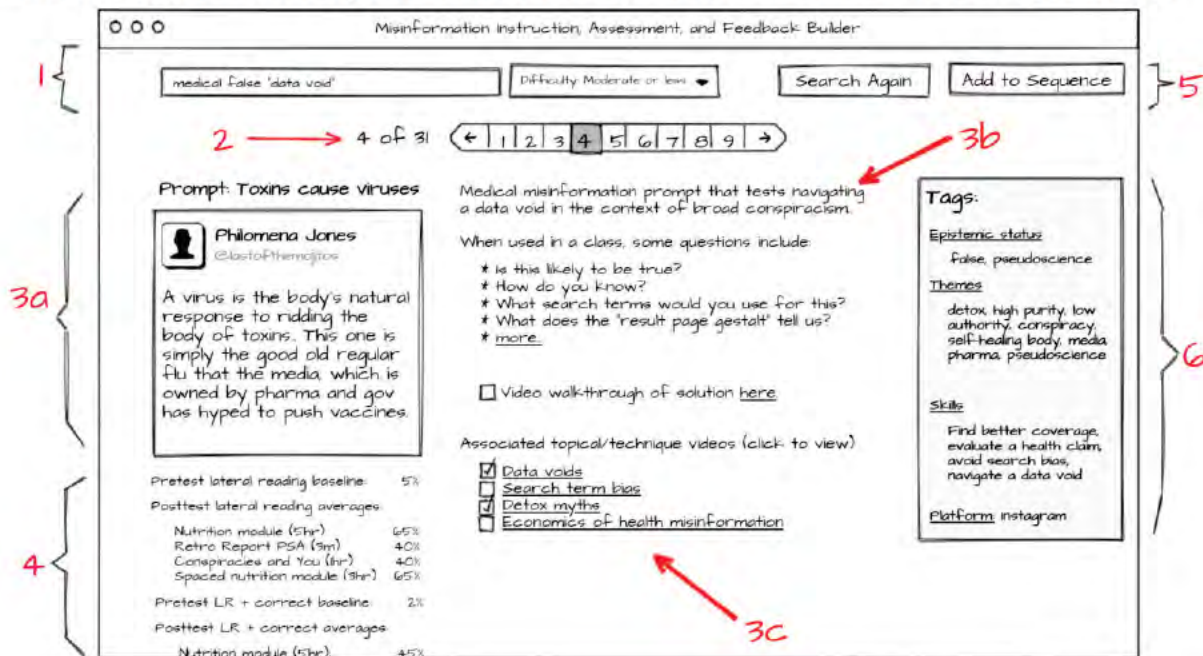
Once participants have used their newly-developed skills to evaluate a source or claim, we use assessment items to ask them to describe their process, findings, decisions, and reasoning. For participants who struggle with a task or approach a task incorrectly, we provide additional, personalized support at this stage through intelligent coaching agents. For instance, in *Sorting Truth from Fiction*, we ask participants to evaluate a tweet from an account called “Republican Teens”. The account is a parody/satire account. Once participants discover this, there is no need to further evaluate the veracity of the particular claim in the tweet. Through natural language processing, we were able to determine with at least 90% accuracy when participants failed to identify the account as satire, and provide targeted

feedback. These digital clinical simulations can be used for skill development, for formative assessment, and within pre-post evaluation frameworks. We plan to use them for all three purposes.

Phase II Objectives. Over the course of Phase II, we will replicate this design cycle and develop analogous deliverables to serve library patrons across the country and underserved populations, including older adults, veterans, and military families. In Phase II, the American Library Association would be brought in as a national partner to help us scale up and implement effective interventions to libraries throughout the U.S. We will serve veterans directly through partnerships with the VA. We will serve military families by adapting our school-based interventions for students in DoDEA schools, and then develop additional supports that help teachers and students share their newly learned search practices with their active-duty family members. We will also seek to develop additional partnerships that would allow us to reach other groups.

A crucial part of developing and testing interventions in multiple contexts is a consistent framework for assessment. A key project in Phase II will be developing a bank of assessment items and digital clinical simulations that can be used across settings and compared in a psychometrically rigorous manner. We will substantially expand our assessment and digital clinical simulation work to allow for the development of hundreds of test items and simulations, and we will use item response theory to develop measures of item difficulty and discrimination that will allow educators and researchers to use different combinations of items for different contexts and assessment purposes while also allowing for consistent estimates of learning and skill development. AI coaching agents will help identify challenges of appropriate difficulty and provide targeted feedback on their performance. AI can then use difficulty tags and data to create learning sequences automatically. In Exhibit 2, we show a wireframe of an integrated platform for assessment and simulation.

Exhibit 2. Wireframe of Integrated Platform for Assessment and Simulation Phase 2 Deliverable



At the end of Phase II, we envision an assessment bank and course builder in which the user can build a customized assessment, online course, or workshop, by searching specific combinations of topics and skills (1 in Exhibit 2 wireframe). The tool generates search results (2) that include a link to a visual preview of the assessment prompt (3a) along with a description of the issues it raises (3b) and a list of related instructional videos that can be added to the sequence (3c). The interface displays data collected about baselines and post-intervention performance (4). Users can add the prompt to the course or slide

deck they are building, along with related instructional media (5), or browse related items by tags (6). AI-driven instruction and analytics insight reports automate tagging and performance data.

By the end of three years, we will have a set of adapted, scaled interventions that work in three important contexts (libraries, VA medical settings, and DoDEA schools on military bases), an online repository of openly-licensed materials and assessments that can be widely used across settings, and a set of design principles explaining how effective civic online reasoning interventions can be adapted to new contexts. We will continue to refine and iteratively improve this preliminary Phase II plan as we gain new insights from Phase I prototyping work and from our work with other convergence accelerator teams.

B. Convergence Research

Issues of trust and authenticity in communications systems are complex social problems that require a convergence approach to make significant progress— “a high level of interdisciplinarity and engagement with multiple diverse stakeholders, including researchers and the ultimate users of research products” (NSF, 2021). The Co-PIs bring deep combined expertise developing, evaluating, automating, and scaling interventions to combat misinformation with K-20 populations. Through close partnership with multi-sector leaders and their constituents in rural communities, military schools and hospitals for older adults and veterans through Phase I and Phase II, we will co-design interventions that will be relevant to these communities in terms of content (*will the examples we choose resonate with them?*), format (*how comfortable will they be with technology?*), and messaging (*do the intervention materials feature individuals who reflect the culture, language, history, and assumptions of the target community?*). An integrated partnership between developer and end-user will catalyze discovery around intervention effectiveness and adaptation, and result in a concrete set of widely available tools, training materials, and an assessment library. We will make our data public so that any sector leader or training facilitator in the country can access community-specific training materials. The **intellectual merit** of this work is in creating a true “research platform” as defined by the NSF solicitation: an “integrated collection of tools, techniques, and educational materials and programs” (NSF, 2021) that are chosen specifically for their ability to accelerate research and impact in this area.

The team brings techniques from multiple disciplines and deep experience engaging multi-sector partners: Co-PI Tripodi, trained in **sociological** methods, has led large-scale **ethnographic** studies that position the team to conduct high-quality end-user and human-centered research with the proposed target populations. She brings deep expertise making her work accessible to the general public, including repeatedly testifying to the Senate on censorship through search engines and its impact on public discourse (Tripodi, 2019a, 2019b). Co-PI Wineburg and Breakstone are trained in **the learning sciences, civics education, and assessment**. Together, they bring three decades of experience in **designing curricula** and rigorously evaluating their effectiveness. They have led some of the most widely cited studies to date about students’ digital literacy and low-cost interventions to help students evaluate online sources (Breakstone et al., 2021a; Breakstone et al., 2021b, McGrew et al., 2018; McGrew et al., 2019; Wineburg & McGrew, 2019; Wineburg et al., 2016). They have also developed digital literacy videos that have been viewed over two million times on YouTube (Crash Course, 2019). With more than two decades of experience in **online and blended learning** and **community outreach**, co-PI Caulfield has spearheaded some of the most widely-adopted techniques in K-16 misinformation interventions and has significant experience tailoring educational materials to community needs. PI Reich is trained in **adult online learning** and **learning at scale**, and has expertise developing online learning tools and leveraging the rich data produced by these environments for rigorous evaluation, including integrating AI features.

C. Roles & Responsibilities and Partnerships

The multidisciplinary team brings expertise in learning science, online learning, civic education, sociology, and political media scholarship. We complement this expertise with partners from nonprofit, military, and industry sectors. Our team includes the following core members and their responsibilities:

Justin Reich (PI) is Associate Professor of Comparative Media Studies/Writing and the director of the MIT Teaching Systems Lab (TSL), where he leads a multidisciplinary team of learning scientists,

technologists, game developers, and evaluation experts. Reich has led the design of seven award-winning open online courses for educators on edX and other platforms, including *Sorting Truth from Fiction: Civic Online Reasoning* (edX, n.d.), developed collaboratively with SHEG. Together, these courses have served nearly 100,000 registrants from around the world. Dr. Reich has managed over \$12.5 million in research grants and projects, and his scholarly work on open online learning has been published in *Science*, *Proceedings of the National Academy of Sciences*, and other high-impact venues. Dr. Reich will provide overall management of the project and lead the development of online intervention materials.

Rachel Slama (Project Manager) is the Associate Director of the MIT Teaching Systems Lab. She brings fifteen years of experience managing complex federally-funded projects in partnership with schools, districts, and other education partners. Hallmarks of her professional trajectory include: (1) analyzing student outcome data for field impact across K-12 (Slama et al., 2017; Slama et al., 2015; Slama, 2014; Slama, 2012) and postsecondary digital and large-scale learning environments (Littenberg-Tobias et al., 2020; Ruipérez-Valiente et al., 2019; Thompson et al., 2019), (2) leading large convenings for a range of stakeholders virtually and in-person, and (3) disseminating technical work in accessible formats including at national state education agency convenings (Slama et al., 2018) and Senate briefings (Slama, 2016). Dr. Slama will serve as primary project manager, and coordinate all aspects of the project.

Sam Wineburg (co-PI) is the Margaret Jacks Professor of Education and, by courtesy, of History & American Studies at Stanford University and Fellow of the National Academy of Education. Wineburg founded the Stanford History Education Group whose curriculum and assessments have been downloaded over ten million times, making it one of the largest providers of free social studies curriculum in the world. His work since 2015 has focused on how people judge the credibility of digital content, research that has been reported in the *Wall Street Journal*, the *New York Times*, the *Washington Post*, NPR, *TIME Magazine*, BBC, MSNBC, and *Die Zeit*, and translated into dozens of languages. He will supervise Stanford's contributions, advise on research design and assessments, and collaborate on public outreach.

Joel Breakstone (co-project manager) is the director of SHEG, and leads their efforts to research, develop, and disseminate free curriculum and assessments. The SHEG website attracts more than 1.3 million visitors annually and their mailing list includes more than 130,000 educators. For the last six years, Breakstone oversaw the creation of the Civic Online Reasoning website, which won a Global Media and Information Literacy Award from UNESCO in 2020. His research has appeared in the *British Journal of Educational Psychology*, *Cognition and Instruction*, and *Harvard Kennedy School Misinformation Review*. He will work with Dr. Slama to co-manage the project and co-lead the development of curricular materials, assessments, and interventions.

Mike Caulfield (co-PI) is the director of blended and networked learning at Washington State University, Vancouver. He was a founding member of the American Association of State Colleges and Universities (AASCU) eCitizenship Project in 2010, and a board member from 2010-2013. Since 2016, he has produced a variety of curricula and educational materials on source and claim contextualization using his SIFT methodology: an award-winning open textbook, *Web Literacy for Student Fact-Checkers* (2017), digital materials and assessments for AASCU's nine university, 1,000+ student pilot on teaching web literacy (2017-2018), the open-source online curriculum "Check, Please!" (2019), the Infodemic website (2020), and materials, assessments, and teacher-training workshops for CIVIX Canada's 3,200 student, 96 classroom pilot for elementary and secondary school institutions (2020-2021). On this project he will lead co-design efforts to develop and implement curricular materials, assessments, and workshops.

Francesca Tripodi (co-PI) is an assistant professor in the School of Information and Library Science (SILS) and a Senior Researcher at the Center for Information Technology & Public Life (CITAP) at UNC-Chapel Hill. Dr. Tripodi's research examines how our interactions with search influence our political reality. In 2019, she testified before the U.S. Senate Judiciary Committee and explained how search processes are gamed to maximize exposure and drive ideologically-based queries. Her forthcoming book with Yale University Press titled *Searching for alternative facts: How conservative politicians and pundits wield the power of search* explores how media practices are

exploited for politics. Dr. Tripodi will lead our ethnographic studies to ensure that interventions are grounded in deep understanding of people and contexts.

Multi-sector Partners Working in Diverse Contexts. We have cultivated partners in media development, librarianship, veterans' care, and the military (please see Letters of Collaboration).

Randi Lynn Tanglen is the Executive Director of **Humanities Montana**, which serves communities through speaking to Montanans' diverse history, literature, and philosophy. The Informed Citizen project seeks to deepen the public's knowledge and appreciation of the vital connections between democracy, the humanities, journalism, and an informed citizenry. The Democracy Project engages teens in civic action through partnerships with local libraries and community organizers. Humanities Montana has a strong network of connections with libraries and tribal groups throughout the state. They will support our efforts to conduct ethnographic research with patrons that use libraries as primary sites of internet access, and help implement interventions to support civic online reasoning among library patrons.

Kyra Darnton, is the Executive Producer of **Retro Report**, a journalism nonprofit that produces high-quality short-form documentaries featuring meaningful context about today's headlines. It has produced more than 250 short documentaries that have reached tens of millions of viewers through partnerships with *The New York Times*, *The New Yorker*, PBS Frontline, NBC, *Politico*, *The Atlantic*, Univision, *Time Magazine* and others. Retro Report has recently expanded its reach with prime-time television series on PBS and Vice TV. With a strong track record of developing engaging public media, Retro Report will help shape the public media aspects of our interventions.

Samantha Oakley is a program manager with the **American Library Association's (ALA)** Public Programs Office who will act as an advisor during Phase I to provide feedback during prototyping and help position our efforts for potential scaling. Oakley led ALA's Media Literacy Education in Libraries for Adult Audiences that this initiative builds on. If funded for Phase II, ALA would be brought in as a national partner to help us scale up and implement effective interventions to wider audiences. ALA is the foremost national organization providing resources to inspire library and information professionals to transform their communities through essential programs and services.

Dr. Andrea Schwartz, MD, MPH is a professor at the Harvard Medical School and Medical Director of the Geriatrics Consult Clinic at VA Boston. In Phase I, she will help address logistical challenges to working with VA populations and develop human-centered design cycles for Phase II.

Dr. Jennifer Fritschi is the DoDEA director of education technology and **Radley Ramirez** is the Teacher of the Year in the DoDEA and an education technology director for Europe, who will partner with us during Phase I to address logistical challenges to working in DoDEA schools and on military bases and develop human-centered design cycles for Phase II research.

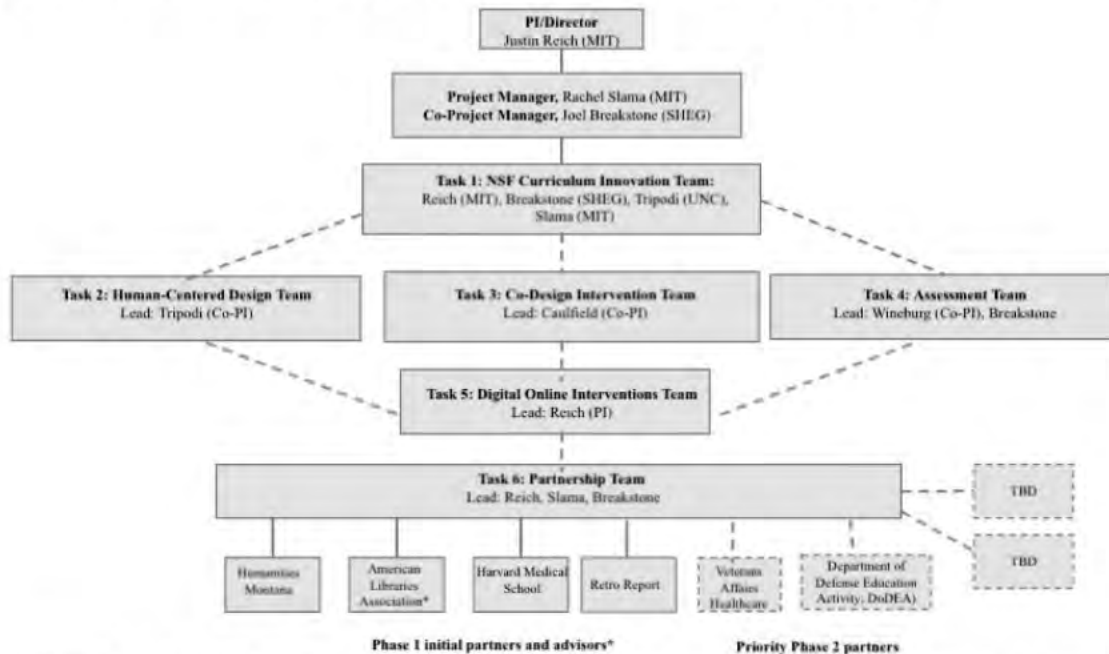
Results from Prior NSF Support

PI Justin Reich's most relevant completed NSF funded project is EAGER: Framing MOOC Learning for Student Success (NSF Division of Undergraduate Education: 1646976; \$300,000; 2016-2018) with Dustin Tingley (Harvard University). Intellectual merits include the testing of a set of behavioral interventions over 2.5 years, with one-quarter million students, from nearly every country, across 247 online courses offered by Harvard, MIT, and Stanford (Kizilcec et al., 2020). Study findings include a process for iterative scientific investigation that can uncover what works for whom in different context. Broader Impacts: The results inform policymakers and school administrators about the relative effectiveness and cost-effectiveness of these interventions, the limits of personalizing interventions with artificial intelligence, and the challenge of scaling interventions across diverse contexts.

Dr. Reich also leads an ongoing Cyberlearning project (with Co-PI, Carolyn Rosé; award #1917668) to incorporate digital clinical simulations in computer science teacher education. The broader impacts include that over 300 digital clinical simulations that have been authored in Teacher Moments serving over 8,000 teachers in training. The intellectual merit includes implementing intelligent coaching agents that scan users' inputs and provide targeted scaffolds and supports. Publications from the project include a timely piece on the role of simulations in teacher education during the pandemic (Sullivan et al., 2020) and a best paper winning article that examines simulation co-design (Dutt et al., 2021).

D. Coordination Plan

Exhibit 3. Organizational Chart with Team Coordination and Management Structure



In Exhibit 3, we describe the coordination and management structure for our project, where the PI and project managers will coordinate task teams. Broadly speaking, MIT will take overall responsibility for management of the project and the coordination of activities and stakeholders. Dr. Rachel Slama, the associate director of the MIT TSL, will be the primary project manager, supported by Dr. Joel Breakstone from SHEG, building off our multi-year collaboration developing the online edX course *Sorting Truth from Fiction: Civic Online Reasoning*. Our human-centered design cycles will generally involve a combination of ethnographic research, collaborative design, intervention and assessment prototyping, and online development. Dr. Tripodi will lead ethnographic work, Caulfield will lead co-design exercises, Drs. Wineburg and Breakstone will lead curriculum, assessment, and intervention development, and Dr. Reich will lead the development of online resources and the online repository. Our project partners and advisors from Humanities Montana, Retro Report, the ALA, Harvard Medical School, and the DoDEA will support development in their respective areas of expertise.

In Exhibit 4, we delineate project roles and activities, and responsibilities. We organize our Phase I work around six project tasks:

- 1) **Task 1: Participate in the NSF convergence curriculum**
- 2) **Task 2: Generate an ethnographic understanding of existing information seeking practices**
- 3) **Task 3: Prototype an intervention design based on patterns identified during qualitative research and co-design sessions**
- 4) **Task 4: Conduct pilot study based on iterative rapid testing and design process with key stakeholders in the community**
- 5) **Task 5: Develop and disseminate openly-licensed online intervention materials**
- 6) **Task 6: Form multidisciplinary, multi-sector partnership**

Our project team will have a weekly stand-up to coordinate activities and identify blockages or obstacles to individual or collaborative goals. We will develop sub teams around ethnographic work, co-design, prototyping, and online development that each meet during the relevant phase of work. We will conduct quarterly project reviews to ensure progress toward our final deliverables, to identify opportunities for stronger collaboration, and to consolidate learning from sub-team work.

Exhibit 4. Proposed Project Activities, Roles, and Responsibilities

Task/Subtask and Deliverables	S	O	N	D	J	J	M	A	M	J	J	A
Task 1: Participate in NSF innovation curriculum (Reich, Breakstone, Tripodi)												
Activities will be based on the sample NSF curriculum including key milestones: Kick-off Workshop (October), Mid-point Research Share Workshop (December), Winter Kick-off Refocus Workshop (January), Pitches (March), Proposal Writing (April), Phase II Applications (May) and Phase II Pitches (June).	X	X	X	X	X	X	X	X	X	X	X	X
Task 2: Generate ethnographic understanding of existing information seeking practices (Lead: Tripodi) +Partners												
Develop user interview protocols based on prior research and partner input, recruit participants and conduct interviews and focus groups	X	X										
Summarize findings and implications in memo for co-design, assessment, and intervention teams			X	X	X							
Task 3: Prototype an intervention design based on patterns identified during qualitative research and co-design sessions (Lead: Caulfield, Wineburg, Breakstone) + Partners												
Curate existing curriculum and assessment materials to build co-design workshops.	X	X										
Conduct curriculum co-design sessions with target populations and refine interventions and prototypes based on co-design findings.						X	X					
Task 4: Conduct pilot study based on iterative rapid testing and design process with key stakeholders in the community (Lead: Breakstone, Wineburg)												
Gather existing instruments that have been used in prior studies and make adaptations based on preliminary findings from Tasks 2 and 3.						X	X	X				
Recruit participants to test pilot intervention and training materials among library patrons in rural settings. Pre-test six weeks before intervention								X	X			
Task 5: Develop openly-licensed online intervention materials that be widely used and adapted to new contexts (Lead: Reich) + Partners												
Curate existing materials developed in Tasks 2-4 to determine appropriate format (e.g. online, face-to-face, video)								X	X	X		
Task 6: Form multidisciplinary, multi-sector partnership (Lead: Reich, Breakstone, Slama) + partners												
Host partner kickoff meeting and develop partner data management plan (privacy, sharing, IRB, protocols; revisit in Phase II if applicable)	X	X										
Convene partners in monthly virtual meetings as a group and individual check-ins/ office hours	X	X	X	X	X	X	X	X	X	X	X	X
Host informational session to recruit Phase 2 partners									X			

E. Deliverables

We propose a set of six deliverables in Phase I, which will contribute to **broader impacts** across society. On the basis of ethnographic field work in rural library settings, (1) we will publish an initial study of the search literacy practices of information seekers who live in rural settings and/or tribal lands, who use libraries as their primary Internet connection. Following our multi-stakeholder co-design sessions with researchers, librarians, patrons and other stakeholders, (2) we will develop a set of intervention and training materials that can be used, formally and informally, in library settings. (3) We will adapt prototype interventions and training materials for online contexts, and develop additional online videos in partnership with Retro Report. To test the effectiveness of our interventions, (4) we will develop an online repository of assessment materials integrated with effectiveness data. On the basis of this Phase I prototyping work, we will publish (5) a design approach to adapting effective interventions to new contents and populations. Throughout the project, we will develop (6) collaboration materials that outline our interdisciplinary effort and provide guidance for other teams pursuing similar aims.

As a team, we have a strong track record of consistently stewarding philanthropic and government funding towards the successful completion of scholarly and educational projects. Given our extensive history of collaboration and the additional support of the convergence accelerator program, we are confident that we have the team, partners, resources, and supports needed to have a high probability of achieving these project goals in Phase I and crafting a successful Phase II proposal, that is refined and informed by additional Track F partners and our Phase I findings.

In Phase II, our goal is to expand our deliverables to two additional contexts by the end of the two-year period—serving older adults in geriatric care through Veterans Administration hospitals and serving military families through the DoDEA educational system. By testing our adaptation process in libraries, elder care, and on military bases and schools (Phase II, Year 1), we will be able to develop a robust set of principles for adapting civic online reasoning materials to a wide variety of other civic, educational, and religious groups (Phase II, Year 2). Our goal is to make sure that civic online reasoning materials are widely and publicly available to help all Americans improve their search literacy skills.

Metrics of Success. Our project will track three kinds of metrics during Phase I: 1) Implementation progress metrics, 2) Effectiveness metrics, and 3) Dissemination metrics.

For implementation metrics, we will use the timeline on Exhibit 4 to track progress towards tasks and goals. To assure smooth functioning of our partnership, the MIT TSL team will send a quarterly survey to all project members and partners to evaluate our collaborative practices, meeting schedules and structures, progress towards deliverables, and communication practices. During each quarterly review meeting, we will collaboratively review these data and identify shortcomings in our collaboration and improve our interdisciplinary collaborative practices. As we set the final number of partner libraries and institutions for prototyping and implementing new interventions, we'll track measures of usage and implementation fidelity, such as downloads, time on site, and similar usage and engagement metrics.

For metrics of the effectiveness of our work, we will draw on SHEG's existing Civic Online Reasoning assessment items and digital clinical simulations that evaluate whether people can successfully perform important search literacy tasks, such as evaluating the credibility of a source or determining if a source supports a certain argument. These assessment items have been essential in developing both national portraits of student search skills (Breakstone et al., 2021), and evaluating the effectiveness of civic online reasoning interventions (McGrew et al., 2019). We can use existing materials to conduct preliminary evaluations of our prototype interventions, and as ethnographic research develops a deeper understanding of context-specific civic online reasoning practices, we will develop new assessment items to evaluate the effectiveness of new kinds of interventions.

For dissemination metrics, as we develop a repository of freely available online resources we will make them available on the SHEG website (with 1.2 million visitors per year) and on MIT online properties such as edX and the Open Learning Library. We will track the total downloads as well as unique institutions using our resources. Dissemination metrics will play a major role during Phase II scale-up efforts and we will set initial interim benchmark dissemination goals in Phase I.

F. Track Alignment

From the solicitation: “The overarching goal of Track F is to develop prototype(s) of novel research platforms forming integrated collection(s) of tools, techniques, and **educational materials and programs to support increased citizen trust in public information of all sorts** (health, climate, news, etc.), through more effectively preventing, mitigating, and adapting to critical threats in our communications systems” (emphasis added). Our team unites leading experts on the development of educational materials to improve civic online reasoning and increase citizen trust in information ecosystems. We supplement this core educational expertise with a leading ethnographer of search practices and experts in online learning at scale. Our combined expertise in pedagogy, digital systems, digital learning, and information systems can serve as a resource to other Track F teams as well. Our project will primarily focus on education, but our team regularly consults with other groups developing techniques and technologies for improving the information ecosystems, and we look forward to bringing our anthropological and education expertise to these teams. Similarly, we look forward to learning how new technologies and other interdisciplinary approaches can improve educational efforts.

G. Broader Impacts and Broadening Participation Plan

Broader Impacts. Herb Lin, the Hank J. Holland Fellow in Cyber Policy and Security at Stanford’s Hoover Institution gave the following testimony to the House Subcommittee on Cyber, Innovative Technology, and Information Systems on 4/30/21: *“The information warfare threat to the United States is different from past threats, and it has the potential to destroy reason and reality as a basis for societal discourse, replacing them with rage and fantasy. Perpetual civil war, political extremism, waged in the information sphere and egged on by our adversaries is every bit as much of an existential threat to American civilization and democracy as any military threat imaginable.”*

Efficient, effective search practices are now well established through rigorous research, but most adults either learned little about effective search practices or learned ineffective techniques. It is an urgent matter for civil society, for democracy, and for national security for adults to learn these crucial skills for participation in 21st century life. The **broader impacts** of our research will be 1) to widely disseminate resources for teaching and learning effective search practices across diverse communities through public media and online learning resources, 2) to publish in journals, conferences, and other venues use-inspired research that provides a road map for understanding the deep stories and search practices of particular communities and using that understanding to adapt existing, effective interventions to new contexts, and 3) to develop an openly-licensed integrated software platform of simulations and assessments that allow for the evaluation of interventions across diverse contexts. Through a multisector, multidisciplinary approach, we will adapt our public education interventions towards educating broad swaths of the American public about the crucial skills of civic online reasoning.

Broadening Participation Plan. A human-centered, co-design approach allows key stakeholders in diverse settings—library patrons in rural settings and tribal lands, DODEA teachers and students, patients in the VA medical care system—to participate in the design and development of learning resources to support fellow community members. The interventions that we co-design will then support the participation of underserved communities in civic life by more effectively navigating our information ecosystem. As we measure adoption of our interventions in libraries and cultural institutions in Phase I, we will track key demographic features of the patrons and communities of those institutions to ensure that our efforts are broadening participation across Montana and beyond. A key goal of this research is that more citizens, especially those from marginalized communities, will be more prepared to engage in civic activities and STEM careers with more robust information literacy practices. Because we seek to serve diverse communities, it is essential for our team to bring diverse students to work on our projects. For instance, at MIT we participate annually in the MIT Summer Research Program that supports trailblazing, first-generation college students in conducting research in MIT labs in preparation for applying to graduate schools. We also actively recruit student researchers through affinity groups like the Black Student Union at MIT. By broadening participation in our research activities, we hope to support diverse leadership in the future of information studies and civic online reasoning.

References Cited

- Bartlett, J., & Miller, C. (2012). Truth, Lies and the Internet. *Synergy*, 10(1). Retrieved from <https://slav.vic.edu.au/index.php/Synergy/article/view/v10i20126>
- Barzilai, S., & Zohar, A. (2012b). Epistemic thinking in action: evaluating and integrating online sources. *Cognition and Instruction*, 30(1), 39–85. <https://doi.org/10.1080/07370008.2011.636495>
- BBC News (2021). The misinformation bubble threatening Brazil's indigenous people. (2021a, May 8). *BBC News*. <https://www.bbc.com/news/blogs-trending-56919424>
- Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021a) Students' civic online reasoning: A national portrait. *Educational Researcher*, 0013189X211017495.
- Breakstone, J., Smith, M., Connors, P., Ortega, T., Kerr, D., & Wineburg, S. (2021b). Lateral reading: College students learn to critically evaluate internet sources in an online course. *Harvard Kennedy School Misinformation Review*, 2(1), 1–17. <https://doi.org/10.37016/mr-2020-56>.
- Breakstone, J., McGrew, S., Smith, M., Ortega, T., & Wineburg, S. (2018). Why we need a new approach to teaching digital literacy. *Phi Delta Kappan*, 99(6), 27–32.
- Brodsky, J., Brooks, P. J., Scimeca, D., Todorova, R., Galati, P., Batson, M., Grosso, R., Matthews, M., Miller, V., & Tachiera, T. (2019). Teaching college students the four moves of expert fact-checkers [Paper presentation]. Technology. *Mind, & Society, an American Psychological Association Conference, Washington, DC, United States*.
- Brodsky, J. E., Brooks, P. J., Scimeca, D., Todorova, R., Galati, P., Batson, M., Grosso, R., Matthews, M., Miller, V., & Caulfield, M. (2021). Improving college students' fact-checking strategies through lateral reading instruction in a general education civics course. *Cognitive Research: Principles and Implications*, 6(1), 23. <https://doi.org/10.1186/s41235-021-00291-4>
- California SB-135, Pupil instruction: media literacy: model curriculum, California Senate Bill (2017-2018). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB135
- Caulfield, M. (2017). Info-environmentalism: An introduction. *Educause Review*, 52(6), 92–93.
- Caulfield, M. (2019, June 19). SIFT (The Four Moves). *Hapgood*. <https://hapgood.us/2019/06/19/sift-the-four-moves/>
- Caulfield, M. (n.d.) Unpublished information literacy workshop materials. *Blended and Networked Learning, Washington State University, Vancouver*.
- CIVIX News Literacy. (n.d). Retrieved June 2, 2021, from <https://newsliteracy.ca/ctrl-f/>
- Coiro, J., Coscarelli, C., Maykel, C., & Forzani, E. (2015a). Investigating criteria that seventh graders use to evaluate the quality of online information. *Journal of Adolescent & Adult Literacy*, 59(3), 287–297.
- Crash Course (2019). *Navigating Digital Info*. <https://thecrashcourse.com/courses/navigatingdigitalinfo>
- Diamond, L. (2020). *Ill winds: Saving democracy from Russian rage, Chinese ambition, and American complacency*. Penguin Books.
- Dutt, R., Hillaire, G., Fang, A., Larke, L., Rosé, C., & Reich, J. (2021a). Investigating Adoption and Collaboration with Digital Clinical Simulations by Teacher Educators. *Society for Information Technology & Teacher Education International Conference*, 1209–1217.
- edX. (n.d.). *Sorting Truth From Fiction: Civic Online Reasoning*. EdX. <https://www.edx.org/course/sorting-truth-from-fiction-civic-online-reasoning>

- Eysenbach, G., & Köhler, C. (2002). How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews. *BMJ*, *324*(7337), 573–577.
- Flanagin, A. J., & Metzger, M. J. (2007). The role of site features, user attributes, and information verification behaviors on the perceived credibility of web-based information. *New Media & Society*, *9*(2), 319–342. <https://doi.org/10.1177/1461444807075015>
- Freelon, D., & Wells, C. (2020). Disinformation as political communication. *Political Communication*, *37*(2), 145–156. <https://doi.org/10.1080/10584609.2020.1723755>
- Groupsense. (2020). *Foreign actors seeking to sow divisions by targeting Native American populations, cyber intelligence firms says*. <https://www.groupsense.io/resources/foreign-actors-seeking-to-sow-divisions-by-targeting-native-american-populations-cyber-intelligence-firms-says>
- Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, *5*(1), eaau4586. <https://doi.org/10.1126/sciadv.aau4586>
- Hargittai, E., Fullerton, L., Menchen-Trevino, E., & Thomas, K. Y. (2010). Trust online: Young adults' evaluation of web content. *International Journal of Communication*, *4*, 27.
- Hargittai, E., & Young, H. (2012). Searching for a “Plan B”: Young adults' strategies for finding information about emergency contraception online. *Policy & Internet*, *4*(2), 1–23.
- Hobbs, R. (2010a). *Digital and Media Literacy: A Plan of Action. A White Paper on the Digital and Media Literacy Recommendations of the Knight Commission on the Information Needs of Communities in a Democracy*. Aspen Institute. <https://eric.ed.gov/?id=ED523244>
- Hochschild, A. R. (2016). *Strangers in their own land: anger and mourning on the American right*. The New Press.
- House Veterans' Affairs Committee (2020, December 9) H. Rept. 116-657- Hijacking Our Heroes: Exploiting Veterans Through Disinformation On Social Media. (n.d.-a). [Legislation]. Retrieved June 2, 2021 from <https://www.congress.gov/congressional-report/116th-congress/house-report/657>
- Kang, B., Xu, H., & McConnell, E. S. (2019). Neurocognitive and psychiatric comorbidities of posttraumatic stress disorder among older veterans: A systematic review. *International Journal of Geriatric Psychiatry*, *34*(4), 522–538. <https://doi.org/10.1002/gps.5055>
- Kizilcec, R. F., Reich, J., Yeomans, M., Dann, C., Brunskill, E., Lopez, G., Turkay, S., Williams, J. J., & Tingley, D. (2020). Scaling up behavioral science interventions in online education. *Proceedings of the National Academy of Sciences*, *117*(26), 14900–14905. <https://doi.org/10.1073/pnas.1921417117>
- Kohnen, A. M., Mertens, G. E., & Boehm, S. M. (2020). Can middle schoolers learn to read the web like experts? Possibilities and limits of a strategy-based intervention. *Journal of Media Literacy Education*, *12*(2), 64–79.
- Lee, C., Yang, T., Inchoco, G. D., Jones, G. M., & Satyanarayan, A. (2021). *Viral Visualizations: How Coronavirus Skeptics Use Orthodox Data Practices to Promote Unorthodox Science Online*. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–18. <https://doi.org/10.1145/3411764.3445211>
- Levitsky, S., & Ziblatt, D. (2018). *How Democracies Die*. Crown.
- Littenberg-Tobias, J., Slama, R., & Reich, J. (2020). *Large-Scale Learning for Local Change: The Challenge of MOOCs as Educator Professional Learning*.

- Lynch, M. P. (2016). *The internet of us: Knowing more and understanding less in the age of big data*. W. W. Norton & Company.
- McGrew, S. (2020). Learning to evaluate: An intervention in civic online reasoning. *Computers & Education*, 145, 103711.
- McGrew, S., Breakstone, J., Ortega, T., Smith, M., & Wineburg, S. (2018). Can students evaluate online sources? Learning from assessments of civic online reasoning. *Theory & Research in Social Education*, 46(2), 165–193.
- McGrew, S., Smith, M., Breakstone, J., Ortega, T., & Wineburg, S. (2019). Improving university students' web savvy: An intervention study. *British Journal of Educational Psychology*, 89(3), 485–500.
- Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and heuristic approaches to credibility evaluation online. *Journal of Communication*, 60(3), 413–439.
<https://doi.org/10.1111/j.1460-2466.2010.01488.x>
- Mihailidis, P., & Thevenin, B. (2013). Media Literacy as a Core Competency for Engaged Citizenship in Participatory Democracy. *American Behavioral Scientist*, 57(11), 1611–1622.
<https://doi.org/10.1177/0002764213489015>
- National Science Foundation [NSF], 2021. NSF Convergence Accelerator Phases I and II for the 2021 Cohort. Program solicitation NSF 21-572. Retrieved from
<https://www.nsf.gov/pubs/2021/nsf21572/nsf21572.pdf>
- Newman, L. H. (2021). *Facebook ad services let anyone target us military personnel*. Wired. Retrieved June 9, 2021, from <https://www.wired.com/story/facebook-ad-targeting-us-military>
- PBS NewsHour. (2021, April 11). *Exploring Hate: An inside look at anti-extremism training in the military*. PBS NewsHour. <https://www.pbs.org/newshour/show/exploring-hate-an-inside-look-at-anti-extremism-training-in-the-military>
- Ruipérez-Valiente, J. A., Halawa, S., Slama, R., & Reich, J. (2020). Using multi-platform learning analytics to compare regional and global MOOC learning in the Arab world. *Computers & Education*, 103776. <https://www.sciencedirect.com/science/article/pii/S0360131519303288>
- Slama, R. B. (2012). A longitudinal analysis of academic English proficiency outcomes for adolescent English language learners in the United States. *Journal of Educational Psychology*, 104(2), 265.
- Slama, R. B. (2014). Investigating whether and when English learners are reclassified into mainstream classrooms in the United States: A discrete-time survival analysis. *American Educational Research Journal*, 51(2), 220–252.
- Slama, R.B. (2016, April). *Monitoring the performance of English learners*. Presented at the United States Senate Briefing: *What Does the Every Student Succeeds Act Mean for English Learners and Accountability?* Washington, D.C. Retrieved from
<https://www.air.org/sites/default/files/Speaker%20bios%20-%20What%20Does%20ESSA%20Mean%20for%20English%20Learners%20and%20Accountability.pdf>
- Slama, R., Goldschmidt, P., & Lee, M. (2018, February). *English Language Proficiency Accountability Tool*. Interactive session presented at the 2018 Council of Chief State School Officers (CCSSO) State Collaborative on Assessment and Student Standards (SCASS) Winter Meeting, Miami, Florida.
- Slama, R., Haynes, E., Sacks, L., Lee, D. H., & August, D. (2015). Massachusetts English Language Learners' Profiles and Progress: A Report for the Massachusetts Department of Elementary and Secondary Education. *American Institutes for Research*.

- Slama, R., Molefe, A., Gerdeman, D., Herrera, A., Brodziak de los Reyes, I., August, D., & Cavazos, L. (2017). Time to Proficiency for Hispanic English Learner Students in Texas. REL 2018-280. *Regional Educational Laboratory Southwest*.
- Sullivan, M. C. (2019). Why librarians can't fight fake news. *Journal of Librarianship and Information Science*, 51(4), 1146–1156.
- Sullivan, F., Hillaire, G., Larke, L., & Reich, J. (2020a). Using teacher moments during the COVID-19 pivot. *Journal of Technology and Teacher Education*, 28(2), 303–313.
- Swire-Thompson, B., & Lazer, D. (2020). Public health and online misinformation: challenges and recommendations. *Annual Review of Public Health*, 41(1), 433–451.
<https://doi.org/10.1146/annurev-publhealth-040119-094127>
- Thompson, M., Owho-Ovuakporie, K., Robinson, K., Kim, Y. J., Slama, R., & Reich, J. (2019). Teacher moments: A digital simulation for preservice teachers to approximate parent–teacher conversations. *Journal of Digital Learning in Teacher Education*, 35(3), 144–164.
- Tripodi, F. (2018). *Searching for alternative facts*. Data and Society Research Institute.
https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Searching-for-Alternative-Facts.pdf
- Tripodi, F. (2019a). *Google and Censorship through Search Engines*, United States Senate Committee on the Judiciary. <https://www.judiciary.senate.gov/meetings/google-and-censorship-through-search-engines>
- Tripodi, F. (2019c). *Stifling Free Speech: Technological Censorship and the Public Discourse*, United States Senate Committee on the Judiciary.
<https://www.judiciary.senate.gov/meetings/stifling-free-speech-technological-censorship-and-the-public-discourse>
- Vaidhyanathan, S. (2019, July 28). *Why Conservatives Allege Big Tech Is Muzzling Them*. The Atlantic. <https://www.theatlantic.com/ideas/archive/2019/07/conservatives-pretend-big-tech-biased-against-them/594916/>
- Walraven, A., Brand-Gruwel, S., & Boshuizen, H. P. (2009a). How students evaluate information and sources when searching the World Wide Web for information. *Computers & Education*, 52(1), 234–246.
- Warzel, C. (2021). Don't go down the rabbit hole. *The New York Times*.
- Wineburg, S., Breakstone, J., Ziv, N., & Smith, M. (2020). Educating for misunderstanding: How approaches to teaching digital literacy make students susceptible to scammers, rogues, bad actors, and hate mongers. *Stanford History Education Group Working Paper No. A-21322*. Retrieved March, 2, 2021.
- Wineburg, Sam, & McGrew, S. (2016a). Why students can't google their way to the truth. *Education Week*, 36(11), 22–28.
- Wineburg, Sam, & McGrew, S. (2016b). *Evaluating information: The cornerstone of civic online reasoning* (United States of America) [Working paper]. Stanford History Education Group, Robert R. McCormick Foundation. <https://apo.org.au/node/70888>
- Wineburg, S., & McGrew, S. (2017). Lateral reading: reading less and learning more when evaluating digital information (SSRN Scholarly Paper ID 3048994). *Social Science Research Network*. <https://papers.ssrn.com/abstract=3048994>
- Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. *Teachers College Record*, 121(11), 1–40.
- Wineburg, Sam, & Ziv, N. (2020). Why can't generation that grew up online spot the misinformation in front of them. *Los Angeles Times*.

- Yang, F., & Horning, M. (2020). Reluctant to share: how third person perceptions of fake news discourage news readers from sharing “real news” on social media. *Social Media + Society*, 6(3), 2056305120955173. <https://doi.org/10.1177/2056305120955173>
- Yin, L., Roscher, F., Bonneau, R., Nagler, J., & Tucker, J. A. (2018). Your friendly neighborhood troll: The Internet Research Agency’s use of local and fake news in the 2016 US presidential campaign. *SMaPP Data Report, Social Media and Political Participation Lab, New York University*.

III. Threats to free speech abroad and the risk at home

The threat to Americans' free speech does not end at America's shores. The global nature of social media has made it possible for foreign censors to target American speech from afar, and the Select Subcommittee has shown that that is happening.⁴⁹ In Brazil, Justice Alexandre de Moraes—who serves on Brazil's Supreme Court and as president of Brazil's Superior Electoral Court, which oversees the country's electoral processes—has become a one-man censorship machine, investigating American citizens because of their online speech and forcing American companies, such as X and Rumble, to cease operations in Brazil after they refused to comply with his illegal censorship orders.⁵⁰ In addition to standing for free speech in Brazil, the Select Subcommittee has also probed a European bureaucrat who threatened American companies with regulatory retaliation under European law simply for facilitating political discourse in the United States.⁵¹ Finally, in response to Australia's efforts to censor online speech globally, the Select Subcommittee called on the Biden-Harris Administration to protect Americans' First Amendment rights and stand for free speech worldwide.⁵²

When X's CEO, Elon Musk, stood for free speech in Brazil and against Moraes' censorship orders in April 2024, the Brazilian government reportedly launched an investigation into Musk for alleged obstruction of justice and other charges.⁵³ This attack of American free speech caused the Select Subcommittee to examine the threats posed by anti-free speech governments abroad. On April 17, 2024, based upon documents received pursuant to a subpoena to X, the Select Subcommittee released a report titled, "[The Attack on Free Speech Abroad and the Biden Administration's Silence: The Case of Brazil](#)," and subsequently released a second report on May 7, 2024, titled, "[The Attack on Free Speech Abroad and the Biden Administration's Silence: The Case of Brazil Part II](#)."⁵⁴ The subpoenaed documents in the reports revealed that, since at least 2022, the Brazilian government, led by Moraes, ordered X, Rumble, and other social media platforms to censor over 300 accounts—including former Brazilian

⁴⁹ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., [THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL](#) (Comm. Print Apr. 17, 2024); STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., [THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL, PART II](#) (Comm. Print May 7, 2024).

⁵⁰ *Id.*

⁵¹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Thierry Breton, Comm'r for Internal Markets, European Comm'n (Aug. 15, 2024); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Thierry Breton, Comm'r for Internal Markets, European Comm'n (Sept. 10, 2024).

⁵² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Uzra Zeya, Under Sec'y for Civilian Security, Democracy, & Human Rights, and Hon. Eileen Donahoe, Special Envoy & Coordinator for Digital Freedom, Dep't of State (Nov. 21, 2024).

⁵³ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., [THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL](#) (Comm. Print Apr. 17, 2024).

⁵⁴ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., [THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL](#) (Comm. Print Apr. 17, 2024); STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., [THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S SILENCE: THE CASE OF BRAZIL, PART II](#) (Comm. Print May 7, 2024).

President Jair Bolsonaro, critics of the Brazilian government, conservative members of the federal legislature, journalists, members of the judiciary, and even a gospel singer and a pop radio station—or else face fines of up to 100,000 reais (about \$20,000 U.S. dollars) per day for noncompliance.⁵⁵

The same day that the Select Subcommittee issued its first report, the Select Subcommittee wrote to the State Department to (1) share its’ findings, (2) ask the Department to produce all documents and communications between the Department and the government of Brazil regarding Moraes’ censorship orders to X, and (3) request a briefing “about how the State Department intend[ed] to respond to these attacks on free speech in Brazil.”⁵⁶ On May 28, 2024, the State Department briefed the Select Subcommittee, noting that it did not intend to publicly comment on, or respond to, Moraes’ actions.⁵⁷

The Select Subcommittee has also stood against censorship threats from the EU.⁵⁸ In August 2024, when Thierry Breton, a European bureaucrat, threatened X, an American company, and Elon Musk, an American citizen, for facilitating political discourse in the United States (i.e., livestreaming an interview with President Trump), the Select Subcommittee demanded that Breton stop “any attempt to intimidate individuals or entities engaged in political speech in the United States” or “otherwise interfere in the American democratic process.”⁵⁹ The Select Subcommittee also arranged a briefing with the State Department to learn about how it planned to respond to Breton’s threats.⁶⁰ During the briefing, the Department confirmed that it did not intend to publicly condemn Breton’s threats.⁶¹ Ultimately, after Breton sent a letter to the Select Subcommittee downplaying his threatening statements and the censorship provisions of the EU law he attempted to wield against X and Musk,⁶² the Select Subcommittee sent him another

⁵⁵ *Id.*

⁵⁶ Letter from Rep. Jim Jordan, Chairman H. Comm. on the Judiciary, to Hon. Uzra Zeya, Under Sec’y for Civilian Security, Democracy, & Human Rights, and Hon. Eileen Donahoe, Special Envoy & Coordinator for Digital Freedom, Dep’t of State (Apr. 17, 2024).

⁵⁷ State Department briefing to Committee staff (May 28, 2024).

⁵⁸ *See, e.g.*, House Judiciary GOP (@JudiciaryGOP), X (Nov. 1, 2024, 10:06 AM), <https://x.com/JudiciaryGOP/status/1852351403030687924>.

⁵⁹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Thierry Breton, Comm’r for Internal Markets, European Comm’n (Aug. 15, 2024); House Judiciary GOP (@JudiciaryGOP), X (Aug. 16, 2024, 5:50 PM), <https://x.com/JudiciaryGOP/status/1824564435853197820>.

⁶⁰ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Uzra Zeya, Under Sec’y for Civilian Security, Democracy, & Human Rights, and Hon. Eileen Donahoe, Special Envoy & Coordinator for Digital Freedom, Dep’t of State (Aug. 15, 2024).

⁶¹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Uzra Zeya, Under Sec’y for Civilian Security, Democracy, & Human Rights, and Hon. Eileen Donahoe, Special Envoy & Coordinator for Digital Freedom, Dep’t of State (Aug. 15, 2024). State Department briefing to Committee staff (Sept. 5, 2024, 4:30 PM).

⁶² Letter from Thierry Breton, Comm’r for Internal Markets, European Comm’n, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 21, 2024).

letter, pointing out the inaccuracies in his reply.⁶³ Six days later, Breton resigned.⁶⁴ Yet, the EU threat to American free speech remains.⁶⁵

Most recently, the Select Subcommittee opposed Australia's efforts to censor Americans' speech and again called on the Biden-Harris Administration to protect Americans' First Amendment rights and stand for free speech worldwide.⁶⁶ On November 21, 2024, the Select Subcommittee wrote to the State Department to request a briefing regarding proposed legislation in Australia that "would effectively require American social media platforms to censor alleged 'misinformation'" and "could pressure American companies to censor online speech outside of Australia, including in the United States."⁶⁷ The Select Subcommittee detailed how "[d]uring the COVID-19 pandemic, the Australian government repeatedly attempted to censor speech *outside* of Australia, including the speech of American citizens and health professionals located in the United States."⁶⁸ The Select Subcommittee emphasized concerns with Australia eSafety Commissioner Julie Inman Grant's April 2024 order to X to remove dozens of posts on the platform "globally," even after the company "had already blocked the posts from [X's] Australian users" and despite the fact that the posts did not violate X's content moderation policies.⁶⁹

On November 22, 2024, just a day after the Select Subcommittee's letter, *The Australian* reported that Australia's third largest political party, the Greens, would oppose the Australian government's censorship legislation.⁷⁰ On November 24, 2024, "after it failed to garner support from a single non-Labor senator,"⁷¹ the Australian government officially withdrew its censorship legislation without a Senate vote, recognizing that there was "no pathway to legislate this proposal through the Senate."⁷²

⁶³ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary to Thierry Breton, Comm'r for Internal Markets, European Comm'n (Sept. 10, 2024).

⁶⁴ Lorne Cook, *A French member of the European Commission resigns and criticizes President von der Leyen*, AP (Sept. 16, 2024).

⁶⁵ See, e.g., House Judiciary GOP (@JudiciaryGOP), X (Nov. 1, 2024, 10:06 AM), <https://x.com/JudiciaryGOP/status/1852351403030687924>.

⁶⁶ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Uzra Zeya, Under Sec'y for Civilian Security, Democracy, & Human Rights, and Hon. Eileen Donahoe, Special Envoy & Coordinator for Digital Freedom, Dep't of State (Nov. 21, 2024); Adam Creighton & Rhiannon Down, *Greens torpedo misinformation bill as top Trump ally raises concerns*, THE AUSTRALIAN (Nov. 22, 2024); see also House Judiciary GOP (@JudiciaryGOP) X (Nov. 1, 2024, 10:06 AM), <https://x.com/JudiciaryGOP/status/1852351452192108710>.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Id.*; X Global Government Affairs (@GlobalAffairs), X (Apr. 19, 2024, 11:20 AM), <https://x.com/GlobalAffairs/status/1781342060668174707>.

⁷⁰ Adam Creighton & Rhiannon Down, *Greens torpedo misinformation bill as top Trump ally raises concerns*, THE AUSTRALIAN (Nov. 22, 2024); Australian Senator Matt Canavan (@mattjcan), X (Nov. 22, 2024, 1:41 AM), <https://x.com/mattjcan/status/1859849715862622622> ("The Labor government hasn't just offended all Australians with their outrageous attempt to silence free speech, they have also done so without any regard for how their clumsy power grab might impact our friends and allies."); see also Craig Kelly (@craigkellyXXX), X (Nov. 22, 2024, 6:40 AM), <https://x.com/craigkellyXXX/status/1859924804121587890> (a former Member of the Australian Parliament noting that it was "[g]reat to see @Jim_Jordan" warning that the bill was an "attempt at worldwide censorship and getting around the US Constitution.").

⁷¹ Oscar Godsell & Andrew Clennell, *Albanese government abandons controversial misinformation bill amid widespread opposition*, SKY NEWS (Nov. 24, 2024).

⁷² *Australia withdraws a misinformation bill after critics compare it to censorship*, AP (Nov. 24, 2024).

The Select Subcommittee has recognized there are foreign threats to American free speech given the cross-border nature of online speech. Increasingly, in the name of promoting “online safety” or combatting so-called “misinformation” or “disinformation,” foreign government officials have attempted to leverage their laws, regulations, and courts to limit what Americans can see and say in the United States.



**THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S
SILENCE: THE CASE OF BRAZIL**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



April 17, 2024

BRAZIL’S CENSORSHIP OF FREE SPEECH ONLINE

“Across the world right now, governments, in the name of the good, are considering or adopting measures like we have in Canada. In Dublin, they’re about to enact a draconian hate-crime bill that poses a dire threat to free speech. In Paris, President Emanuel Macron has called for censoring online speech. In Brussels, the EU’s Internal Market Commissioner is calling for a crackdown on ‘illegal content.’ **In Brasilia, they’re fighting ‘fake news’ and ‘disinformation’ by clamping down on legitimate online speech.** To say nothing of Russia and China and Iran. America is so exceptional—indispensable really. Please do not succumb to the same illiberal, the same authoritarianism. Please keep fighting for what you know is right. Canada is watching. The *whole world* is watching.”¹

—Rupa Subramanya, Canadian journalist, testifying before the Select Subcommittee on the Weaponization of the Federal Government, November 30, 2023

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government are conducting oversight of how and to what extent the Executive Branch has coerced or colluded with companies and other intermediaries to censor lawful speech.² In the past sixteen months, the Committee and Select Subcommittee have uncovered serious violations of the First Amendment committed by officials throughout the Executive Branch. The Committee and Select Subcommittee have documented:

- The Biden White House directly coercing large social media companies, such as Facebook, to censor true information, memes, and satire, eventually leading Facebook to change its content moderation policies;³
- The Biden White House directly coercing the world’s largest online book store, Amazon, to censor books;⁴
- Stanford’s Election Integrity Partnership (EIP)—created at the request of the Department of Homeland Security’s (DHS) Cybersecurity & Infrastructure

¹ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Nov. 30, 2023) (submitted written statement of Rupa Subramanya) (bolded emphasis added; italicized emphasis in original).

² See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

³ See *id.*; Jim Jordan (@Jim_Jordan), X, (July 27, 2023, 12:03 PM), (Facebook Files, Part 1), https://twitter.com/Jim_Jordan/status/1684595375875760128; Jim Jordan (@Jim_Jordan), X, (July 28, 2023, 12:03 PM), (Facebook Files, Part 2), https://twitter.com/Jim_Jordan/status/1684957660515328001; Jim Jordan (@Jim_Jordan), X, (Aug. 3, 2023, 11:00 AM), (Facebook Files Part 3), https://twitter.com/Jim_Jordan/status/1687116316073930752; Jim Jordan (@Jim_Jordan), X, (Sept. 5, 2023, 6:17 PM), (Facebook Files Part 5), https://twitter.com/Jim_Jordan/status/1699184930331267539; Jim Jordan (@Jim_Jordan), X, (Nov. 30, 2023, 8:44 AM) (YouTube Files Part 1), https://twitter.com/Jim_Jordan/status/1730221179632226337; Jim Jordan (@Jim_Jordan), X, (Dec. 1, 2023, 2:26 PM) (YouTube Files Part 2), https://twitter.com/Jim_Jordan/status/1730669728002142706.

⁴ See Jim Jordan (@Jim_Jordan), X, (Feb. 5, 2024, 5:44 PM) (Amazon Files), https://twitter.com/Jim_Jordan/status/1754637204146581783.

Security Agency (CISA)—working with the federal government to flag thousands of links and submit recommendations directly to large social media platforms to censor Americans’ online speech in the lead-up to the 2020 U.S. election;⁵ and

- The Federal Trade Commission (FTC) harassing Elon Musk’s Twitter (now X) because of Musk’s commitment to free speech, even going so far as to target several journalists who reported on the anti-free speech stance of the old Twitter regime.⁶

The Committee and Select Subcommittee’s oversight has shown that the government censorship that begins with a stated purpose of combatting alleged “misinformation” or “disinformation” inevitably mutates into silencing political opponents and views disfavored by those currently in power.⁷

These violations of the First Amendment and attacks on the most fundamental American civil liberty—freedom of speech—are deeply troubling. But they often pale in comparison to how some foreign governments are eroding basic democratic values and stifling debate in their countries. In furtherance of its legislative oversight, the Select Subcommittee has received testimony about how other countries’ governments, including Canada, France, and Brazil, have sought to censor speech online.⁸ These examples of foreign governments cracking down on free

⁵ STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023); *see also* Jim Jordan (@Jim_Jordan), X, (Nov. 6, 2023, 6:42 PM), https://twitter.com/Jim_Jordan/status/1721674461408006431; STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

⁶ Ryan Tracy, *FTC Twitter Investigation Sought Elon Musk’s Internal Communications, Journalist Names*, WALL ST. J. (Mar. 8, 2023); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION: AN AGENCY’S OVERREACH TO HARASS ELON MUSK’S TWITTER (Comm. Print Mar. 7, 2023), at 5 (“[O]n December 13, the FTC demanded details of Twitter’s interactions with journalists, including ‘Bari Weiss, Matt Taibbi, Michael Shellenberger, Abigail Shrier,’ and the identities of all other journalists to whom Twitter had potentially provided access of its internal records.”)

⁷ *See* Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023); Jim Jordan (@Jim_Jordan), X, (July 27, 2023, 12:03 PM), (Facebook Files, Part 1), https://twitter.com/Jim_Jordan/status/1684595375875760128; Jim Jordan (@Jim_Jordan), X, (July 28, 2023, 12:03 PM), (Facebook Files, Part 2), https://twitter.com/Jim_Jordan/status/1684957660515328001; Jim Jordan (@Jim_Jordan), X, (Aug. 3, 2023, 11:00 AM), (Facebook Files Part 3), https://twitter.com/Jim_Jordan/status/1687116316073930752.

⁸ *See, e.g.*, Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary, 118th Cong. (Nov. 30, 2023) (submitted written statement of Rupa Subramanya) (“Across the world right now, governments, in the name of the good, are considering or adopting measures like we have in Canada. In Dublin, they’re about to enact a draconian hate-crime bill that poses a dire threat to free speech. In Paris, President Emanuel Macron has called for censoring online speech. In Brussels, the EU’s Internal Market Commissioner is calling for a crackdown on ‘illegal content.’ **In Brasilia, they’re fighting ‘fake news’ and ‘disinformation’ by clamping down on legitimate online speech.** To say nothing of Russia and China and Iran. America is so exceptional—indispensable really. Please do not succumb to the same illiberal, the same authoritarianism. Please keep fighting for what you know is right. Canada is watching. The *whole world* is watching.”) (bolded emphasis added; italicized emphasis in original).

speech abroad serve as a stark warning to Americans about the threats posed by government censorship here at home. They also help to inform the Committee’s and Select Subcommittee’s legislative work to fight government censorship and promote freedom of speech.

In 2019, Brazil’s Supreme Court granted itself new powers to “act as an investigator, prosecutor and judge all at once in some cases.”⁹ Rather than relying on a prosecutor or a law enforcement officer to open an investigation, the president of Brazil’s Supreme Court, José Antonio Dias Toffoli, “issued an order granting the Supreme Court itself the authority to open an investigation.”¹⁰ Former Brazilian Supreme Court justices openly criticized the move as unprecedented and in violation of Brazil’s constitution.¹¹

In this unprecedented order, Toffoli selected fellow Brazil Supreme Court Justice Alexandre de Moraes to run the first investigation conducted by the court.¹² Moraes first joined the Supreme Federal Court in 2017.¹³ Moraes has been described as a “political animal” with hopes of being president of Brazil someday.¹⁴ Moraes has also served as president of the Superior Electoral Court since August 2022.¹⁵ The Superior Electoral Court is the highest court in Brazil that oversees the country’s electoral processes and is frequently the court that issues orders compelling the censorship of alleged misinformation about elections.¹⁶

With this new, extraordinary power, Moraes attacked critics from the right and left with impunity. Moraes reportedly ordered social media platforms to remove posts and accounts even when “much of the content did not break [the companies’] rules” and “often without giving a reason.”¹⁷ As another example, he ordered federal agents to raid eight businessmen in July 2019, in addition to freezing their bank accounts and suspending their social media accounts.¹⁸ Previously, Moraes had “ordered a federal police raid on 10 addresses tied to social media users

⁹ Jack Nicas and André Spigariol, *To Defend Democracy, Is Brazil’s Top Court Going Too Far?*, N.Y. TIMES (Sept. 26, 2022).

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

¹⁴ Ramon Sahmkow, *Alexandre De Moraes: Brazil Judge In Feud With Elon Musk*, BARRON’S (April 15, 2024).

¹⁵ Jack Nicas and André Spigariol, *To Defend Democracy, Is Brazil’s Top Court Going Too Far?*, N.Y. TIMES (Sept. 26, 2022).

¹⁶ The “Electoral Justice Permanent Program on Countering Disinformation,” created in August 2021, issued a report in 2022 detailing a “strategic plan” to be developed for the 2022 election cycle. *Strategic Plan Elections 2022, BRAZIL’S ELECTORAL JUSTICE PERMANENT PROGRAM ON COUNTERING DISINFORMATION* (2022). The report cites the Election Integrity Partnership’s (“EIP”) final report in 2020 as an international document used by the Program as a “main theoretical reference[.]” for addressing alleged disinformation. *Id.* at 16, 19. The Select Subcommittee’s investigation unveiled that the EIP was set up at the request of the U.S. Department of Homeland Security. STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH* (Comm. Print Nov. 6, 2023). The Select Subcommittee also obtained the secret misinformation reports that the EIP sent directly to social media companies with specific censorship recommendations; contrary to its purported purpose of combatting disinformation, the EIP targeted Americans’ posts containing true information, satire, and political opinions. *Id.*

¹⁷ Jack Nicas and André Spigariol, *To Defend Democracy, Is Brazil’s Top Court Going Too Far?*, N.Y. TIMES (Sept. 26, 2022).

¹⁸ *Id.*

who had criticized the court.”¹⁹ After Moraes ordered a Brazilian magazine to remove an online article alleging links between Toffoli and a corruption investigation, then-Justice Marco Aurélio Mello remarked, “I’ve been on the court for 28 years and I’ve never seen a decision like this, to take down an article,” adding that, “The Supreme Court was always engaged in preserving freedom of speech. This is a step backward.”²⁰

Recent reporting and public statements from X’s Global Government Affairs team have indicated that X is being “forced by court decisions to block certain popular accounts in Brazil” or else face serious consequences, such as incurring large fines, arresting X employees, and causing X to shut down in Brazil.²¹ On April 6, 2024, X Corp.’s CEO, Elon Musk, in the name of defending free speech online, posted that the social media platform would be “lifting all restrictions” demanded by the Brazilian government.²² The Brazilian government has reportedly launched an investigation into Musk for alleged obstruction of justice and other charges because Musk has refused to acquiesce to the Brazilian court’s, most notably Moraes’s, censorship demands.²³ To that end, to understand the threats posed by anti-free speech governments abroad, the Committee issued a subpoena to X Corp. for documents and records relating to recent efforts by the Superior Electoral Court and the Supreme Federal Court in Brazil to compel X to censor social-media accounts in the country.

The subpoenaed documents and records reveal that, since at least 2022, the Supreme Federal Court in Brazil, on which Moraes serves as a justice, and the Superior Electoral Court in Brazil, led by Moraes, have ordered X Corp. to suspend or remove nearly 150 accounts on the popular social media platform. These censorship demands were targeted specifically at critics of the Brazilian government: conservative members of the federal legislature, journalists, members of the judiciary, and even a gospel singer and a pop radio station—in other words, anyone with a platform to criticize the ruling leftist government. The Brazilian court, specifically Moraes, justified the censorship on the grounds that “it is necessary, appropriate[,] and urgent to stop the possible spread of hate speech, subversion of order[,] and encouragement to break institutional and democratic normality by blocking accounts on social networks.”²⁴ Frequently, these orders have given the social media companies only two hours to comply with the censorship demands or else face fines of up to 100,000 reais (about \$20,000 dollars) per day for noncompliance.²⁵

¹⁹ Leticia Casado and Manuela Andreoni, *Brazil’s Judiciary, Once Symbol of Anti-Corruption Drive, Now Faces Scrutiny*, N.Y. TIMES (Apr. 27, 2019).

²⁰ *Id.*

²¹ X Global Government Affairs (@GlobalAffairs), X (Apr. 6, 2024, 5:52 PM), <https://twitter.com/GlobalAffairs/status/1776729732970594483>; Elon Musk (@elonmusk), X (Apr. 6, 2024, 6:31 PM), <https://twitter.com/elonmusk/status/1776739518240170254>.

²² Elon Musk (@elonmusk), X (Apr. 6, 2024, 6:31 PM), <https://twitter.com/elonmusk/status/1776739518240170254>.

²³ See Alex Hern and Tom Phillips, *Elon Musk faces Brazil inquiry after defying X court order*, GUARDIAN (April 8, 2024); see also Michael Shellenberger, *Elon Musk Is All That Stands In The Way Of Totalitarianism*, PUBLIC (Apr. 8, 2024); Michael Shellenberger, *Socialist Strategy Behind Brazilian President Lula’s War On Free Speech*, PUBLIC (Apr. 11, 2024).

²⁴ See, e.g., Order to Discord, Meta (Facebook and Instagram), Rumble, Telegram, and Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.923 at HJCX-00054 (June 13, 2023); see Monark Voltou (@MonarkVoltou), X, <https://twitter.com/monarkvoltou>.

²⁵ See, e.g., *id.*

Most notably, the Superior Electoral Court in Brazil censored former Brazilian President Jair Messias Bolsonaro, one of the main critics of Moraes, in the weeks following Brazil's presidential election in 2022.²⁶ According to a November 22, 2023 order obtained by the Select Subcommittee, the court found Bolsonaro guilty of “practicing irregular propaganda” on X for “messages [that] are either untrue or out of context.”²⁷

As another example, in a June 13, 2023 order obtained by the Select Subcommittee, Moraes ordered the censorship of Bruno Aiub, a YouTuber and Rumble podcaster who goes by the username “Monark” and has been called “Brazil’s Joe Rogan” due to his popularity.²⁸ In the order, Moraes noted that despite his previous order deplatforming Aiub from every major social media platform, Aiub had since created new accounts and channels.²⁹ Moraes was particularly upset that Aiub allegedly “spread fraudulent news about the actions of this SUPREME COURT and the SUPERIOR ELECTORAL COURT.”³⁰ Specifically, Moraes took issue with Aiub’s statements about Moraes: “We see the TSE [Superior Electoral Court] censoring people, we see Alexandre de Moraes arresting people.”³¹ In other words, Moraes ordered the censorship of a Brazilian citizen for criticizing Moraes for censoring Brazilians.

Below is just a subset of the over 300 accounts that the Brazilian government is currently trying to force X and other social media companies to censor:

Political Opposition:

- Jair Messias Bolsonaro: 38th President of Brazil.³²
- Marcos do Val: Current Member of the Federal Senate in Brazil (the upper house of the National Congress of Brazil, the country’s federal legislative body) with 300,000 followers on X.³³
- Alan Rick: Current Member of the Federal Senate in Brazil.³⁴

²⁶ Order to Twitter, Justice Benedito Gonçalves of Superior Electoral Court of Brazil, at HJCX-00209-217 (Nov. 22, 2023).

²⁷ *Id.*

²⁸ Order to Discord, Meta (Facebook and Instagram), Rumble, Telegram, and Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.923 at HJCX-00054 (June 13, 2023); *see* Jack Nicas and Ana Ionova, *Brazil’s Joe Rogan Faces His Own Firestorm Over Free Speech*, N.Y. TIMES (Feb. 13, 2022).

²⁹ Order to Discord, Meta (Facebook and Instagram), Rumble, Telegram, and Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.923 at HJCX-00054 (June 13, 2023).

³⁰ *Id.*; *see* Monark Voltou (@MonarkVoltou), X, <https://twitter.com/monarkvoltou>.

³¹ *Id.*

³² Order to Twitter, Justice Benedito Gonçalves of Superior Electoral Court of Brazil, at HJCX-00209-217 (Nov. 22, 2023).

³³ Order to Meta (Facebook and Instagram), Gettr, LinkedIn, TikTok, Telegram, Twitter (X), and YouTube; Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Petition 10.975 at HJCX-00045 (June 15, 2023); *see* Marcos do Val (@marcosdoval), X, <https://twitter.com/marcosdoval>.

³⁴ Order to Facebook, Rumble, Telegram, TikTok, Twitter, and YouTube, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.879 at HJCX-00130 (Jan. 11, 2023); *see* Alan Rick (@alan_rick), X, https://twitter.com/alan_rick.

- Carla Zambelli: Current Member of the Brazil Chamber of Deputies (the lower house of the National Congress of Brazil, the country's federal legislative body) with 2.4 million followers on X.³⁵
- Marcel van Hattem: Current Member of the Brazil Chamber of Deputies with 969,000 followers on X.³⁶
- Cristiane Brasil: Former member of the Brazil Chamber of Deputies.³⁷
- Ed Raposo: Former candidate for the Brazil Chamber of Deputies.³⁸

Journalists and Commentators:

- Guilherme Fiuza: Brazilian journalist with 1.8 million followers on X.³⁹
- Paulo Figueiredo Filho: Brazilian journalist with 1.3 million followers on X.⁴⁰
- Rodrigo Constantino: Brazilian political commentator with 1.6 million followers on X.⁴¹
- Elisa Robson: Brazilian journalist; former candidate for the Brazil Chamber of Deputies.⁴²
- Flávio Gordon: Brazilian journalist with 229,000 followers on X.⁴³

³⁵ Order to Facebook, Twitter, Instagram, YouTube, Telegram, TikTok, Gettr, WhatsApp, and LinkedIn, Justice Alexandre de Moraes of Superior Electoral Court of Brazil, Civil Petition 241 at HJCX-00238 (Nov. 1, 2022); *see* Carla Zambelli (@Zambelli2210), X, <https://twitter.com/Zambelli2210>.

³⁶ Order to Facebook, Instagram, LinkedIn, YouTube, TikTok, Telegram, and Twitter, Justice Alexandre de Moraes of Superior Electoral Court of Brazil, Civil Petition 241 at HJCX-00262 (Nov. 3, 2022); *see* Marcel van Hattem (@marcelvanhattem), X, <https://twitter.com/marcelvanhattem>.

³⁷ Order to Twitter and Facebook, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.781 at HJCX-00100 (Oct. 22, 2022); *see* Cristiane Brasil (@crisbrasilreal), X, <https://twitter.com/crisbrasilreal>.

³⁸ Order to Twitter, YouTube, and Instagram, Justice Alexandre de Moraes of Superior Electoral Court of Brazil, Civil Petition 241 at HJCX-00394 (Nov. 26, 2022); *see* Ed Raposo (@EdRaposo_), X, https://twitter.com/edraposo_.

³⁹ Order to Facebook, Telegram, Twitter, and YouTube, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.781 at HJCX-00112 (Jan. 2, 2023); *see* Guilherme Fiuza (@GFiuzaOficial), X, https://twitter.com/GFiuza_Oficial.

⁴⁰ Order to Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Petition 10.802 at HJCX-00061 (May 17, 2023); *see* Paulo Figueiredo Filho (@OPFigueiredo), X, <https://twitter.com/OPFigueiredo>; *see also* Paulo Figueiredo Filho (@realpfigueiredo), X, <https://twitter.com/realpfigueiredo>.

⁴¹ Order to Facebook, Twitter, YouTube, and Patreon, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.781 at HJCX-00146 (Dec. 30, 2022); *see* Rodrigo Constantino (@Rconstantino), X, <https://twitter.com/Rconstantino>.

⁴² Order to Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Petition 10.625 at HJCX-00106 (Jan. 12, 2024); *see* Elisa Robson (@elisarobsondf), X, <https://twitter.com/elisarobsondf>.

⁴³ Order to Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Civil Petition 241 at HJCX-00383 (Nov. 23, 2022); *see* Flávio Gordon (@flaviogordon), X, <https://twitter.com/flaviogordon>.

Judiciary & Legal Profession:

- Ludmila Lins Grilo: Former judge with 341,000 followers on X.⁴⁴
- Marcelo Rocha Monteiro: Public prosecutor and law professor.⁴⁵

Pop Culture:

- Davi Sacer: Brazilian gospel singer-songwriter with more than 600,000 followers on X.⁴⁶
- Radio RCN: Pop radio station.⁴⁷

Government-directed censorship is not a problem contained only to authoritarian governments in faraway lands; it is happening here in the United States. The Committee's and Select Subcommittee's findings of the Biden Administration's attack on free speech reveal how the Biden Administration, like Brazil, has sought to silence the Administration's critics. On just its third day of the new Administration, the Biden White House demanded that Twitter remove Robert F. Kennedy, Jr.'s tweet that contained no misinformation "ASAP" and urged Twitter to "keep an eye out for tweets that fall in this same ~genre."⁴⁸ Turning its attention to Facebook, the Biden Administration demanded that the company censor one of its top critics on cable television, Tucker Carlson, even though his reporting was truthful and did not violate Facebook's standards.⁴⁹ Unsatisfied with going after social media companies, the Biden White House even turned its attention to book stores, pressuring Amazon to censor books expressing skepticism of vaccines.⁵⁰

Perhaps unsurprisingly, then, the Biden Administration seems to have been silent in the face of these free speech attacks abroad. The State Department's Office of the Under Secretary for Civilian Security, Democracy, and Human Rights exists to "advance the security of the American people by assisting countries around the world to build more democratic, secure,

⁴⁴ Order to Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Petition 9.935 at HJ CX-00114 (Sept. 23, 2022); *see* Ludmila Lins Grilo (@ludmilagrilo), X, <https://twitter.com/ludmilagrilo>.

⁴⁵ Order to Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.781 at HJ CX-00118 (Nov. 7, 2023); *see* Marcelo Rocha Monteiro (@MarceloRochaMon), X, <https://twitter.com/MarceloRochaMon>.

⁴⁶ Order to Facebook and Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Petition 4.781 at HJ CX-00094 (Nov. 14, 2022); *see* Davi Sacer (@DaviSacer), X, <https://twitter.com/DaviSacer>.

⁴⁷ Order to Twitter, Justice Alexandre de Moraes of Supreme Federal Court of Brazil, Inquiry 4.954 at HJ CX-00126 (Order Not Dated); *see* Rádio RCN (@RCNradiochatnet), X, <https://twitter.com/RCNradiochatnet>.

⁴⁸ Missouri v. Biden, 3:22-cv-01213, (W.D. La. Jan. 11, 2023) ECF No. 174-1 (Ex. A), <https://www.courtlistener.com/docket/63290154/174/1/missouri-v-biden/>; *see also* Robert F. Kennedy Jr (@RobertKennedyJr), X (Jan. 22, 2021, 5:41 PM), <https://twitter.com/RobertKennedyJr/status/1352748139665645569>.

⁴⁹ Rep. Jim Jordan (@Jim_Jordan), X (July 27, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684595394515214336.

⁵⁰ *See* Jim Jordan (@Jim_Jordan), X, (Feb. 5, 2024, 5:44 PM) (Amazon Files), https://twitter.com/Jim_Jordan/status/1754637204146581783.

stable, and just societies.”⁵¹ The Department, and Under Secretary Uzra Zeya, have been noticeably silent as Brazil and other countries have sought to censor speech online.⁵²

This interim report exposes Brazil’s censorship campaign and presents a startling case study of how a government can justify censorship in the name of stopping so-called “hate” speech and the “subversion” of “order.” This report includes the following documents:

- Two copies each of 28 orders, in Portuguese and in English translation, issued by Justice Alexandre de Moraes to X Corp.;⁵³
- An additional 23 orders issued by Justice Alexandre de Moraes for which X Corp. does not have an English translation;⁵⁴ and
- 37 orders issued by the Superior Electoral Court of Brazil.⁵⁵

Congress must take seriously the warnings from Brazil and other countries seeking to suppress speech online. We must never think that it cannot happen here. The Committee and Select Subcommittee have aggressively conducted oversight—issuing subpoenas, conducting fact-finding, and convening multiple hearings—to shed light on government-induced censorship in the United States and to inform additional legislative remedies. Members of the Committee and Select Subcommittee have proposed legislation, including H.R. 4791, the Free Speech Protection Act, and H.R. 4848, the Censorship Accountability Act, to protect the First Amendment and to put a stop to these constitutional abuses.⁵⁶

The Committee and Select Subcommittee will continue to investigate, hold hearings, and consider additional legislation to protect free speech online and hold those who violate Americans’ fundamental First Amendment freedoms accountable. The attacks on free speech abroad serve as a warning for America. Since his public commitment to free speech, Mr. Musk has faced criticism and attacks from governments around the world, including the United States. In Brazil, censorship of the opposing political party and investigative journalists occurs via court order. Under the Biden Administration, censorship demands are delivered in closed-door meetings with implicit regulatory threats, on top of lawfare for political opponents. Now, more than ever, Congress must act to uphold its duty to protect free expression.

⁵¹ Our Mission, Under Secretary for Civilian Security, Democracy, and Human Rights, U.S. Dep’t of State (last accessed Apr. 11, 2024).

⁵² To date, neither the State Department nor the U.S. Embassy in Brazil have issued any public statements mentioning X, Moraes, the Court’s censorship demands, or this troubling attack on free speech despite extensive public reporting on Moraes’s yearslong censorship campaign and recent targeting of Musk.

⁵³ See App’x at 13-165.

⁵⁴ See App’x at 166-220.

⁵⁵ See App’x at 221-540.

⁵⁶ See Press Release, House Judiciary Committee, Chairman Jordan, Senator Paul Fight to Protect Americans’ First Amendment Rights Against Government Censorship (July 20, 2023), <https://judiciary.house.gov/media/press-releases/chairman-jordan-senator-paul-fight-protect-americans-first-amendment-rights>; Press Release, Rep. Dan Bishop, Reps. Bishop and Hageman Introduce Bill to Hold Government Censors Accountable (July 26, 2023), <https://danbishop.house.gov/media/press-releases/rebs-bishop-and-hageman-introduce-bill-hold-government-censors-accountable>; Press Release, Rep. Harriet Hageman, Judiciary Committee Passes Two Hageman Sponsored Bills (Feb. 29, 2024), <https://hageman.house.gov/media/press-releases/judiciary-committee-passes-two-hageman-sponsored-bills>.

APPENDIX

Federal Supreme Court, Petition 10.851 (Jan. 19, 2023).....	13
Federal Supreme Court, Petition 10.981 (Feb. 28, 2023).....	18
Federal Supreme Court, Petition 9.935 (Dec. 14, 2023).....	53
Federal Supreme Court, Petition 10.975 (June 15, 2023).....	57
Federal Supreme Court, Petition 4.923 (June 13, 2023).....	63
Federal Supreme Court, Petition 10.802 (May 17, 2023).....	73
Federal Supreme Court, Petition 10.824 (Jan. 14, 2023).....	78
Federal Supreme Court, Petition 10.464 (July 17, 2023).....	82
Federal Supreme Court, Petition 11.022 (Mar. 9, 2023).....	84
Federal Supreme Court, Inquiry 4.781 (Oct. 27, 2023).....	88
Federal Supreme Court, Petition 10.800 (May 17, 2023).....	90
Federal Supreme Court, Petition 11.075 (Mar. 31, 2023).....	94
Federal Supreme Court, Petition 9.935 (Feb. 8, 2023).....	100
Federal Supreme Court, Inquiry 4.781 (Nov. 14, 2023).....	104
Federal Supreme Court, Petition 10.800 (Jan. 5, 2024).....	108
Federal Supreme Court, Inquiry 4.781 (Oct. 22, 2022).....	112
Federal Supreme Court, Petition 10.373 (Oct. 23, 2022).....	114
Federal Supreme Court, Petition 10.625 (Jan. 12, 2024).....	118
Federal Supreme Court, Inquiry 4.781 (Jan. 2, 2023).....	122
Federal Supreme Court, Petition 9.935 (Sep. 23, 2022).....	126
Federal Supreme Court, Inquiry 4.781 (Nov. 7, 2023).....	130
Federal Supreme Court, Petition 10.685 (Dec. 10, 2022).....	132
Federal Supreme Court, Inquiry 4.954 (No date listed).....	138
Federal Supreme Court, Inquiry 4.879 (Jan. 11, 2023).....	142
Federal Supreme Court, Inquiry 4.781 (Jan. 9, 2023).....	150
Federal Supreme Court, Petition 10.802 (Jan. 5, 2023).....	154
Federal Supreme Court, Inquiry 4.781 (Dec. 30, 2022).....	158

Federal Supreme Court, Petition 10.391 (Feb. 6, 2022).....	166
Federal Supreme Court, Inquiry 4.781 (Nov. 13, 2022).....	171
Federal Supreme Court, Petition 10.802 (No Date Listed).....	173
Federal Supreme Court, Petition 9.935 (Nov. 14, 2022).....	177
Federal Supreme Court, Petition 10.474 (July 20, 2022).....	179
Federal Supreme Court, Petition 9.935 (Sep. 26, 2023).....	180
Federal Supreme Court, Inquiry 4.879 (Aug. 16, 2021).....	182
Federal Supreme Court, Inquiry 4.781 (Aug. 23, 2023).....	187
Federal Supreme Court, Petition 10.391 (June 20, 2022).....	189
Federal Supreme Court, Petition 9.935 (Feb. 11, 2022).....	192
Federal Supreme Court, Petition 10.792 (Mar. 27, 2023).....	194
Federal Supreme Court, Petition 10.708 (Dec. 24, 2022).....	196
Federal Supreme Court, Petition 10.373 (June 18, 2022).....	198
Federal Supreme Court, Petition 10.373 (Aug. 23, 2022).....	200
Federal Supreme Court, Petition 10.464 (July 12, 2022).....	202
Federal Supreme Court, Petition 10.535 (Aug. 22, 2022).....	203
Federal Supreme Court, Petition 10.648 (Dec. 24, 2022).....	205
Federal Supreme Court, Petition 10.648 (Oct. 31, 2022).....	207
Federal Supreme Court, Petition 9.935 (Oct. 5, 2022).....	209
Federal Supreme Court, Petition 11.704 (Aug. 31, 2023).....	212
Federal Supreme Court, Petition 10.484 (July 28, 2022).....	214
Federal Supreme Court, Inquiry 4.923 (June 2, 2023).....	215
Superior Electoral Court, No. 0601752-80.2022.6.00.0000 (Nov. 22, 2023).....	221
Rondônia Regional Electoral Court, No. 0601765-67.2022.6.22.0000 (Sep. 26, 2022).....	230
Regional Electoral Court of Mato Grosso, No. 0601831-53.2022.6.11.0000 (Oct. 14, 2022).....	242
Superior Electoral Court, No. 0601823-82.2022.6.00.0000 (Oct. 31, 2022).....	246
Superior Electoral Court, No. 0601843-73.2022.6.00.0000 (Nov. 1, 2022).....	250
Superior Electoral Court, No. 0601843-73.2022.6.00.0000 (Dec. 1, 2022).....	257

Superior Electoral Court, No. 0601843-73.2022.6.00.0000 (Feb. 17, 2023).....	261
Superior Electoral Court, No. 0601853-20.2022.6.00.0000 (Nov. 10, 2022).....	263
Superior Electoral Court, No. 0601811-68.2022.6.00.0000 (Nov. 3, 2022).....	274
Superior Electoral Court, No. 0601867-04.2022.6.00.0000 (Nov. 4, 2022).....	281
Superior Electoral Court, No. 0601864-49.2022.6.00.0000 (Nov. 4, 2022).....	288
Superior Electoral Court, No. 0601872-26.2022.6.00.0000 (Nov. 22, 2022).....	295
Superior Electoral Court, No. 0601875-78.2022.6.00.0000 (Nov. 5, 2022).....	298
Superior Electoral Court, No. 0601877-48.2022.6.00.0000 (Nov. 8, 2022).....	303
Superior Electoral Court, No. 0601881-85.2022.6.00.0000 (Nov. 6, 2022).....	308
Superior Electoral Court, No. 0601881-85.2022.6.00.0000 (Feb. 1, 2023).....	328
Superior Electoral Court, No. 0601889-62.2022.6.00.0000 (Nov. 8, 2022).....	332
Superior Electoral Court, No. 0601889-62.2022.6.00.0000 (Feb. 6, 2022).....	365
Superior Electoral Court, No. 0601894-84.2022.6.00.0000 (Nov. 8, 2022).....	369
Superior Electoral Court, No. 0601912-08.2022.6.00.0000 (Nov. 14, 2022).....	380
Superior Electoral Court, No. 0601942-43.2022.6.00.0000 (Nov. 20, 2022).....	383
Superior Electoral Court, No. 0601942-43.2022.6.00.0000 (Nov. 25, 2022).....	387
Superior Electoral Court, No. 0601941-58.2022.6.00.0000 (Nov. 20, 2022).....	389
Superior Electoral Court, No. 0601963-19.2022.6.00.0000 (Nov. 24, 2022).....	395
Superior Electoral Court, No. 0601963-19.2022.6.00.0000 (Feb. 1, 2023).....	404
Superior Electoral Court, No. 0601969-26.2022.6.00.0000 (Nov. 26, 2022).....	406
Superior Electoral Court, No. 0601969-26.2022.6.00.0000 (Feb. 1, 2023).....	421
Superior Electoral Court, No. 0602037-73.2022.6.00.0000 (Dec. 26, 2022).....	425
Superior Electoral Court, No. 0602041-13.2022.6.00.0000 (Dec. 29, 2022).....	434
Superior Electoral Court, No. 0600003-91.2023.6.00.0000 (Jan. 6, 2023).....	447
Superior Electoral Court, No. 0600004-76.2023.6.00.0000 (Jan. 8, 2023).....	453
Superior Electoral Court, No. 0600004-76.2023.6.00.0000 (Feb. 1, 2023).....	457
Superior Electoral Court, No. 0600011-68.2023.6.00.0000 (Jan. 11, 2023).....	461
Superior Electoral Court, No. 0601755-35.2022.6.00.0000 (May 17, 2023).....	494

Zanin Martins & Aragao y Ferraro, Letter to Alexandre de Moraes, President of the Superior Electoral Court (Oct. 26, 2022).....	501
Superior Electoral Court, No. 0601869-71.2022.6.00.0000 (Nov. 4, 2022).....	527
Superior Electoral Court, No. 0601964-04.2022.6.00.0000 (June 5, 2023).....	533

PETITION 10.851 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 19, 2023.

To the company
FACEBOOK ONLINE SERVICES BRAZIL LTDA

Ref: Pet 10.851

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

I ALSO ORDER THE FOLLOWING MEASURES:

(8) THE ISSUANCE OF AN ORDER to the companies FACEBOOK and TWITTER, so that, within two (2) hours, they block the channel/profile/account listed below, as well as any groups managed by the users identified below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

FACEBOOK

<https://www.facebook.com/rubemabdalla.barrosojunior?mibextid=LQQJ4d>

<https://www.facebook.com/abdallapatriota.junior.5?mibextid=LQQJ4d>

PET 10851 / DF

INSTAGRAM

[https://instagram.com/rubemabdalla?
igshid=NDk5N2NlZjQ=](https://instagram.com/rubemabdalla?igshid=NDk5N2NlZjQ=)

TWITTER

[https://twitter.com/abdallaabraba02?
s=21&t=SMcq7u1zCMFbaUwXDJgMwQ](https://twitter.com/abdallaabraba02?s=21&t=SMcq7u1zCMFbaUwXDJgMwQ)

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy for the Federal Police

PETIÇÃO 10.851 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 19 de janeiro de 2023.

À empresa
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA

Ref: Pet 10.851

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA, AS SEGUINTE MEDIDAS:

(8) a EXPEDIÇÃO DE OFÍCIO às empresas FACEBOOK e TWITTER, para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminado, bem como de quaisquer grupos que sejam administrados pelos usuários abaixo identificados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

FACEBOOK

<https://www.facebook.com/rubemabdalla.barrosojunior?mibextid=LQQJ4d>

<https://www.facebook.com/abdallapatriota.junior.5?mibextid=LQQJ4d>

PET 10851 / DF

INSTAGRAM

[https://instagram.com/rubemabdalla?
igshid=NDk5N2NIZjQ=](https://instagram.com/rubemabdalla?igshid=NDk5N2NIZjQ=)

TWITTER

[https://twitter.com/abdallaabrpa02?
s=21&t=SMcq7u1zCMFbaUwXDJgMwQ](https://twitter.com/abdallaabrpa02?s=21&t=SMcq7u1zCMFbaUwXDJgMwQ)

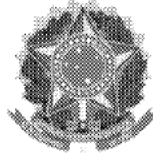
Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente



Federal Supreme Court

URGENT

SECRET

Electronic letter no. 2140/2023

Brasilia, February 28, 2023.

To the Administrator of TWITTER Brasil
Rede de Informação Ltda.

Petition No. 10981

Mr. Administrator,

Pursuant to the confidential decision handed down in the case in question, I ask you to **urgently** block, **within two (2) hours**, the channels/profiles/accounts listed in the decision, as well as any groups administered by the identified users, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this Court and the full preservation of their content.

Sincerely,

Minister Alexandre de Moraes
Rapporteur
Digitally signed document

PETITION 10.981 FEDERAL DISTRICT

Rapporteur : MIN. ALEXANDRE DE MORAES
 Author : UNDISCLOSED
 Lawyer : UNDISCLOSED

DECISION

These are statements by the Federal Council of the Brazilian Bar Association (CFOAB), through which it reports alleged unlawful actions and requests against the Brazilian Conservative Bar Association - OACB (STF petitions n' 4.014/2023 and 8.544/2023).

The petitioner states that the defendant, which has the legal nature of an association, has *"waged a veritable Tumult against the Brazilian democracy, through its social media profiles, especially on twitter (<https://twitter.com/AdvogadosOacb?s=20&t=9WJNCjBadeB7etQoLoXv3A>) and Instagram (https://www.instagram.com/oacb_advogados_conservadores/)* which he has approximately 100 (one hundred) thousand followers. The claimant's narrative is accompanied by posts made by the Defendant, such as *tweets* and videos, with the following words:

"Bolsonaro will be President of the Republic from 2023 to 2026 - Understand!!!" - video, on 25/12/2022;

"We must continue to populate Brasilia and the fronts of the barracks demanding an answer that the previous Minister of Defense did not have: the delivery of the information (the source codes?), which the TSE has so far failed to provide. Prevarication is a crime! Pay attention to the sole paragraph of art. 1 of the Constitution." - tweet, on 6/1/2023;

"Make no mistake: those who call themselves 'jurists or lawyers for democracy' but support this government have nothing democratic about them. They are just like them. Sadly, this is the truth." - *tweet*, on 6/1/2023;

PET 10981 / DF

"THE STF CAN NEVER BE THE LAST WORD BECAUSE he became a dictator, since he was not elected by the people. Floriano Peixoto arrested 13 general officers. Rui Barbosa filed a writ of habeas corpus with the Supreme Court. Floriano remarked: 'and who will give habeas-corpus to the Supreme Court?' (Book The Republic is Born)." - tweet, 8/1/2023;

"We reiterate our commitment to the truth and in the same way that the colleague in the video, who does not belong to our ranks, received information about the death of protesters (with confirmation), we also received it. We ask Mr. @marcosdoval and Mr. @Biakicis to look into the matter." - tweet, 10/1/2023;

"GILMAR MENDES said that 'Brazil has lived through an era of darkness when it comes to criminal procedure'. No! Under the military governments, armed subversives and guerrillas were arrested. The military didn't arrest children and innocent people. At that time, good citizens were respected and protected" - tweet, on 15/1/2023;

"The Brazilian state will suffer sanctions and compensation for these victims of abuse of authority and torture to which the INNOCENTS are being subjected. The bill will be paid by everyone, due to the irresponsibility of public agents from a government of unprepared people." - tweet, on 15/1/2023;

"Of course, it was the most ludicrous of narratives. It is astonishing that the Judiciary should put INNOCENTS in jail under anti-legal arguments. The Constitution continues to be violated." - tweet, on 18/1/2(123;

The plaintiff's narrative is also illustrated by a report that reads: "Influential names from Bolsonaro's base share false information from the non-governmental organization Ordem dos Advogados Conservadores do Brasil (OACB) as if they were from the general entity of lawyers" and "Parliamentarians attribute false information about the attacks in Brasilia to the OAB", dated 13/1/2023, published by "Redação O Sul", as transcribed below:

2

PET 10981 / DF

"In the middle of the repercussions of the acts that culminated in the depredation of the headquarters of the Three Powers in Brasilia last Sunday (08), parliamentarians and influential names from the Bolsonaro base are sharing false information from the non-governmental organization Ordem dos Advogados Conservadores do Brasil (OACB) as if they were from the Brazilian Bar Association (OAB) - the highest entity representing and regulating the legal profession in the country.

The movement that induces intemauts to misinform was started by federal deputy-elect Gustavo Gayer (PL-GO) last Monday (09). At the time, he said via Twitter that lawyers from the OAB had left the provisional prison of the Federal Police (PF) and were "shocked by the fact that they had children in prison". In fact, they were OACB professionals.

The attitude was repeated in the tribune of the House of Deputies by Bia Kicis (PL-SE). At the time, she spread fake news that she claimed had been backed by the Chamber's the Order of Bar of Brazilian of the Federal District (OAB- DF). 'I've just received news that a lady died today on the premises of the Federal Police. Not on the premises of the Military Police. I'm talking about a lady who was denied food and water and who, after hours and hours and hours of being mistreated and neglected, died," said Kicis on Tuesday morning (10) in the gallery.

Later, on Twitter, the parliamentarian apologized for the mistake' *and insisted* that the confirmation *was* actually from the OACB. The group gained notoriety in 2021 when it threatened to sue anyone who insulted then-president Jair Bolsonaro (PL). At the time, the OAB went to court against the OACB for attempting to misuse the

8

PET 10981 / DF

name of the Bar and disciplinary infraction.

Also on Tuesday, the federal deputy elected with the most votes in Ceara, Andre Fernandes, published the fake news of the death of the elderly woman in the PF gymnasium with the endorsement of the OACB. 'Imprisoned children, elderly people having heart attacks, a death of an elderly woman detained in the PF confirmed by the OACB. Lack of water, food and toilets. The videos that are circulating are revolting," he said.

Since Sunday, the non-governmental organization has made itself available to the arrested protesters: associate lawyers provide services without charging fees. On social media, the OACB also spread fake news such as the narrative that Sunday's acts of vandalism were carried out by infiltrators. "We will not tolerate acts of violence and vandalism. On the other hand, we will not abandon who did not commit any crime. The Order of Conservative Lawyers of Brazil - OACB is in Brailia and will provide assistance to all Paraibans, he wrote." (<https://www.osul.com.br/parlamentares-oabinformacoes-false-attacks/>)

In proof of the fact reported and individualized above, the Applicant presents the following posts by Federal Deputies ANDRÉ JANONES and BIA KICIS, on the social network Twitter, both dated 11/1/2023:

"The bolsonarist MP Bia Kicis, investigated in the fake news inquiry, used the chamber's rostrum to LIE. Bia Kicis in her speech said that the president of the OAB confirmed the death of a lady in PF custody and this lie has been used to imitate the coup plotters" -Federal Deputy André Janones;

"You irresponsible bastard! I'll take you to the ethics council. I didn't use the rostrum to lie. I said that the death had not been confirmed. When I came down from the Tribune, I said that I had received a post from the OAB (I've already clarified that it was the OACB) confirming the death, which was later denied by the PF.

4

PET 10981 / DF

I've sent a letter to the PF asking for information." - Federal Deputy Bia Kicis.

The petitioner goes on to say that *"the posts are far from the simple exercise of the free expression of thought and represent a real threat to the democratic rule of law" and that "the repercussions resulting from the sharing of information as if it were from the OAB - an entity that represents and governs the country - confirms the disorder practiced by the OACB." "The repercussions resulting from the sharing of information [that] appears to be that of the OAB - the body that represents and regulates the legal system in the country - confirms the disorder caused by the OACB, by distorting the OAB's purpose, which is to defend the legal order of the democratic state of law, human rights and social justice, and to advocate for the proper application of the laws, for the swift administration of the judiciary and for the improvement of legal culture and institutions, in accordance with Art. 44, I, of Federal Law n. 8.906/1994 '.*

The applicant informs that he notified the mentioned association by means of Official Letter No. 26/2023 so that it would cease the irregular registration of its volunteer lawyers in custody hearings, in favor of detainees as a result of the anti-democratic acts of 8/1/2023, without proof of the granting of a mandate, but, despite the confirmation of receipt of the notification by the representative of the entity, *"recent publications on their social media profiles (<https://twitter.com!AdvogadosOacb>) show the continuity of their supposedly 'pro bano' work (...) with a warning that lawyers could be using their status as 'volunteers' associated with the 'OACB' but, at the same time, asking for payment of a pecuniary consideration for their defense (<https://twitter.com/AdvogadosOacb/status/1616156133844193283>), which would, in theory, be repudiated by the association".*

In the second petition, the applicant asked for the *"extrajudicial notification" to be attached, signed by the representatives of the Respondent and addressed at the same time to the President of the Sectional Council/DF of the Brazilian Bar Association and to the President of the Federal Council of the OAB, from which he highlights the following excerpts, which he believes reinforce the arguments already made:*

"there are complaints from inmates of alleged veiled suggestions that the

PET 10981 / DF

inducing them to confess to crimes and make agreements that supposed to help them "get out of jail";

"in addition to prohibiting judges from granting any order for the release or relaxation of arrests, until that moment, the criminal classification was not even individualized on the basis of evidence";

"the victims of the authoritarianism of the Brazilian state are being tortured physically and psychologically in prisons in this city";

"this process has so many contaminations that it is completely invalid.";

"terms such as 'terrorists' and 'coup plotters' were fallaciously coined, indiscriminately, affecting the population made up of good citizens and even entire families present there, without individualizing the accusations and keeping them imprisoned, without now entering into meritorious questions."

"We denounce to Your Excellency what has been happening, *in the past*, within the premises of buildings of the Brazilian State (by actions and omissions), SERIOUS VIOLATION OF HUMAN RIGHTS resulting from the complaints of citizens, which denote the CRIMES OF TORTURE (physical and psychological), MISTREATMENT, SUPPRESSION OF MOVEMENT AND OF EXPRESSION, affecting mostly innocent citizens";

"We are perplexed by decisions based on judicial inventions, creating legal and procedural artifices that run counter to the law in order to serve the desire to persecute and punish disaffected people. If anyone is practicing anti-democratic acts, it is the agents of the State."

"OUR CLASS is suffocating in the face of the imbalance of the

PET 10981 / DF

"tripod of Justice", not with a sword massacring Brazilian society with a superiority not provided for in the legal system. This skewed handling of the Magna Carta and infra-constitutional legislation occurs with a high degree of authoritarianism and arrogance, without respect for due process of law and the tripartite nature of the Powers, as well as the PEOPLE, the real holder of Power."

"The overwhelming majority are good citizens (since we disregard the infiltrators), families, ladies, gentlemen, the elderly, workers, with a fixed address and documented, were arrested on 08/01/2023, in an arbitrary and UNCONSTITUTIONAL manner, and remain so, illegally, in inhuman conditions, without having committed a crime."

"It has become clear that there was orchestrated vandalism, financed by groups sympathetic to the current government and perhaps even with the connivance of the authorities, as reported by Brazilian intelligence. The purpose of *this* was to incite destruction and blame the patriotic demonstrators, overwhelmingly orderly people, legitimately dissatisfied with the lack of transparency in the electoral system, which is lawful and any demonstration that intends to brand them as 'Scammers' should be repudiated (families with children, the elderly, wheelchair users and unarmed people will give what goal to the President??? not even asking for military intervention can make them out to be coup plotters because there is a constitutional provision - and it's one thing to ask for it, but quite another to be granted it!!!). The action orchestrated by vandals was not born out of a meeting of demonstrators, but only to generate a narrative and justification for the authoritarian advance of the habitual abusers of authority, under the frivolous pretext of 'action against terrorism'. What a load of crap!".

The Applicant points out that the promotion of false news must be repressed, in an attack on the Democratic Rule of Law and the rule of law.

PET 10981 / DF

disinformation "of thousands of followers" and, above all, the *"petty and media attack on the independence and harmony of the branches of government."*

It gives an example of the conduct to be repressed, highlighting the inferences made by the Respondent about "the alleged constitutionality of mining in favor of pressure on democratic rights, in addition to the recurring 'thesis' of an 'infiltrated' movement to incriminate 'good citizens' and the constant questioning of the Brazilian electoral system". It points out that the Respondent claims that there have been "repeated complaints of gross human rights violations perpetrated by the Brazilian government, and that the OAB has been silent", without the presentation of any probative document, without individualizing the names of those who were allegedly reduced to confessing to crimes and entering into agreements, nor those who were allegedly tortured (physically and psychologically), ill-treated or had their freedom of movement suppressed outside the hypotheses provided for in the Constitution and criminal law.

Finally, it makes the following requests:

"a) A immediate SUSPENSION OF ACTIVITIES JURISDICTIONS EXERCISED BY THE 'represented', i.e. that OACB refrains from providing/offering legal services;

b) that the 'defendant' immediately refrain from using the imitation of the acronym and name of the Brazilian Bar Association for any purpose, in particular that it STOP USING THE ACLUDE AND NAME OF THE OAB TO DISSEMINATE FAKE NEWS AGAINST DEMOCRACY;

c) that the 'defendant' stops attracting/managing cases/clients for lawyers, especially in favor of the members of its associative courts;

d) that the 'defendant' refrain from perpetrating offenses and disparaging the image of the Brazilian Bar Association and its members;

e) that the defendant' be prevented from promoting censorship, restricting the free expression of thought, freedom of communication and information through the

PET 10981 / DF

filing of lawsuits; and

f) that the 'defendant' refrains from carrying out any advertising for the provision/offering of legal services".

The Attorney General's Office, summoned to express its opinion, requested *"that continuity jurisdiction and Brazilian Bar*

This is the report. SO I DECIDE.

The facts narrated in the representations of the Federal Council of the Brazilian Bar Association, as reported, are pertinent to those that are the subject of the investigation initiated by decision in these proceedings and referred to Inq. 4.923/DF.

The reported conduct of the Conservative Bar Association of Brazil took place in the context of anti-democratic acts, in which groups - financed by businessmen - dissatisfied with the legitimate result of the election, with violence and serious threats to people, began to block traffic on several highways in the country, with the intention of abolishing the Democratic Rule of Law, calling for a "military coup" and the return of the Dictatorship, resulting in the terrorist acts that took place on the Esplanade of Ministries on January 8, 2023, with the destruction of the buildings of the NATIONAL CONGRESS, the PALACIO DO PLANALTO and, with much more anger and hatred, the SUPREME FEDERAL COURT, facts that have been widely investigated in various proceedings before this SUPREME COURT.

In fact, the numerous manifestations of the "Conservative Bar Association of Brazil", in a preliminary analysis, have the character of instigating the acts that took place on 8/1/2023, which may constitute the crimes provided for in arts. 2, 3, 5 and 6 (terrorist acts, including preparatory acts) of Law 13.260/16 and in arts. 147 (threat), 147-A, § 1º, item III, (persecution), 163 (damage), art. 286 (incitement to crime), art.

9

PET 10981 / DF

250, § 1', item I, paragraph "b" (arson), 288, sole paragraph (armed criminal association), 359-L (violent abolition of the Democratic State of Law), 359-M (coup d'état), all of the Penal Code:

Law n. 13.260/2016

Terrorism

Art. 2 Terrorism consists of one or more individuals committing the acts provided for in this article, for reasons of xenophobia, discrimination or prejudice of *race, color, ethnicity and religion*, when committed with the purpose of provoking social or generalized terror, exposing people, property, public peace or public safety to danger.

§ 1 The following are acts of terrorism:

I - using or threatening to use, transporting, storing, carrying or bringing with them explosives, toxic gases, poisons, biological, chemical, nuclear contents or other means capable of causing damage or promoting mass destruction;

IV - sabotage the operation or seize, with violence, serious threat to the person or using cyber-medical mechanisms, total or partial control, even temporarily, of means of communication or transportation, ports, airports, railway or bus stations, hospitals, health care facilities, schools, sports stadiums, public facilities or places where essential public services are provided, power generation or transmission facilities, military facilities, oil and gas exploration, refining and processing facilities and banking institutions and their service network;

V - attempt against the life or physical integrity of a person:

Penalty - imprisonment, from twelve to thirty years, in addition to the following sanctions corresponding to threats or violence.

§ Paragraph 2 The provisions of this article do not apply to the individual or collective conduct of people in political demonstrations, social movements, trade unions, religious movements, class or professional category movements, which are directed by social purposes or

PET 10981 / DF

claims, aimed at contesting, criticizing, protesting or supporting, with the aim of defending constitutional rights, guarantees and freedoms, without prejudice to the criminal classification contained in the law.

Art. 3 To promote, constitute, join or assist, personally or through an intermediary, a terrorist organization:

Penalty - imprisonment from five to eight years and a fine.

Art. 5 - Carrying out preparatory acts of terrorism with the unequivocal intention of committing the crime:

Penalty - that corresponding to the consummated offense, reduced by one quarter to one half.

§ Paragraph 1 - The same penalties apply to the agent who, with the intention of committing acts of terrorism:

I - recruiting, organizing, transporting or supplying individuals who travel to a country other than that of their residence or nationality; or

II - provide or receive training in a country other than that of their residence or nationality.

§ 2 In the cases of § 1º, when the conduct does not involve training or travel to a country other than that of their residence or nationality, the penalty will be that corresponding to the consummated offense, reduced by half to two thirds.

Art. 6 Receive, provide, offer, obtain, keep, deposit, request, invest, in any way, directly or indirectly, resources, assets, goods, rights, values or services of any nature, for the planning, preparation or execution of the crimes provided for in this Law:

Penalty - imprisonment from fifteen to thirty years.

Sole paragraph. The same penalty applies to anyone who offers or receives, obtains, stores, keeps in deposit, solicits, invests in or in any way contributes to obtaining assets, goods or financial *resources* for the purpose of financing, in whole or in part, a person, group of people, association, entity or criminal organization whose main or secondary activity, even on an occasional basis, is the commission of the crimes provided for in this Law.

PET 10981 / DF

Threats

Art. 147 - Threatening someone, by word, writing or gesture, or any other symbolic means, to cause them unjust and serious harm:

Penalty - detention, from one to six months, or a fine

Sole Paragraph - This will only be done through representation.

Persecution

Art. 147-A Stalking someone, repeatedly and by any means, threatening their physical or psychological integrity, restricting their ability to move or, in any way, violating or disturbing their freedom or privacy.

Penalty - imprisonment, from 6 (six) months to 2 (two) years, and a fine.

Damage

Art. 163 - Destroying, rendering useless or deteriorating something else: Penalty - detention, from one to six months, or a fine.

Qualified damage

Sole paragraph - If the crime is committed:

I - with violence against the person or serious threat;

II - with the use of a flammable or explosive substance, if this does not constitute a more serious crime;

III - against the assets of the Union, a state, the Federal District, a municipality or an autarchy, public foundation, public company, mixed-capital company or public service concessionaire;

IV - for a selfish motive or with considerable prejudice for the victim:

Penalty - detention, from six months to three years, and a fine, in addition to the penalty corresponding to the violence.

Fire

PET 10981 / DF

5

Art. 250 - Causing fire, exposing t h e life, physical integrity or property of others to danger:

Penalty - imprisonment from three to six years and a fine. Penalty increase

§ Paragraph 1 - Penalties are increased by one third:

I - if the crime is committed with the intention of obtaining a pecuniary advantage for one's own benefit or for the benefit of others:

b) in a public building or a building intended for public use or for social welfare or cultural work

Crime call

Art. 286 - Publicly inciting the commission of a crime: Penalty - detention, from three to six months, or a fine.

Sole paragraph. Anyone who publicly incites animosity between the Armed Forces, or between the Armed Forces and the constitutional powers, civil institutions or society, shall incur the same penalty.

Criminal association

Art. 288. Three (3) or more persons associate for the purpose of specific purpose of committing crimes:

Penalty - imprisonment from one (1) to three (3) years.

Sole paragraph. The penalty is increased by up to half if the association is armed or if a child or adolescent is involved.

Violent abolition of the democratic rule of law

Art. 359-L. Attempting, with the use of violence or serious threat, to abolish the democratic rule of law by preventing or restricting the exercise of constitutional powers:

Penalty - imprisonment from 4 (five) to 8 (eight) years, in addition to the penalty corresponding to violence.

Coup d'état

Art. 359-M. Attempting to depose, by means of violence or serious threat, the legitimately constituted government:

13
8

PET 10981/DF

Penalty - imprisonment, from 4 (four) to 12 (twelve) years, in addition to the penalty corresponding to the violence.

Law n. 9.605/1998

Art. 62: Destroy, render useless or deteriorate.

I - well specially protected by law, act administrative or judicial decision;

II - archive, registry, museum, library, art gallery, scientific facility or similar protected by law, administrative act or court decision:

Penalty - imprisonment from one to three years and a fine.

Sole paragraph. If the crime is culpable, the penalty is six months to one year in prison, without prejudice to a fine.

Art. 65. Graffiti or other means of defacing a building or urban monument:

Penalty - detention, from 3 (three) months to 1 (one) year, and a fine.

§ Paragraph 1' *if the* act is carried out on a monument or thing listed for its artistic, archaeological or historical value, the penalty is 6 (six) months to 1 (one) year imprisonment and a fine.

There is, therefore, sufficient evidence in the case file to partially and provisionally grant the requests made by the Applicant Federal Council of the Brazilian Bar Association, under the terms of Law no. 8.906/94 (in particular, art. 1, I and II, art. 3, art. 4, sole paragraph, art. 15, art. 16, § 1, § 2, § 3 and § 4, art. 34, IV and XVII, art. 44, I, II and § 2, art. 54, I, II, and III), Decree-Law n. 3.688/41 (art. 47), Law n. 9.279/96 (art. 124, V, XIX, XXIII, and art. 189, I and II), the Civil Code (arts. 50, § 1º, and 53), the General Regulations of the OAB (arts. 4 and 27, § 2), the Code of Ethics and Discipline of the OAB (arts. 5, 7, 31, 39 and 47) and Provision n. 94/2000 of the Federal Council of the OAB.

In view of the circumstances outlined, it is essential to carry out due diligence, including the exceptional withdrawal of individual guarantees that cannot be used as a real shield

PET 10981 / DF

protection for the practice of illicit activities, nor as an argument for the removal or diminution of civil or criminal liability for criminal acts, under penalty of disrespecting a true State of Law (HC n* 70.814-5/SP, Rel. Min. CELSO DE MELLO, First Panel, DJ of 24/6/1994).

Therefore, it is necessary, appropriate and urgent to suspend the legal activities carried out by the Brazilian Conservative Bar Association, as well as to block its social networks, which are used to attack the democratic rule of law, given the possibility of their use to encourage illegal and anti-democratic acts, with the aim of interrupting the injury or threat to a right (art. 5, XXXV, Federal Constitution).

In view of all the above, I DETERMINE the adoption of the following measures, under penalty of a daily fine of R\$ 20,000.00 (twenty thousand reais), by personally summoning GERALDO JOSÉ BARRAL LIMA (OAB/PB 18.014-A), President of the Brazilian Bar Association:

1) IMMEDIATE SUSPENSION of the legal activities carried out by the Brazilian Conservative Bar Association, with the association refraining from providing/offering legal services and from any advertising of the provision/offering of legal services;

2) a ban on the use of imitation acronyms of the imitation of the acronym and name of the Brazilian Bar Association for any purpose, especially to disseminate *fake* news against the Democratic Rule of Law and its institutions;

3) PROHIBITION OF ACTION of the Conservative Bar Association of Brazil in order to attract/agency causes/clients for any lawyers, especially in favor of its members; and

15

132
S

PET 10981 / DF

4) THE PROHIBITION of the Conservative Bar Association of Brazil to perpetrate offenses and disparage the image of the Brazilian Bar Association and its members

AFTER REGISTRATION, I RECOMMEND THAT THE CASE FILE BE SENT TO THE FEDERAL POLICE so that, within 15 (fifteen) days, they can hear the people named below, as well as to adopt all the appropriate measures to investigate the facts, except those subject to the jurisdictional reserve clause:

- (a) GERALDO JOSÉ BARRAL LIMA (President of the defendant - OAB/PB 18.014-A);
- (b) JOÃO ALBERTO DA CUN HA FILHO (Vice-President of the Defendant - OAB/PB 10.705)
- (c) SARA PATRICIA RIBEIRO FARIAS (Director-Secretary of the Defendant - OAB/RR 1.008),
- (d) MAILSOM LIMA MACIEL (Defendant's Financial Director - OAB/PB 10.732),
- (e) RAQUEL DIAS MAGALHÃES DE BARROS LEAL (Defendant's Regional Director - OAB/CE. 22.808-B),
- (f) PATRICIA MUNHOZ E SILVA (Defendant's External Relations Director - OAB/PR. 50.893) and
- (g) FREDERICO AUGUSTO ANDRADE VIEGAS (Director-Internal Relations of the Defendant - OAB/RJ 167.448).

I FINALLY DETERMINED:

(1) SENDING LETTERS TO COMPANIES **TWITTER** and **FACEBOOK**, to block, within 2 (two) hours, the channels/profiles/accounts listed below, as well as any groups managed by the users identified below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

16



sf

PET 10981 / DF

FACEBOOK

<https://www.facebook.com/OACB.ORG.BR>

<https://www.facebook.com/ordem.adv.conservadores>

/

GETTR

https://gettr.com/user/oacb_org_br

INSTAGRAM

https://www.instagram.com/oacb_advogados_conservadores/

LINKEDIN

<https://www.linkedin.com/Jin/oacbadvogadosconservadores>

TWITTER

<https://twitter.com/AdvogadosOacb>

YOUTUBE

<https://www.youtube.com/c/OACBBrasil>

(2) TO EXEDIT AN OFFICE to ANATEL so that proceed to the specific withdrawal from the website <https://www.oacb.org.br/> of operation in the national territory.

The Secretariat, for the necessary measures. Inform the Attorney General's Office.

The Federal Council of the Brazilian Bar Association should be notified, with a copy of decision.

Brasilia, February 28, 2023.

Minister ALEXANDRE DE MORAES

Rapporteur

Digitally signed document



Supremo Tribunal Federal

URGENTE

SIGILOSO

Ofício eletrônico nº 2140/2023

Brasília, 28 de fevereiro de 2023.

Ao Senhor
Administrador do TWITTER Brasil Rede de Informação Ltda.

Petição nº 10981

Senhor Administrador,

Nos termos de decisão sigilosa proferida nos autos em referência, solicito a Vossa Excelência que proceda, **com urgência, no prazo de 2 (duas horas)**, ao bloqueio dos canais/perfis/contas discriminadas na decisão, bem como de quaisquer grupos que sejam administrados pelos usuários identificados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta Corte e a integral preservação de seu conteúdo.

Atenciosamente,

Ministro Alexandre de Moraes
Relator
Documento assinado digitalmente

PETIÇÃO 10.981 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
 REQTE.(S) : SOB SIGILO
 ADV.(A/S) : SOB SIGILO

DECISÃO

Trata-se de manifestações do Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), por meio das quais noticia suposta atuação ilícita e veiculam requerimentos em desfavor da Ordem dos Advogados Conservadores do Brasil – OACB (petições STF nº 4.014/2023 e 8.544/2023).

Narra o requerente que a noticiada, que tem natureza jurídica de associação, tem *“empreendido verdadeiro tumulto contra a Democracia brasileira, por intermédio de seus perfis em redes sociais, notadamente do Twitter (<https://twitter.com/AdvogadosOacb?lang=en&t=9WfNCjBadeB7etQoLoXv3A>) e Instagram (https://www.instagram.com/oacb_advogados_conservadores/)”*, nos quais conta com aproximadamente 100 (cem) mil seguidores. A narrativa do requerente vem acompanhada de postagens feitas pela Requerida, tais como *tweets* e vídeo, com os seguintes dizeres:

“Bolsonaro será o Presidente da República de 2023 a 2026 – Entenda!!!” – vídeo, em 28/12/2022;

“Deve-se continuar povoando Brasília e frentes dos quartéis exigindo resposta que Ministro da Defesa anterior não teve: a entrega das informações (os códigos fonte?), que TSE até agora não atendeu. Prevaricação é crime! Atente-se para o parágrafo único do art. 1 ° da Constituição.” - tweet, em 6/1/2023;

“Não se enganem: os que se denominam ‘juristas, ou advogados pela democracia’ mas apoiam este governo, nada têm de democráticos. São iguais àqueles. Lamentavelmente, mas esta é a verdade.” - tweet, em 6/1/2023;

123
S

PET 10981 / DF

"O STF NUNCA PODE SER A ÚLTIMA PALAVRA POIS SE TORNA DITADOR, uma vez que não é eleito pelo povo. Floriano Peixoto prendeu 13 oficiais generais. Rui Barbosa impetrou Habeas-corpus no STF. Floriano fez a observação: 'e quem dará habeas-corpus ao Supremo?' (Livro Nasce a República)." - tweet, em 8/1/2023;

"Reiteramos nosso compromisso e a verdade e da mesma forma que o colega do vídeo, que não pertence aos nossos quadros, recebeu a informação de falecimento de manifestantes (com confirmação), também recebemos. Requeremos aos senhores @marcosdoval e @Biakicis que averiguem o fato." - tweet, em 10/1/2023;

"GILMAR MENDES disse que 'o Brasil viveu uma era de trevas no que diz respeito ao processo penal'. Não! Nos Governos Militares eram presos subversivos armados, guerrilheiros. Os militares não prendiam crianças e inocentes. Naquele tempo o cidadão de bem era respeitado e protegido" - tweet, em 15/1/2023;

"O Estado Brasileiro sofrerá sanções e processos indenizatórios destas vítimas de abuso de autoridade, e tortura a que estão sendo submetidos os INOCENTES. A conta será paga por todos, em razão da irresponsabilidade de agentes públicos de um governo de gente despreparada." - tweet, em 15/1/2023;

"Claro que foi a mais esdrúxula das narrativas. É de se pasmar que o Judiciário coloque na cadeia INOCENTES sob argumentos antijurídicos. A Constituição segue violada." - tweet, em 18/1/2023;

Ilustra, ainda, a narrativa do requerente, reportagem com os seguintes dizeres: "*Nomes influentes da base bolsonarista compartilham informações falsas da organização não governamental Ordem dos Advogados*

124
S**PET 10981 / DF**

Conservadores do Brasil (OACB) como se fossem da entidade geral dos advogados” e “Parlamentares atribuem à OAB informações falsas sobre os ataques em Brasília”, datada de 13/1/2023, veiculada por “Redação O Sul”, conforme se transcreve a seguir:

“Em meio à repercussão dos atos que culminaram na depredação das sedes dos Três Poderes em Brasília no último domingo (08), parlamentares e nomes influentes da base bolsonarista compartilham informações falsas da organização não governamental Ordem dos Advogados Conservadores do Brasil (OACB) como se fossem da Ordem dos Advogados do Brasil (OAB) - entidade máxima de representação e regulamentação da advocacia no país.

O movimento que induz internautas à desinformação foi iniciado pelo deputado federal eleito Gustavo Gayer (PL-GO) na última segunda-feira (09). Na ocasião, ele afirmou via Twitter que advogados da OAB teriam deixado a prisão provisória da Polícia Federal (PF) e estavam ‘chocados com o fato de terem crianças presas’. Na verdade, tratavam-se de profissionais da OACB.

A atitude foi repetida na tribuna da Câmara dos Deputados por Bia Kicis (PL-SE). Na ocasião, ela disseminou uma notícia falsa que, segundo ela, teria sido respaldada pela seção da Ordem dos Advogados do Brasil do Distrito Federal (OAB-DF). ‘Acabo de receber uma notícia de que uma senhora veio a óbito hoje nas dependências da Polícia Federal. Não foi nas dependências da Polícia Militar, não. Falo de uma senhora a quem foi negado comida e água e que depois de horas, e horas, e horas a fio sendo destratada e descuidada, veio a falecer’, afirmou Kicis na manhã de terça-feira (10) na tribuna.

Posteriormente, no Twitter, a parlamentar pediu desculpas pelo equívoco e informou que a confirmação era, na verdade, da OACB. O grupo ganhou notoriedade em 2021 quando ameaçou processar qualquer pessoa que fizesse injúrias contra o então presidente Jair Bolsonaro (PL). À época, a OAB entrou na justiça contra a OACB por tentativa de uso indevido do

PET 10981 / DF

nome da Ordem e infração disciplinar.

Também na terça-feira, o deputado federal eleito com mais votos no Ceará, André Fernandes, publicou a fake news da morte da idosa no ginásio da PF com o aval da OACB. 'Crianças presas, idosos infartando, uma morte de uma senhora detida na PF confirmada pela OACB. Falta de água, comida e sanitários. Os vídeos que estão circulando são revoltantes', disse.

Desde domingo, a organização não governamental se colocou à disposição dos manifestantes presos: advogados associados prestam serviço sem cobrar honorários. Nas redes sociais, a OACB também divulga notícias falsas como a narrativa de que os atos de vandalismo de domingo teriam sido realizados por infiltrados. 'Não toleraremos atos de violência e baderna. Por outro lado, não abandonaremos quem não cometeu nenhum delito. A Ordem dos Advogados Conservadores do Brasil - OACB está em Brasília e dará assistência gratuita a todos o Paraibanos', escreveu." (<https://www.osul.com.br/parlamentares-oab-informacoes-falsas-ataques/>)

Em comprovação ao fato noticiado e acima individualizado, o Requerente apresenta as seguintes postagens dos Deputados Federais ANDRÉ JANONES e BIA KICIS, na rede social Twitter, ambas datadas de 11/1/2023:

"A deputada bolsonarista Bia Kicis investigada no inquérito das fake news, usou a tribuna da câmara para MENTIR. Bia Kicis em seu discurso afirmou que o presidente da OAB confirmou a morte de uma senhora sob custódia da PF e essa mentira tem sido usada para incitar os golpistas" - Dep. Fed. André Janones;

"Seu irresponsável! Irei levá-lo ao conselho ética. Não usei da tribuna p/mentir. Disse q a morte não fora confirmada. Qd descí da Tribuna, avisei q recebi um post da OAB(já esclareci ser a OACB)q confirmava a morte, depois desmentida pela PF.

PET 10981 / DF

Oficiei a PF pedindo informações." - Dep. Fed. Bia Kicis.

Prossegue o requerente afirmando que *"as postagens colacionadas desbordam do simples exercício da livre manifestação do pensamento e representam verdadeira ameaça ao Estado Democrático de Direito"* e que *"a repercussão decorrente do compartilhamento de informações falsas como se fossem da OAB - entidade máxima de representação e regulamentação da advocacia no país - confirma a desordem causada pela OACB, ao desvirtuar a finalidade da OAB, que é a de defender a Constituição, a ordem jurídica do Estado democrático de direito, os direitos humanos, a justiça social, e pugnar pela boa aplicação das leis, pela rápida administração da justiça e pelo aperfeiçoamento da cultura e das instituições jurídicas, consoante o art. 44, I, da Lei Federal n. 8.906/1994"*.

Informa o requerente que notificou a referida associação por intermédio do Ofício n. 26/2023 para que fizesse cessar a atuação irregular de seus advogados voluntários em audiências de custódia, em favor de custodiados em decorrência dos atos antidemocráticos do dia 8/1/2023, sem prova da outorga de mandato, mas, não obstante a confirmação do recebimento da notificação pelo representante da entidade, *"publicações recentes em seus perfis em redes sociais (<https://twitter.com/AdvogadosOacb>) dão conta da continuidade da atuação supostamente 'pro bono' (...) com advertência de que advogados poderiam estar se valendo da condição de 'voluntários' associados à 'OACB' mas, ao mesmo tempo, pedindo pagamento de contraprestação pecuniária para defesa (<https://twitter.com/AdvogadosOacb/status/1616156133844193283>), o que seria, entesse, repudiado pela associação"*.

Na segunda petição, o requerente pugnou pela juntada da *"contranotificação extrajudicial"*, subscrita pelos representantes da Requerida e endereçada, a um só tempo, ao Presidente do Conselho Seccional/DF da Ordem dos Advogados do Brasil e ao Presidente do Conselho Federal da OAB, da qual destaca os seguintes excertos, que entende virem em reforço à argumentação já expendida:

"há queixas dos presos de suposta sugestão velada os

PET 10981 / DF

induzindo a confessarem crimes e a fazerem acordos que supostamente contribuirá para se 'livrarem do cárcere';

"além proibição aos juízes de concederem qualquer ordem de soltura e relaxamento de prisões, até aquele momento sequer foi individualizada a tipificação penal com base em provas";

"as vítimas do autoritarismo do Estado Brasileiro estão sendo torturadas física e psicologicamente em presídios desta Cidade";

"este processo tem tantas contaminações que o INVALIDAM DE PLANO";

"se cunhou, falaciosamente, termos como 'terroristas' e 'golpistas', indistintamente, atingindo a população compostas de cidadãos de bem e até famílias inteiras ali presentes, sem individualizar as imputações e as mantendo presas, sem entrarmos, agora, em questões meritórias";

"DENUNCIAMOS à Vossa Excelência o que vem ocorrendo, *ab initio*, dentro das instalações de prédios do Estado Brasileiro (por ações e omissões), GRAVÍSSIMA VIOLAÇÃO A DIREITOS HUMANOS resultante das queixas dos cidadãos, que denotam os CRIMES DE TORTURA (física e psicológica), MAUS TRATOS, SUPRESSÃO DE LOCOMOÇÃO E DE EXPRESSÃO, atingindo majoritariamente cidadãos inocentes";

"Deparamo-nos perplexos com decisões baseadas em invencionismos judiciais, criando artificiais jurídicos e processuais ao arrepio da lei para servir À vontade de perseguir e punir desafetos. Se há alguém praticando 'atos antidemocráticos' são os agentes dos Estado";

"A NOSSA CLASSE está sufocada face o desequilíbrio do

PET 10981 / DF

'tripé da Justiça', não com a espada massacrando a sociedade brasileira com uma superioridade não prevista no ordenamento jurídico. Esse manuseio enviesado da Carta Magna e da legislação infraconstitucional ocorre com elevado grau de autoritarismo, arrogância e prepotência, sem respeito ao devido processo legal e à tripartição dos Poderes, bem como ao POVO, real titular do Poder";

"A maioria esmagadora são cidadãos de bem (já que desconsideramos os infiltrados), famílias, senhoras, senhores, idosos, trabalhadores, com endereço fixo e documentados, foram presos no dia 08/01/2023, de forma arbitrária e INCONSTITUCIONAL, e assim permanecem, ilegalmente, em condições desumanas, sem que tenham cometido crime";

"ficou evidenciado que houve vandalismo orquestrado, financiado por grupos simpáticos ao atual Governo e, quem sabe, até com conivência de autoridades, conforme relatou a inteligência brasileira. Isso teve o propósito de incitar a destruição e jogar a culpa nos manifestantes de mote patriótico, esmagadoramente pessoas ordeiras, legitimamente inconformadas com a falta de transparência do sistema eleitoral, o que é lícito e se deve repudiar qualquer manifestação que intencione lhes imputar a pecha de 'GOLPISTAS' (famílias com crianças, idosos, cadeirantes e desarmadas darão que golpe Presidente??? sequer pedir intervenção militar pode colocar tais pessoas como golpistas porque há previsão constitucional - e uma coisa é pedir, outra coisa é ser atendido!!!). A ação orquestrada por vândalos não nasceu da reunião dos manifestantes, mas tão somente para gerar a narrativa e justificativa ao avanço autoritário dos já contumazes abusadores de autoridade, sob o pretexto leviano de 'ação contra o terrorismo'. Tremenda balela!".

Pontua o Requerente que devem ser reprimidos a promoção de notícias falsas em agressão ao Estado Democrático de Direito e de

PET 10981 / DF

desinformação "às centenas de milhares de seguidores" e, sobretudo, o "ataque mesquinho e midiático à independência e harmonia dos Poderes da União".

Exemplifica a conduta a ser reprimida, ressaltando as ilações feitas pela Requerida acerca de "suposta constitucionalidade de um movimento a favor supressão de direitos democráticos, além da recorrente tese conspiracionista de um movimento 'infiltrado' para incriminar 'cidadãos de bem' e dos questionamentos sempre lançados ao sistema eleitoral brasileiro". Ressalta que a Requerida assevera haver "reiteração de denúncias de graves violações a direitos humanos perpetrados pelo Estado brasileiro e sobre o qual a OAB seria omissa", sem apresentação de qualquer documento probatório, sem individualização dos nomes daqueles que supostamente teriam sido induzidos a confessar crimes e celebrar acordos, tampouco daqueles que supostamente foram torturados (física e psicologicamente), sofreram maus-tratos ou tiveram a liberdade de locomoção suprimida fora das hipóteses previstas na Constituição e na lei penal.

Formula, ao final, os seguintes requerimentos:

"a) A imediata SUSPENSÃO DAS ATIVIDADES JURÍDICAS EXERCIDAS PELA 'representada', isto é, que OACB se abstenha de prestar/oferecer serviços jurídicos;

b) que a 'representada' se abstenha imediatamente de utilizar a imitação da sigla e do nome da Ordem dos Advogados do Brasil para quaisquer fins, especialmente que DEIXE DE USAR A SIGLA E O NOME DA OAB PARA DISSEMINAR FAKE NEWS CONTRA A DEMOCRACIA;

c) que a 'representada' deixe de captar/agenciar causas/clientes para advogados, especialmente em favor dos integrantes de seus quadros associativos;

d) que a 'representada' se abstenha de perpetrar ofensas e depreciar a imagem da Ordem dos Advogados do Brasil e de seus membros;

e) que a 'representada' seja impedida de promover censura, cerceamento à livre manifestação de pensamento, à liberdade de comunicação e de informação por intermédio do

PET 10981 / DF

ajuizamento de ações judiciais; e

f) que a 'representada' se abstenha de praticar toda e qualquer publicidade de prestação/oferecimento de serviços jurídicos".

Intimada para se manifestar, a Procuradoria-Geral da República requereu "o arquivamento dos autos em epígrafe, sem prejuízo da continuidade da ação civil pública em trâmite no 1º grau de jurisdição federal e de eventuais medidas de iniciativa do Conselho Federal da Ordem dos Advogados do Brasil" (fl. 121).

É o relatório. DECIDO.

Os fatos narrados nas representações do Conselho Federal da Ordem dos Advogados do Brasil, tal como relatados, guardam pertinência com aqueles objeto de investigação iniciada por decisão nestes autos e remetida ao Inq. 4.923/DF.

As condutas noticiadas da Ordem dos Advogados Conservadores do Brasil ocorreram no contexto dos atos antidemocráticos, nos quais grupos – financiados por empresários – insatisfeitos com o legítimo resultado do pleito, com violência e grave ameaça às pessoas, passaram a bloquear o tráfego em diversas rodovias do país, com o intuito de abolirem o Estado Democrático de Direito, pleiteando um "golpe militar" e o retorno da Ditadura, resultando nos atos terroristas ocorridos na Esplanada dos Ministérios em 8/1/2023, com destruição dos prédios do CONGRESSO NACIONAL, do PALÁCIO DO PLANALTO e, com muito mais raiva e ódio, do SUPREMO TRIBUNAL FEDERAL, fatos amplamente investigados em diversos procedimentos que tramitam nesta SUPREMA CORTE.

Efetivamente, as inúmeras manifestações da "Ordem dos Advogados Conservadores do Brasil", em análise preliminar, se revestem de caráter instigador dos atos ocorridos em 8/1/2023, o que pode configurar os crimes de previstos nos arts. 2ª, 3ª, 5ª e 6ª (atos terroristas, inclusive preparatórios) da Lei 13.260/16 e nos arts. 147 (ameaça), 147-A, § 1º, inciso III, (perseguição), 163 (dano), art. 286 (incitação ao crime), art.

PET 10981 / DF

250, § 1º, inciso I, alínea "b" (incêndio majorado), 288, parágrafo único (associação criminosa armada), 359-L (abolição violenta do Estado Democrático de Direito), 359-M (golpe de Estado), todos do Código Penal:

Lei n. 13.260/2016**Terrorismo**

Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

§ 1º São atos de terrorismo:

I - usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;

IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;

V - atentar contra a vida ou a integridade física de pessoa:

Pena - reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.

§ 2º O disposto neste artigo não se aplica à conduta individual ou coletiva de pessoas em manifestações políticas, movimentos sociais, sindicais, religiosos, de classe ou de categoria profissional, direcionados por propósitos sociais ou

PET 10981 / DF

reivindicatórios, visando a contestar, criticar, protestar ou apoiar, com o objetivo de defender direitos, garantias e liberdades constitucionais, sem prejuízo da tipificação penal contida em lei.

Art. 3º Promover, constituir, integrar ou prestar auxílio, pessoalmente ou por interposta pessoa, a organização terrorista.

Pena - reclusão, de cinco a oito anos, e multa.

Art. 5º Realizar atos preparatórios de terrorismo com o propósito inequívoco de consumar tal delito:

Pena - a correspondente ao delito consumado, diminuída de um quarto até a metade.

§ 1º Incorre nas mesmas penas o agente que, com o propósito de praticar atos de terrorismo:

I - recrutar, organizar, transportar ou municiar indivíduos que viajem para país distinto daquele de sua residência ou nacionalidade; ou

II - fornecer ou receber treinamento em país distinto daquele de sua residência ou nacionalidade.

§ 2º Nas hipóteses do § 1º, quando a conduta não envolver treinamento ou viagem para país distinto daquele de sua residência ou nacionalidade, a pena será a correspondente ao delito consumado, diminuída de metade a dois terços.

Art. 6º Receber, prover, oferecer, obter, guardar, manter em depósito, solicitar, investir, de qualquer modo, direta ou indiretamente, recursos, ativos, bens, direitos, valores ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução dos crimes previstos nesta Lei:

Pena - reclusão, de quinze a trinta anos.

Parágrafo único. Incorre na mesma pena quem oferecer ou receber, obtiver, guardar, mantiver em depósito, solicitar, investir ou de qualquer modo contribuir para a obtenção de ativo, bem ou recurso financeiro, com a finalidade de financiar, total ou parcialmente, pessoa, grupo de pessoas, associação, entidade, organização criminosa que tenha como atividade principal ou secundária, mesmo em caráter eventual, a prática dos crimes previstos nesta Lei.

PET 10981 / DF

Ameaça

Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

Pena - detenção, de um a seis meses, ou multa

Parágrafo único - Somente se procede mediante representação.

Perseguição

Art. 147-A Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

Dano

Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:

Pena - detenção, de um a seis meses, ou multa.

Dano qualificado

Parágrafo único - Se o crime é cometido:

I - com violência à pessoa ou grave ameaça;

II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave;

III - contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos;

IV - por motivo egoístico ou com prejuízo considerável para a vítima:

Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Incêndio

PET 10981 / DF

Art. 250 – Causar incêndio, expondo a perigo a vida, a integridade física ou o patrimônio de outrem:

Pena – reclusão de três a seis anos, e multa.

Aumento de pena

§ 1º – As penas aumentam-se de um terço:

I – se o crime é cometido com o intuito de obter vantagem pecuniária em proveito próprio ou alheio:

b) em edifício público ou destinado ao uso público ou a obra de assistência social ou de cultura

Incitação do crime

Art. 286 – Incitar, publicamente, a prática de crime:

Pena – detenção, de três a seis meses, ou multa.

Parágrafo único. Incorre na mesma pena quem incita, publicamente, animosidade entre as Forças Armadas, ou delas contra os poderes constitucionais, as instituições civis ou a sociedade.

Associação Criminosa

Art. 288. Associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes:

Pena - reclusão, de 1 (um) a 3 (três) anos.

Parágrafo único. A pena aumenta-se até a metade se a associação é armada ou se houver a participação de criança ou adolescente.

Abolição violenta do Estado Democrático de Direito

Art. 359-L. Tentar, com emprego de violência ou grave ameaça, abolir o Estado Democrático de Direito, impedindo ou restringindo o exercício dos poderes constitucionais:

Pena - reclusão, de 4 (quatro) a 8 (oito) anos, além da pena correspondente à violência.

Golpe de Estado

Art. 359-M. Tentar depor, por meio de violência ou grave ameaça, o governo legitimamente constituído:

135
8

PET 10981 / DF

Pena - reclusão, de 4 (quatro) a 12 (doze) anos, além da pena correspondente à violência.

Lei n. 9.605/1998

Art. 62. Destruir, inutilizar ou deteriorar:

I - bem especialmente protegido por lei, ato administrativo ou decisão judicial;

II - arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar protegido por lei, ato administrativo ou decisão judicial:

Pena - reclusão, de um a três anos, e multa.

Parágrafo único. Se o crime for culposo, a pena é de seis meses a um ano de detenção, sem prejuízo da multa.

Art. 65. Pichar ou por outro meio conspurcar edificação ou monumento urbano:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Se o ato for realizado em monumento ou coisa tombada em virtude do seu valor artístico, arqueológico ou histórico, a pena é de 6 (seis) meses a 1 (um) ano de detenção e multa.

Há, portanto, comprovação bastante nos autos para deferir, parcial e cautelarmente, os requerimentos formulados pelo Requerente Conselho Federal da Ordem dos Advogados do Brasil, nos termos da Lei n. 8.906/94 (em especial, art. 1º, I e II, art. 3º, art. 4º, parágrafo único, art. 15, art. 16, § 1º, § 2º, § 3º e § 4º, art. 34, IV e XVII, art. 44, I, II e § 2º, art. 54, I, II, e III), do Decreto-Lei n. 3.688/41 (art. 47), da Lei n. 9.279/96 (art. 124, V, XIX, XXIII, e art. 189, I e II), do Código Civil (arts. 50, § 1º, e 53), do Regulamento Geral da OAB (arts. 4º e 27, § 2º), do Código de Ética e Disciplina da OAB (arts. 5º, 7º, 31, 39 e 47) e do Provimento n. 94/2000 do Conselho Federal da OAB.

Em face das circunstâncias delineadas, imprescindível a realização de diligências, inclusive com o afastamento excepcional de garantias individuais que não podem ser utilizadas como um verdadeiro escudo

136
S

PET 10981 / DF

protetivo para a prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito (HC nº 70.814-5/SP, Rel. Min. CELSO DE MELLO, Primeira Turma, DJ de 24/6/1994).

Assim, torna-se necessário, adequado e urgente a suspensão das atividades jurídicas exercidas pela Ordem dos Advogados Conservadores do Brasil, bem como o bloqueio de suas redes sociais, utilizadas para atacar o Estado Democrático de Direito, diante da possibilidade de sua utilização para o incentivo de atos ilícitos e antidemocráticos, com objetivo de interromper a lesão ou ameaça a direito (art. 5º, XXXV, Constituição Federal).

Diante de todo o exposto, **DETERMINO** a adoção das seguintes providências, sob pena de multa diária de R\$ 20.000,00 (vinte mil reais), mediante intimação pessoal de **GERALDO JOSÉ BARRAL LIMA** (OAB/PB 18.014-A), Presidente da Ordem dos Advogados Conservadores do Brasil:

1) A **IMEDIATA SUSPENSÃO** das atividades jurídicas exercidas pela Ordem dos Advogados Conservadores do Brasil, devendo a associação se abster de prestar/oferecer serviços jurídicos e de praticar toda e qualquer publicidade de prestação/oferecimento de serviços jurídicos;

2) A **PROIBIÇÃO DE UTILIZAÇÃO** da imitação da sigla e do nome da Ordem dos Advogados do Brasil para quaisquer fins, especialmente para disseminar *fake news* contra o Estado Democrático de Direito e contra as suas Instituições;

3) A **PROIBIÇÃO DE ATUAÇÃO** da Ordem dos Advogados Conservadores do Brasil no sentido captar/agenciar causas/clientes para quaisquer advogados, especialmente em favor dos integrantes de seus quadros associativos; e

137
S

PET 10981 / DF

4) A PROIBIÇÃO da Ordem dos Advogados Conservadores do Brasil perpetrar ofensas e depreciar a imagem da Ordem dos Advogados do Brasil e de seus membro

APÓS A AUTUAÇÃO, DETERMINO SEJAM OS AUTOS ENCAMINHADOS À POLÍCIA FEDERAL para que, no prazo de 15 (quinze) dias, proceda à oitiva das pessoas abaixo nominadas, bem como para adoção de todas as medidas cabíveis para apuração dos fatos, salvo aquelas submetidas à cláusula de reserva jurisdicional:

(a) GERALDO JOSÉ BARRAL LIMA (Presidente da requerida – OAB/PB 18.014-A);

(b) JOÃO ALBERTO DA CUNHA FILHO (Vice-Presidente da Requerida – OAB/PB 10.705);

(c) SARA PATRÍCIA RIBEIRO FARIAS (Diretora-Secretária da Requerida – OAB/RR 1.008),

(d) MAILSON LIMA MACIEL (Diretor-Financeiro da Requerida – OAB/PB 10.732),

(e) RAQUEL DIAS MAGALHÃES DE BARROS LEAL (Diretora-Regional da Requerida – OAB/CE. 22.808-B),

(f) PATRÍCIA MUNHOZ E SILVA (Diretora-Relações Externas da Requerida – OAB/PR. 50.893) e

(g) FREDERICO AUGUSTO ANDRADE VIEGAS (Diretor-Relações Internas da Requerida – OAB/RJ 167.448).

DETERMINO, POR FIM:

(1) A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS TWITTER e FACEBOOK, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, bem como de quaisquer grupos que sejam administrados pelos usuários abaixo identificados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

138
g

PET 10981 / DF

FACEBOOK

<https://www.facebook.com/OACB.ORG.BR>

<https://www.facebook.com/ordem.adv.conservadores>

/

GETTR

https://gettr.com/user/oacb_org_br

INSTAGRAM

https://www.instagram.com/oacb_advogados_conservadores/

LINKEDIN

<https://www.linkedin.com/in/oacbadvogadosconservadores>

TWITTER

<https://twitter.com/AdvogadosOacb>

YOUTUBE

<https://www.youtube.com/c/OACBBrasil>

(2) A EXPEDIÇÃO DE OFÍCIO à ANATEL para que proceda à retirada específica do site <https://www.oacb.org.br/> de funcionamento no território nacional.

À Secretaria, para as necessárias providências.

Ciência à Procuradoria-Geral da República.

Intime-se o Conselho Federal da Ordem dos Advogados do Brasil, com cópia da presente decisão.

Brasília, 28 de fevereiro de 2023.

Ministro ALEXANDRE DE MORAES

Relator

Documento assinado digitalmente



PETITION 9.935 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, December 14, 2023.

To TWITTER INC.

Ref: Petition 9.935

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of all the above, I DETERMINE, in a complementary and integrative manner in relation to the decisions of 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/202, 22/9/2023, 27/9/2023 and 20/10/2012, the subpoena of the companies TWITTER, META, TELEGRAM, RUMBLE and LOCALS, so that, within 2 (two) hours, they block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

TWITTER

<https://twitter.com/NsmNews>

<https://twitter.com/canedocando>

PET 9935 / DF

I ORDER TO REFERRED COMPANIES, furthermore a immediate suspension of the transfer of amounts from monetization, services used for donations, payment for advertising and registration of supporters, and monetization from *lives*, including those made by providing transmission keys to the channels/profiles mentioned above, informing this SUPREME COURT of all transfers made up to the date of receipt of the court order.

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

Copy for TWITTER INC



PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 14 de dezembro de 2023.

À empresa
TWITTER INC.

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação às decisões de 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/202, 22/9/2023, 27/9/2023 e 20/10/2012, a intimação das empresas TWITTER, META, TELEGRAM, RUMBLE e LOCALS, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/NsmNews>

<https://twitter.com/canedocando>

PET 9935 / DF

DETERMINO ÀS REFERIDAS EMPRESAS, ainda, a suspensão imediata do repasse de valores oriundos de monetização, dos serviços usados para doações, do pagamento de publicidades e da inscrição de apoiadores, e advindos de monetização oriunda de *lives*, inclusive as realizadas por meio de fornecimento de chaves de transmissão aos canais/perfis acima referidos, informando a esta SUPREMA CORTE todos os repasses efetuados até a data do recebimento da ordem judicial.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETITION 10.975 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
REQUEST(S) : UNDER SEAL
PROSECUTOR(A/S)(ES) : UNDER SEAL
APPLICANT : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, June 15, 2023.

To the companies
META INC.
GETTR
LINKEDN
TIK TOK
TELEGRAM
TWITTER
YOUTUBE

Ref: Petition 10.975

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, pursuant to Article 21 of the STF's Rules of Procedure, I AUTHORIZE:

(4) THE ISSUANCE OF AN ORDER to the companies FACEBOOK, INSTAGRAM, GETTR, LINKEDN, TIK TOK, TELEGRAM, TWITTER and YOUTUBE so that, at the latest, they may within 02 (two) hours, block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their

PET 10975 / DF

FACEBOOK

<https://www.facebook.com/marcosdoval>

INSTAGRAM

<https://www.instagram.com/marcosdoval/>

GETTR

<https://gettr.com/user/marcosdoval>

LINKEDIN

<https://www.linkedin.com/in/marcos-do-val-258b8822/>

TIK TOK

<https://www.tiktok.com/@marcosdoval.fc>

TELEGRAM

<https://web.telegram.org/k/#@marcosdovalchannel>

TWITTER

<https://twitter.com/marcosdoval>

YOUTUBE

<https://www.youtube.com/@marcosdoval>

(4.1) The companies must inform, within 24 (twenty-four) hours, the existence of any sponsors of the respective channels/profiles/accounts, as well as the existence of the transfer of amounts derived from monetization, indicating individually the gains made in each of the channels/profiles/accounts indicated.

In view of the confidential nature of these proceedings, the following steps should be taken .

PETIÇÃO 10.975 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
PROC.(A/S)(ES) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 15 de junho de 2023.

Às empresas
META INC.
GETTR
LINKEDN
TIK TOK
TELEGRAM
TWITTER
YOUTUBE

Ref: Petição 10.975

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, nos termos do art. 21 do Regimento Interno do STF, AUTORIZO:

(4) A EXPEDIÇÃO DE OFÍCIO às empresas FACEBOOK, INSTAGRAM, GETTR, LINKEDN, TIK TOK, TELEGRAM, TWITTER e YOUTUBE para que, no prazo de 02 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

PET 10975 / DF

FACEBOOK

<https://www.facebook.com/marcosdoval>

INSTAGRAM

<https://www.instagram.com/marcosdoval/>

GETTR

<https://gettr.com/user/marcosdoval>

LINKEDIN

<https://www.linkedin.com/in/marcos-do-val-258b8822/>

TIK TOK

<https://www.tiktok.com/@marcosdoval.fc>

TELEGRAM

<https://web.telegram.org/k/#@marcosdovalchan.net>

TWITTER

<https://twitter.com/marcosdoval>

YOUTUBE

<https://www.youtube.com/@marcosdoval>

(4.1) As empresas deverão informar, no prazo de 24 (vinte e quatro) horas, a existência de eventuais patrocinadores dos respectivos canais/perfis/contas, bem como a existência de repasse de valores advindos de monetização, indicando de forma individualizada os ganhos auferidos em cada um dos canais/perfis/contas indicados.

Diante do caráter sigiloso destes autos, deverão ser adotadas as

PET 10975 / DF

providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Cópia destinada às plataformas de mídias sociais

INQUIRY 4.923 FEDERAL DISTRICT

REPORTER	: MIN. ALEXANDRE DE MORAES
AUTHOR(S)(ES)	: FEDERAL PUBLIC MINISTRY
PROC.(A/S)(ES)	: ATTORNEY GENERAL OF THE REPUBLIC
INVEST.(A/S)	: IBANEIS ROCHA BARROS JÚNIOR
ATT.(A/S)	: CLEBER LOPES DE OLIVEIRA AND OTHERS
INVEST.(A/S)	: ANDERSON GUSTAVO TORRES
ATT.(A/S)	: EUMAR ROBERTO NOVACKI
INVEST.(A/S)	: FERNANDO DE SOUSA OLIVEIRA
ATT.(A/S)	: DANILO DAVID RIBEIRO AND OTHERS
INVEST.(A/S)	: FÁBIO AUGUSTO VIEIRA
ATT.(A/S)	: JOAO PAULO DE OLIVEIRA BOAVENTURA E OTHER
AUT. POL.	: FEDERAL POLICE DELEGATE

DECISION

In a decision handed down in these proceedings on January 8, 2023, due to the violent escalation of criminal acts that resulted in the invasion of the buildings of the PALÁCIO DO PLANALTO, the NATIONAL CONGRESS of the SUPREME FEDERAL COURT, with the depredation of public property, as widely reported by the national press, I ordered, among other measures, the dispatch of a letter to the companies Facebook, Tik Tok and Twitter, so that, within two (2) hours, they block the channels/profiles/accounts indicated, which instigated and disseminated the criminal acts investigated, under penalty of a daily fine of R\$ 100.000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content.

The Special Office for Combating Disinformation of the SUPERIOR ELECTORAL COURT informs that, through research on open social media data, it detected a publication made by the influencer and *podcaster* "Monark", on the digital platform Rumble, containing an interview with Federal Deputy FILIPE BARROS (PL-PR), in the wake of which false news is spread about the integrity of the

INQ 4923 / DF

electoral institutions (Letter AEED/GAB-SPR/GAB-PRES no. 2419/2023).

This is a brief report. DECIDED.

As I emphasized in the decision handed down on January 8, 2023, the despicable terrorist attacks on Democracy and Republican Institutions will be held accountable, as will the financiers, instigators and the former and current conniving and criminal public officials who continue in the illicit conduct of practicing anti-democratic acts. On January 8, 2023, as is widely known nationally and internationally, the violent escalation of criminal acts resulted in the invasion of the PALÁCIO DO PLANALTO, CONGRESSO NACIONAL and SUPREME FEDERAL COURT buildings, with the depredation of public property.

The role of the instigators of the acts, especially on social networks, is no less relevant, and it is clear that these media are an essential part of the criminal enterprise that resulted in the appalling acts witnessed on January 8, 2023, and the subsequent acts scheduled for the following days, which are the subject of decisions in these cases and in ADPF 519.

In this context, I have repeatedly emphasized that the Federal Constitution enshrines the binomial "FREEDOM and RESPONSIBILITY"; not irresponsibly allowing abuse in the exercise of a constitutionally enshrined right; not allowing the use of "freedom of expression" as a protective shield for the practice of hate speech, anti-democracy, threats, aggression, criminal offenses and all sorts of illegal activities.

Freedom of expression is not freedom for aggression!

Freedom of expression is not freedom to destroy democracy, institutions and the dignity and honor of others!

Freedom of expression is not freedom to propagate untruthful, aggressive, hateful speech and prejudiced!

INQ 4923 / DF

In view of the circumstances pointed out, it is essential to carry out investigations, including the exceptional removal of individual guarantees that cannot be used as a real protective shield for the practice of illegal activities, nor as an argument for removing or diminishing civil or criminal liability for criminal acts, under penalty of disrespecting a true Rule of Law (HC n° 70.814-5/SP, Rel. Min. CELSO DE MELLO, First Class, DJ of 24/6/1994).

Thus, as reported, the decision handed down on 8/1/2023 ordered the blocking of several profiles/channels owned by BRUNO AIUB MONTEIRO, known as "Monark", on the social networks Instagram (@monarkoficial), Rumble (<https://rumble.com/Monark>), Telegram (<https://t.me/monarktalks> and <https://t.me/monarkk>), Tik Tok (https://www.tiktok.com/@monarktalks_) Twitter (@monark) e Youtube (<https://www.youtube.com/@MonarkTalksCortesOficial>).

However, in a new channel created on the Rumble platform (<https://rumble.com/c/Monarkx>), which already has 287,000 followers, BRUNO MONTEIRO AIUB, as reported by AEED/TSE, once again spread fraudulent news about the actions of this SUPREME COURT and the SUPERIOR ELECTORAL COURT, in the following terms:

"Monark says: 'And it's not the guy who's going out there, fighting and putting up... because every time the Supreme Court makes a move like that, it spends political chips. That costs him. [...] So why is it (the Supreme Court) willing to pay this cost? Why is it willing to **guarantee non-transparency in the elections? We see the TSE censoring people, we see Alexandre de Moraes arresting people, you see a lot of things happening, and at the same time they prevent the ballot boxes from being transparent? You get suspicious, what kind of shenanigans are going on in those ballot boxes?**

INQ 4923 / DF

Why is that? Why doesn't our political system want to let the Brazilian people have more security? What is their interest? Manipulating the ballot box? Manipulating the elections? That's what I keep thinking..."

In addition, the AEED/TSE indicated the creation of several other profiles, in complete disregard of the decision previously handed down:

Twitter: <https://twitter.com/MonarkVoltou> (16,2 thousand followers)

Instagram: <https://www.instagram.com/monark.talks/> (101,000 followers)

Telegram: <https://t.me/monarktalks>

Discord: <https://discord.gg/8NKCauHf9>

Thus, it is necessary, appropriate and urgent to stop the possible spread of hate speech, subversion of order and encouragement to break institutional and democratic normality by blocking accounts on social networks, with the aim of stopping the injury or threat to the right (art. 5, XXXV, Federal Constitution), as previously pointed out.

In view of the above, I hereby DETERMINE that a letter be sent to DISCORD, META INC., RUMBLE, TELEGRAM and TWITTER, so that, at the earliest possible date, the following may be sent to them within 2 (two) hours, block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content: [add all the links indicated:

DISCORD

<https://discord.gg/8NKCauHf9>

META INC.

<https://www.instagram.com/monark.talks/>

INQ 4923 / DF

RUMBLE

<https://rumble.com/c/Monarkx>

TELEGRAM

<https://t.me/monarktalks>

TWITTER

<https://twitter.com/MonarkVoltou>

I ALSO ORDER THE IMPOSITION OF A PRECAUTIONARY MEASURE against BRUNO MONTEIRO AIUB, consisting of abstaining from publishing, promoting, replicating and sharing the fraudulent news (fake news) that is the subject of this decision, under penalty of a DAILY FINE OF R\$ 10,000.00 (ten thousand reais) in the event of non-compliance.

Attach Official Letter AEED/GAB-SPR/GAB-PRES no. 2419/2023 to the case file. Notify the police authority.

Inform the Attorney General's Office.

Publish.

Brasilia, June 13, 2023.

Minister **ALEXANDRE DE MORAES**

Rapporteur

Digitally signed document

INQUÉRITO 4.923 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES)	: MINISTÉRIO PÚBLICO FEDERAL
PROC.(A/S)(ES)	: PROCURADOR-GERAL DA REPÚBLICA
INVEST.(A/S)	: IBANEIS ROCHA BARROS JÚNIOR
ADV.(A/S)	: CLEBER LOPES DE OLIVEIRA E OUTRO(A/S)
INVEST.(A/S)	: ANDERSON GUSTAVO TORRES
ADV.(A/S)	: EUMAR ROBERTO NOVACKI
INVEST.(A/S)	: FERNANDO DE SOUSA OLIVEIRA
ADV.(A/S)	: DANILO DAVID RIBEIRO E OUTRO(A/S)
INVEST.(A/S)	: FÁBIO AUGUSTO VIEIRA
ADV.(A/S)	: JOAO PAULO DE OLIVEIRA BOAVENTURA E OUTRO(A/S)
AUT. POL.	: DELEGADO DE POLÍCIA FEDERAL

DECISÃO

Em decisão proferida nestes autos em 8/1/2023, em razão da escalada violenta dos atos criminosos resultou na invasão dos prédios do PALÁCIO DO PLANALTO, do CONGRESSO NACIONAL do SUPREMO TRIBUNAL FEDERAL, com depredação do patrimônio público, conforme amplamente noticiado pela imprensa nacional, determinei, entre outras medidas, a expedição de ofício às empresas Facebook, Tik Tok e Twitter, para que, no prazo de 2 (duas) horas, procedessem ao bloqueio dos canais/perfis/contas indicados, que instigaram e divulgaram os atos criminosos investigados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo.

A Assessoria Especial de Enfrentamento à Desinformação do TRIBUNAL SUPERIOR ELEITORAL informa que, mediante pesquisa em dados abertos de mídias sociais, detectou publicação realizada pelo influenciador e *podcaster* “Monark”, na plataforma digital Rumble, contendo entrevista com o Deputado Federal FILIPE BARROS (PL-PR), na esteira da qual são difundidas notícias falsas sobre a integridade das

INQ 4923 / DF

instituições eleitorais (Ofício AEED/GAB-SPR/GAB-PRES nº 2419/2023).

É o breve relato. DECIDO.

Conforme ressaltei por ocasião da decisão proferida em 8/1/2023, os desprezíveis ataques terroristas à Democracia e às Instituições Republicanas serão responsabilizados, assim como os financiadores, instigadores e os anteriores e atuais agentes públicos coniventes e criminosos, que continuam na ilícita conduta da prática de atos antidemocráticos. Na data de 8/1/2023, como é de amplo conhecimento nacional e internacional, a escalada violenta dos atos criminosos resultou na invasão dos prédios do PALÁCIO DO PLANALTO, do CONGRESSO NACIONAL e do SUPREMO TRIBUNAL FEDERAL, com depredação do patrimônio público.

O papel dos instigadores dos atos, especialmente nas redes sociais, não é circunstância de menor relevância, ficando claro que os referidos meios de comunicação são parte essencial da empreitada criminosa que resultou nos estarecedores atos testemunhados no dia 8/1/2023, e nos subsequentes atos programados para os dias seguintes, objeto de decisões nestes autos e na ADPF 519.

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio “LIBERDADE e RESPONSABILIDADE”; não permitindo de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da “liberdade de expressão” como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e

INQ 4923 / DF

preconceituosos!

Em face das circunstâncias apontadas, imprescindível a realização de diligências, inclusive com o afastamento excepcional de garantias individuais que não podem ser utilizadas como um verdadeiro escudo protetivo para a prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito (HC nº 70.814-5/SP, Rel. Min. CELSO DE MELLO, Primeira Turma, DJ de 24/6/1994).

Desse modo, conforme relatado, por meio da decisão proferida em 8/1/2023, foi determinado o bloqueio de diversos perfis/canais de titularidade de BRUNO AIUB MONTEIRO, conhecido como “Monark”, nas redes sociais Instagram (@monarkoficial), Rumble (<https://rumble.com/Monark>), Telegram (<https://t.me/monarktalks> e <https://t.me/monarkk>), Tik Tok (https://www.tiktok.com/@monarktalks_) Twitter (@monark) e Youtube (<https://www.youtube.com/@MonarkTalksCortesOficial>).

Entretanto, em novo canal criado na plataforma Rumble (<https://rumble.com/c/Monarkx>), que já conta com 287 mil seguidores, BRUNO MONTEIRO AIUB, conforme relatado pela AEED/TSE, voltou a divulgar notícias fraudulentas acerca da atuação desta SUPREMA CORTE e do TRIBUNAL SUPERIOR ELEITORAL, nos seguintes termos:

“Monark diz: ‘E não é o cara que tá indo lá, lutando e colocando... porque, toda vez que o Supremo faz um movimento desse, ele gasta fichas políticas. Isso tem um custo pra ele. [...] Então, porque ele (Supremo) está disposto a pagar este custo? **Por que ele (Supremo) está disposto a garantir uma não-transparência nas eleições? A gente vê o TSE censurando gente, a gente vê o Alexandre de Moraes prendendo pessoas, você vê um monte de coisa acontecendo, e ao mesmo tempo eles impedindo a transparência das urnas? Você fica desconfiado, que maracutaia está acontecendo nas urnas ali?**”

INQ 4923 / DF

Por quê? Por que o nosso sistema político não quer deixar o povo brasileiro ter mais segurança? Qual é o interesse? Manipular as urnas? Manipular as eleições? É isso que eu fico pensando...’”

Além disso, a AEED/TSE indicou a criação de diversos outros perfis, em completo desrespeito à decisão anteriormente proferida:

Twitter: <https://twitter.com/MonarkVoltou> (16,2 mil seguidores)

Instagram: <https://www.instagram.com/monark.talks/> (101 mil seguidores)

Telegram: <https://t.me/monarktalks>

Discord: <https://discord.gg/8NKCauHf9>

Assim, se torna necessária, adequada e urgente a interrupção de eventual propagação dos discursos com conteúdo de ódio, subversão da ordem e incentivo à quebra da normalidade institucional e democrática mediante bloqueio de contas em redes sociais, com objetivo de interromper a lesão ou ameaça a direito (art. 5º, XXXV, Constituição Federal), conforme anteriormente ressaltado.

Diante do exposto, DETERMINO a expedição de ofício às empresas DISCORD, META INC., RUMBLE, TELEGRAM e TWITTER, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo: [acrescentar todos os links indicados:

DISCORD

<https://discord.gg/8NKCauHf9>

META INC.

<https://www.instagram.com/monark.talks/>

INQ 4923 / DF

RUMBLE

<https://rumble.com/c/Monarkx>

TELEGRAM

<https://t.me/monarktalks>

TWITTER

<https://twitter.com/MonarkVoltou>

DETERMINO, AINDA, A IMPOSIÇÃO DE MEDIDA CAUTELAR em face de BRUNO MONTEIRO AIUB, consistente na abstenção de publicação, promoção, replicação e compartilhamento das notícias fraudulentas (*fake news*) objeto da presente decisão, sob pena de MULTA DIÁRIA DE R\$ 10.000,00 (dez mil reais) no caso de descumprimento.

Junte-se aos autos o Ofício AEED/GAB-SPR/GAB-PRES nº 2419/2023.

Comunique-se à autoridade policial.

Ciência à Procuradoria-Geral da República.

Publique-se.

Brasília, 13 de junho de 2023.

Ministro **ALEXANDRE DE MORAES**

Relator

Documento assinado digitalmente

PETITION 10.802 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, May 17, 2023.

To TWITTER DO BRASIL

Ref: Petition 10.802

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of all the above, I DETERMINE, in a complementary and integrative manner in relation to the decision of 30/12/2022 and 3/5/2023, the summoning of the social network TWITTER, so that, within 2 (two) hours, it proceeds to block the channel/profile/account detailed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of its registration data, identifying the user, to this SUPREME COURT and the full preservation of its content:

TWITTER

<https://twitter.com/OPFigueiredo>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

PETITION 10.802 FEDERAL DISTRICT
Minister ALEXANDRE DE MORAES



PETIÇÃO 10.802 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 17 de maio de 2023.

À empresa TWITTER DO BRASIL

Ref: Petição 10.802

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação à decisão de 30/12/2022 e 3/5/2023, a intimação das rede social TWITTER, para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminado, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário, a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/OPFigueiredo>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

PET 10802 / DF

Relator

documento assinado digitalmente

Cópia destinada ao Twitter do Brasil



PETITION 10.824 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 14, 2023.

To the
companies
FACEBOOK
TIK TOK
TWITTER
TELEGRAM
KWAI
YOUTUBE

Ref: Pet 10.824

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms.

I ALSO ORDER THE FOLLOWING MEASURES:

(IX) THE ISSUANCE OF AN ORDER to the company FACEBOOK, to block, within two (2) hours, the channels/ profiles/accounts listed below, as well as any groups managed by the users identified below, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

FACEBOOK

PET 10824 / DF

<https://www.facebook.com/RamiroCaminhoneiros>

INSTAGRAM

<https://www.instagram.com/ramirodoscaminhoneiros/>

TIK TOK

<https://vm.tiktok.com/ZMNqS1xm1/>

TWITTER

[https://twitter.com/RCaminhoneiros?
t=UVtD9gbXbA0QN0spCWuEZA&s=09](https://twitter.com/RCaminhoneiros?t=UVtD9gbXbA0QN0spCWuEZA&s=09)

TELEGRAM

<https://t.me/+Uu1dvBu0t345OTBh>

KWAI

<https://s.kwai.com/u/d6uCD-cp>

YOUTUBE

<https://youtube.com/c/RamirodosCaminhoneiros>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

PETIÇÃO 10.824 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 14 de janeiro de 2023.

Às empresas
FACEBOOK
TIK TOK
TWITTER
TELEGRAM
KWAI
YOUTUBE

Ref: Pet 10.824

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA, AS SEGUINTE MEDIDAS:

(IX) a EXPEDIÇÃO DE OFÍCIO à empresa FACEBOOK, para que, no prazo de 2 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, bem como de quaisquer grupos que sejam administrados pelos usuários abaixo identificados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

FACEBOOK

PET 10824 / DF

<https://www.facebook.com/RamiroCaminhoneiros>

INSTAGRAM

<https://www.instagram.com/ramirodoscaminhoneiros/>

TIK TOK

<https://vm.tiktok.com/ZMNqS1xm1/>

TWITTER

[https://twitter.com/RCaminhoneiros?
t=UVtD9gbXbA0QN0spCWuEZA&es=09](https://twitter.com/RCaminhoneiros?ref=twimg&source=09)

TELEGRAM

<https://t.me/+Uu1dvBuOf345OTBh>

KWAI

<https://s.kwai/u/d6uCD-cp>

YOUTUBE

<https://youtube.com/c/RamirodosCaminhoneiros>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETITION 10.464 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
REQUEST(S) : UNDER SEAL
ATT.(A/S) : UNDER SEAL

Brasilia, July 17, 2023.

To TWITTER DO BRASIL

Ref: Petition 10.464

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER that TWITTER be sent an official letter to block the channels/profiles/accounts listed below within two (2) hours, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

TWITTER

<https://twitter.com/ricardomartinpr>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

PETIÇÃO 10.464 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 17 de julho de 2023.

À empresa TWITTER DO BRASIL

Ref: Petição 10.464

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO a expedição de ofício à empresa TWITTER para que, no prazo de 02 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/ricardomartinpr>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETITION 11.022 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
REQUEST(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
APPLICANT : UNDER SEAL
APPLICANT : UNDER SEAL
APPLICANT : UNDER SEAL
APPLICANT : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, March 9, 2023.

To companies
FACEBOOK, TIK TOK and YOUTUBE

Ref: Pet 11.022

Directors,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

I ALSO ORDER THE FOLLOWING MEASURES:

(8) **THE ISSUANCE OF AN ORDER** to the companies FACEBOOK, INSTAGRAM, TWITTER and YOUTUBE to, within 2 (two) hours, block the channel/profile/account listed below, as well as any groups managed by the users identified below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

FACEBOOK:

<https://www.facebook.com/marlucia.ramiro.9>
<https://www.facebook.com/katia.graceli>



PET 11022 / DF

<https://www.facebook.com/profile.php?id=100085434710015>

INSTAGRAM:

<https://www.instagram.com/lucinharamiro/>
<https://www.instagram.com/katiagraceli/>

TWITTER:

<https://twitter.com/KatiaGraceli>
https://twitter.com/rossi_beto

YOUTUBE

<https://www.youtube.com/@katiagraceli4170>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

PETIÇÃO 11.022 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 9 de março de 2023.

Às empresas
FACEBOOK, TIK TOK e YOUTUBE

Ref: Pet 11.022

Senhores Diretores,

Comunico-lhes que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA, AS SEGUINTE MEDIDAS:

(8) a **EXPEDIÇÃO DE OFÍCIO** às empresas FACEBOOK, INSTAGRAM, TWITTER e YOUTUBE para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminados, bem como de quaisquer grupos que sejam administrados pelos usuários abaixo identificados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

FACEBOOK:

<https://www.facebook.com/marlucia.ramiro.9>

<https://www.facebook.com/katia.graceli>

PET 11022 / DF

<https://www.facebook.com/profile.php?id=100085434710015>

INSTAGRAM:

<https://www.instagram.com/lucinharamiro/>

<https://www.instagram.com/katiagraceli/>

TWITTER:

<https://twitter.com/KatiaGraceli>

https://twitter.com/rossi_beto

YOUTUBE

<https://www.youtube.com/@katiagraceli4170>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

Documento assinado digitalmente

INQUIRY 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S)(ES) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, October 27, 2023.

To TWITTER
INC

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER that TWITTER INC, within 2 (two) hours, block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of its registration data to identify the account holder to this SUPREME COURT, and the full preservation of its content:

TWITTER

<https://twitter.com/spaceliberdade/>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of esteem and consideration.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 27 de outubro de 2023.

À empresa
TWITTER INC

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO que a empresa TWITTER INC. no prazo de 2 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais para identificação do titular da conta a esta SUPREMA CORTE, e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/spaceliberdade/>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETITION 10.800 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, May 17, 2023.

To TWITTER DO BRASIL

Ref: Petition 10.800

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of all the above, I DETERMINE, in a complementary and integrative manner in relation to the decision of January 1, 2023 and May 10, 2023, the subpoena of the social networks META, PATREON, TWITTER, YOUTUBE, so that, within 2 (two) hours, proceed to block the channel/profile/account detailed below, under penalty of a daily fine of R\$ 100.000.00 (one hundred thousand reais), with the provision of its registration data, identifying the user, to this SUPREME COURT and the full preservation of its content:

TWITTER

<https://twitter.com/tudoconsta76>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

PET 10800 / DF

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy for Twitter Brazil



PETIÇÃO 10.800 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 17 de maio de 2023.

À empresa TWITTER DO BRASIL

Ref: Petição 10.800

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação à decisão de 1º/1/2023 e 10/05/2023, a intimação das redes sociais META, PATREON, TWITTER, YOUTUBE, para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminado, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário, a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/tudoconsta76>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

PET 10800 / DF

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada ao Twitter do Brasil

PETITION 11.075 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, March 31, 2023.

To companies

FACEBOOK, INSTAGRAM, TWITTER, YOUTUBE, TIKTOK
and TELEGRAM

Ref: Pet 11.075

Directors,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

I ALSO ORDER THE FOLLOWING MEASURES:

(8) ISSUANCE OF NOTICE to the companies FACEBOOK, INSTAGRAM, TWITTER, YOUTUBE, TIKTOK and TELEGRAM

to, within two (2) hours, block the channel/profile/account listed below, as well as any groups managed by the users identified below, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:



PET 11075 / DF

TWITTER:

@leandrOGustavo
@leandrofoxgoias
@leandrofoxgo
@realidadedopovo
@vasc07099161

FACEBOOK:

<https://www.facebook.com/Raphaelandreleite/>
[facebook.com/fernando.souza.realidade](https://www.facebook.com/fernando.souza.realidade)
[facebook.com/profile.php?id=100003873235282](https://www.facebook.com/profile.php?id=100003873235282)
[facebook.com/leandromunizgoias](https://www.facebook.com/leandromunizgoias)
[facebook.com/leandrofoxgoias](https://www.facebook.com/leandrofoxgoias)
<https://www.facebook.com/realidadedopovo/>
<https://www.facebook.com/jose.vasconcelosviana>
<https://www.facebook.com/agorafalei.jv/>

INSTAGRAM:

<https://www.instagram.com/tatilouren.seg/>
https://www.instagram.com/fernando_rdp/
@leandrofox
@leandrofoxgoias
<https://www.instagram.com/realidadedopovo>
<https://www.instagram.com/josevasconcelosviana/>

YOUTUBE:

@LeandroFoxgoias
@RealidadedoPovo
<https://www.youtube.com/@AgoraFalei>

TELEGRAM:

Group: Olive Green

TIKTOK:

@leandrofoxgoias

PET 11075 / DF

@realidadedopovo

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy for the Federal Police

PETIÇÃO 11.075 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
REQTE.(S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
REQDO.(A/S)	: SOB SIGILO
REQDO.(A/S)	: SOB SIGILO
REQDO.(A/S)	: SOB SIGILO
REQDO.(A/S)	: SOB SIGILO
REQDO.(A/S)	: SOB SIGILO
REQDO.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO

Brasília, 31 de março de 2023.

Às empresas
FACEBOOK, INSTAGRAM, TWITTER, YOUTUBE, TIKTOK e
TELEGRAM

Ref: Pet 11.075

Senhores Diretores,

Comunico-lhes que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA, AS SEGUINTE MEDIDAS:

(8) a EXPEDIÇÃO DE OFÍCIO às empresas FACEBOOK, INSTAGRAM, TWITTER, YOUTUBE, TIKTOK e TELEGRAM para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminados, bem como de quaisquer grupos que sejam administrados pelos usuários abaixo identificados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

PET 11075 / DF

TWITTER:

@leandrOGustavo
@leandrofoxgoias
@leandrofoxgo
@realidadedopovo
@vasc07099161

FACEBOOK:

<https://www.facebook.com/Raphaelandreite/>
[facebook.com/fernando.souza.realidade](https://www.facebook.com/fernando.souza.realidade)
[facebook.com/profile.php?id=100003873235282](https://www.facebook.com/profile.php?id=100003873235282)
[facebook.com/leandromunizgoias](https://www.facebook.com/leandromunizgoias)
[facebook.com/leandrofoxgoias](https://www.facebook.com/leandrofoxgoias)
<https://www.facebook.com/realidadedopovo/>
<https://www.facebook.com/jose.vasconcelosviana>
<https://www.facebook.com/agorafalei.jv/>

INSTAGRAM:

<https://www.instagram.com/tatilouren.seg/>
https://www.instagram.com/fernando_rdp/
@leandrofox
@leandrofoxgoias
<https://instagram.com/realidadedopovo>
<https://www.instagram.com/josevasconcelosviana/>

YOUTUBE:

@LeandroFoxgoias
@RealidadedoPovo
<https://www.youtube.com/@AgoraFalei>

TELEGRAM:

Grupo: Verde Oliva

TIKTOK:

@ leandrofoxgoias

PET 11075 / DF

@realidadedopovo

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETITION 9.935 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, February 8, 2024.

To TWITTER INC.

Ref: Petition 9.935

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of all the above, I DETERMINE, in a complementary and integrative manner in relation to the decisions of 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/202, 22/9/2023, 27/9/2023, 20/10/2012, 13/12/2023 and 15/1/2024, to order company X (TWITTER) to block the channel/profile/account listed below within 2 (two) hours, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of its registration data to this SUPREME COURT and the full preservation of its content:

X (TWITTER)

https://twitter.com/Ar_1News

https://twitter.com/ar_1news/status/1755616882361819575?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

Copy intended for Twitter/INC



PET 9935 / DF

I DETERMINE À REFERRED COMPANY,
furthermore a

Immediate suspension of the transfer of amounts █████
monetization, services used for donations, payment █████
advertising and registration of supporters, and monetization
from *lives*, including those made by providing transmission
keys to the channels/profiles mentioned above, informing this
SUPREME COURT of all transfers made up to the date of
receipt of the court order.

In view of the confidential nature of these proceedings, the necessary
steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions
of high esteem and consideration.

Justice ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy intended for Twitter INC

PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 8 de fevereiro de 2024.

À empresa
TWITTER INC.

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação às decisões de 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/202, 22/9/2023, 27/9/2023, 20/10/2012, 13/12/2023 e 15/1/2024, a intimação da empresa X (TWITTER) para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

X (TWITTER)

https://twitter.com/Ar_1News

https://twitter.com/ar_1news/status/1755616882361819575?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

PET 9935 / DF

DETERMINO À REFERIDA EMPRESA, ainda, a suspensão imediata do repasse de valores oriundos de monetização, dos serviços usados para doações, do pagamento de publicidades e da inscrição de apoiadores, e advindos de monetização oriunda de *lives*, inclusive as realizadas por meio de fornecimento de chaves de transmissão aos canais/perfis acima referidos, informando a esta SUPREMA CORTE todos os repasses efetuados até a data do recebimento da ordem judicial.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Inquiry 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, November 14, 2022.

To the company
TWITTER BRASIL

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER that a letter be sent to the companies FACEBOOK and TWITTER to block the channel/profile/group linked to the defendant and itemized below, within a maximum period of 2 (two) hours, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of its registration data to this SUPREME COURT and the full preservation of its content:

TWITTER

<https://twitter.com/carloscabarilbr1>

<https://twitter.com/DaviSacer>

<https://twitter.com/heytauat>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

INQ 4781 / DF

Airton Vieira

Teaching Magistrate in the Office of Justice

ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy sent to the Federal Police

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
AUTOR(A/S)(ES) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 14 de novembro de 2022.

À empresa
TWITTER DO BRASIL
Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento nos seguintes termos:

Diante do exposto, DETERMINO a expedição de ofício às empresas FACEBOOK e TWITTER, para que, no prazo de 02 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/carloscabralbr1>

<https://twitter.com/DaviSacer>

<https://twitter.com/heytauat>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

AIRTON VIEIRA

Magistrado Instrutor do Gabinete do
Ministro **ALEXANDRE DE MORAES**

INQ 4781 / DF

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETITION 10.800 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
REQUEST(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
APPLICANT : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 5, 2024.

To TWITTER BRASIL

Ref: Petition 10.800

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of all the above, I DETERMINE, in a complementary and integrative manner in relation to the decisions of 12/30/2022, 8/5/2023, 17/5/2023, the summoning of the social network Twitter, so that, within 2 (two) hours, it proceeds to block the channel/profile/account detailed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of its registration data, identifying the user to this SUPREME COURT and the full preservation of its content:

TWITTER

https://twitter.com/constajornalist/status/1742901482557444284?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I would like to take this opportunity to renew

PET 10800 / DF

my highest regards.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

Copy for TWITTER

PETIÇÃO 10.800 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 5 de janeiro de 2024.

À empresa TWITTER DO BRASIL

Ref: Petição 10.800

Senhor Diretor,

Comunicação que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação às decisões de 30/12/2022, 8/5/2023, 17/5/2023, a intimação da rede social Twitter, para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminado, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

https://twitter.com/constajornalist/status/1742901482557444284?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar

PET 10800 / DF

meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Cópia destinada ao TWITTER

INQUIRY 4.781 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, October 22, 2022.

To the company
TWITTER BRAZIL

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

I also DETERMINE:

(c) the dispatch of a letter to Twitter and Facebook, so that, within two (2) hours, they block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

Twitter

<https://twitter.com/crisbrasilreal>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 22 de outubro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, ainda:

(c) a expedição de ofício às empresas Twitter e Facebook, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

Twitter

<https://twitter.com/crisbrasilreal>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETITION 10.373 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, October 23, 2022.

To the company
TWITTER BRAZIL

Ref: Petition 10.373

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER THAT THE SOCIAL NETWORK Twitter, through its representative in the national territory, be summoned to block the channel/profile/group linked to the defendant and itemized below, **within a maximum period of 2 (two) hours, under penalty of a daily fine of RS 100,000.00 (one hundred thousand reais)**, with the provision of its registration data to this SUPREME COURT and the full preservation of its content:

TWITTER
https://twitter.com/danielsemperfi_

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

PET 10373 / DF

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy sent to the Federal Police

PETIÇÃO 10.373 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 23 de outubro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.373

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO A INTIMAÇÃO DA REDE SOCIAL Twitter, através de sua representante no território nacional, para que proceda ao bloqueio dos canal/perfil/grupo vinculado ao réu e abaixo discriminado, **no prazo máximo de 2 (duas horas), sob pena de multa diária de R\$ 100.000,00 (cem mil reais)**, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

https://twitter.com/danielsemperfi_

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

PET 10373 / DF

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETITION 10.625 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 12, 2024.

To TWITTER INC.

Ref: Petition 10.625

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, on the basis of Article 21 of the Internal Rules of the Supreme Federal Court, I ORDER that TWITTER be sent a letter to block the channel/profile/account listed below within two (2) hours, under penalty of a daily fine of one hundred thousand reais (R\$100,000.00), with the provision of its registration data, identifying the user, to this SUPREME COURT and the full preservation of its content:

TWITTER

<https://twitter.com/elisarobsondf>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

PET 10625 / DF

digitally signed document

Copy intended for Twitter INC



PETIÇÃO 10.625 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 12 de janeiro de 2024.

À empresa
TWITTER INC.

Ref: Petição 10.625

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, com fundamento no art. 21 do Regimento Interno do Supremo Tribunal Federal, DETERMINO a expedição de ofício à empresa TWITTER para que, no prazo de 02 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminado, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário, a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/elisarobsondf>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

PET 10625 / DF

documento assinado digitalmente

Cópia destinada ao Twitter INC



INQUIRY 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 2, 2023.

To companies

FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
TELEGRAM INC.
TWITTER BRAZIL
YOUTUBE BRAZIL

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

FINALLY:

(g) the dispatch of a letter to the companies FACEBOOK, TELEGRAM, TWITTER and YOUTUBE so that, within two (2) hours, they block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

FACEBOOK

<https://www.facebook.com/guilhermefiuzacanal>

INSTAGRAM

<https://www.instagram.com/guilhermefiuzaooficial/>

INQ 4781 / DF

TELEGRAM

<https://telegram.me/guilhermefiuzaooficial>

TWITTER

https://twitter.com/GFiuza_Oficial

YOUTUBE

<https://www.youtube.com/c/GuilhermeFiuzacanal>

(h) the dispatch of a letter to the companies FACEBOOK, TELEGRAM, TWITTER and YOUTUBE to inform them within 24 (twenty-four) hours of the existence of any sponsors of the respective channels/profiles/accounts, as well as the existence of the transfer of amounts arising from monetization, indicating individually the gains made in each of the channels/profiles/accounts mentioned in item "g".

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 2 de janeiro de 2023.

Às empresas
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
TELEGRAM INC.
TWITTER DO BRASIL
YOUTUBE BRASIL

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, por fim:

(g) a expedição de ofício às empresas FACEBOOK, TELEGRAM, TWITTER e YOUTUBE para que, no prazo de 02 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

FACEBOOK

<https://www.facebook.com/guilhermefiuzacanal>

INSTAGRAM

<https://www.instagram.com/guilhermefiuzaooficial/>

INQ 4781 / DF

TELEGRAM

<https://telegram.me/guilhermefiuzaoficial>

TWITTER

https://twitter.com/GFiuza_Oficial

YOUTUBE

<https://www.youtube.com/c/GuilhermeFiuza Canal>

(h) a expedição de ofício às empresas FACEBOOK, TELEGRAM, TWITTER e YOUTUBE para que informem no prazo de 24 (vinte e quatro) horas a existência de eventuais patrocinadores dos respectivos canais/perfis/contas, bem como a existência de repasse de valores advindos de monetização, indicando de forma individualizada os ganhos auferidos em cada um dos canais/perfis/contas apontadas no item “g”.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETITION 9.935 FEDERAL DISTRICT

RAPPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, September 23, 2022.

To the company
TWITTER BRAZIL

Ref: Petition 9.935

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, pursuant to Article 21 of the Rules of Procedure of the SUPREME FEDERAL COURT, I ORDER:

(2) The subpoena of social networks, through their representatives in the national territory to block the channels/ profiles/ groups linked to those investigated and listed below, within a maximum period of 24 (twenty-four) hours, with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

TWITTER

<https://twitter.com/ludmilagrilo>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I would like to take this opportunity to renew



PET 9935 / DF

my highest regards.

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

Copy for the Federal Police

PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 23 de setembro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, nos termos do art. 21 do Regimento Interno do SUPREMO TRIBUNAL FEDERAL, DETERMINO:

(2) A INTIMAÇÃO DAS REDES SOCIAIS, através de suas representantes no território nacional, para que procedam ao bloqueio dos canais/perfis/grupos vinculados aos investigados e abaixo discriminados, **no prazo máximo de 24 (vinte e quatro horas)**, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/ludmilagrilo>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar

PET 9935 / DF

meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

INQUIRY 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, November 7, 2023.

To TWITTER INC

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER that TWITTER INC., within 2 (two) hours, block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of its registration data to identify the account holder to this SUPREME COURT, and the full preservation of its content:

TWITTER

<https://twitter.com/MarceloRochaMon>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of esteem and consideration.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 7 de novembro de 2023.

À empresa
TWITTER INC

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO que a empresa TWITTER INC. no prazo de 2 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais para identificação do titular da conta a esta SUPREMA CORTE, e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/MarceloRochaMon>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETITION 10.685 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
DEFENDANT(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, December 10, 2022.

To the company
TWITTER BRAZIL

Ref: Petition 10.685

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the foregoing, I **ORDER THE FOLLOWING MEASURES:**

(VII) send a letter to the companies **FACEBOOK, GETTR, TELEGRAM, TIK TOK, TWITTER and YOUTUBE**, in order to within two (2) hours, to block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

TWITTER

https://mobile.twitter.com/luiz_pampolha
<https://mobile.twitter.com/Sunamit28948614>
<https://mobile.twitter.com/DraSirleiRatier>
<https://mobile.twitter.com/DaJacksuel>
<https://mobile.twitter.com/RenatoBezerraAL>
https://mobile.twitter.com/thiagohfs_tst
<https://mobile.twitter.com/Marcelo00683250>
<https://mobile.twitter.com/TaquesFonseca>

PET 10685 / DF

<https://mobile.twitter.com/MarceloKalin3>
<https://twitter.com/LuizAlbertoZan1>
<https://mobile.twitter.com/Marcelo29626370>
<https://mobile.twitter.com/Michaeldiniz357>
<https://mobile.twitter.com/ProMonarquia>
<https://mobile.twitter.com/ThiagooConde>
https://mobile.twitter.com/ricabral7/with_replies

<https://mobile.twitter.com/ricardocabrald7>
https://mobile.twitter.com/Washington_advo
<https://mobile.twitter.com/Rogério9054>
<https://mobile.twitter.com/SalesPatriota>
<https://twitter.com/jairocoelho164>
<https://twitter.com/MARCOSA54648009>
<https://twitter.com/TicianiRossi/likes>
<https://twitter.com/vargasezequiell>
https://twitter.com/deputado_Zucco
<https://twitter.com/doHeliomar>
<https://twitter.com/cmichels77>
<https://twitter.com/marcelo06838377>
<https://twitter.com/MrcioPereiraFe3>
<https://twitter.com/ClaudiomiroAra5/likes>
<https://twitter.com/leandrofoxgoias>
<https://twitter.com/FeijoKairo>
<https://twitter.com/IusakuSuzuki>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

In order, Airton Vieira Magistrate
Instructor of the Office of the
Minister **ALEXANDRE DE MORAES**

PETIÇÃO 10.685 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 10 de dezembro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.685

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, **DETERMINO AS SEGUINTE MEDIDAS:**

(VII) a expedição de ofício às empresas **FACEBOOK, GETTR, TELEGRAM, TIK TOK, TWITTER e YOUTUBE**, para que, no prazo de 02 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

https://mobile.twitter.com/luiz_pampolha

<https://mobile.twitter.com/Sunamit28948614>

<https://mobile.twitter.com/DraSirleiRatier>

<https://mobile.twitter.com/DaJacksuel>

<https://mobile.twitter.com/RenatoBezerraAL>

https://mobile.twitter.com/thiagohfs_tst

<https://mobile.twitter.com/Marcelo00683250>

<https://mobile.twitter.com/TaquesFonseca>

PET 10685 / DF

<https://mobile.twitter.com/MarceloKalinoss3>
<https://twitter.com/LuizAlbertoZan1>
<https://mobile.twitter.com/Marcelo29626370>
<https://mobile.twitter.com/Michaeldiniz357>
<https://mobile.twitter.com/ProMonarquia>
<https://mobile.twitter.com/ThiagooConde>
https://mobile.twitter.com/ricabral7/with_replies

s

<https://mobile.twitter.com/ricardocabrald7>
https://mobile.twitter.com/Washington_advoc
<https://mobile.twitter.com/Rogério9054>
<https://mobile.twitter.com/SalesPatriota>
<https://twitter.com/HernaniJoseAlv1>
<https://twitter.com/jairocoelho164>
<https://twitter.com/MARCOSA54648009>
https://twitter.com/Mws_will/
<https://twitter.com/TicianiRossi/likes>
<https://twitter.com/vargasezequiell>
https://twitter.com/deputado_Zucco
<https://twitter.com/doHeliomar>
<https://twitter.com/cmichels77>
<https://twitter.com/marcelo06838377>
<https://twitter.com/MrcioPereiraFe3>
<https://twitter.com/ClaudiomiroAra5/likes>
<https://twitter.com/leandrofoxgoias>
<https://twitter.com/FeijoKairo>
<https://twitter.com/IusakuSuzuki>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

De ordem, Airton Vieira
 Magistrado Instrutor do Gabinete do
 Ministro **ALEXANDRE DE MORAES**

PET 10685 / DF

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

INQUIRY 4.954 RIO DE JANEIRO

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ATTORNEY(S)(ES) : UNDER SEAL

Brasília, on the date
of

electronic signature.

To TWITTER
INC.

Ref: Inq 4.954

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential Inquiry, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER TWITTER INC. to block the channels/profiles/accounts listed below within 2 (two) hours, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), providing this SUPREME COURT with their registration data to identify the account holders, and fully preserving their content:

TWITTER

<https://twitter.com/marcio37>

https://twitter.com/enzo_nil/

<https://twitter.com/Hedilbe49136857>

<https://twitter.com/TerraBrasilnot>

<https://twitter.com/NeoStina>

<https://twitter.com/eloarcastelaci>

<https://twitter.com/RCNradiochatnet>

<https://twitter.com/PadraoAlexandre>

In view of the confidential nature of these proceedings, the following steps should be taken

INQ 4954 / RJ

necessary measures for its maintenance.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

Copy for TWITTER INC



INQUÉRITO 4.954 RIO DE JANEIRO

RELATOR : MIN. ALEXANDRE DE MORAES
 AUTOR(A/S)(ES) : SOB SIGILO
 PROC.(A/S)(ES) : SOB SIGILO

Brasília, na data da
 assinatura eletrônica.

À empresa
 TWITTER INC.

Ref: Inq 4.954

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO à empresa TWITTER INC. que, no prazo de 2 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais para identificação dos titulares das contas a esta SUPREMA CORTE, e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/marcio37>

https://twitter.com/enzo_nil/

<https://twitter.com/Hedilbe49136857>

<https://twitter.com/TerraBrasilnot>

<https://twitter.com/NeoStina>

<https://twitter.com/eloarcastelaci>

<https://twitter.com/RCNradiochatnet>

<https://twitter.com/PadraoAlexandre>

Diante do caráter sigiloso destes autos, deverão ser adotadas as

INQ 4954 / RJ

providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à empresa TWITTER INC



INQUIRY 4.879 FEDERAL DISTRICT

RAPPORTEUR : JUSTICE ALEXANDRE DE MORAES
AUTHOR(S) : UNDER SEAL
ATTORNEY(S)(ES) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
INVEST.(A/S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 11, 2023.

To companies

- FACEBOOK ONLINE SERVICES BRAZIL LTDA
- RUMBLE
- TELEGRAM
- TIK TOK
- TWITTER
- YOUTUBE

Ref: Inquiry 4.879



INQ 4879 / DF

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of the above, I ORDER that letters be sent to the companies FACEBOOK, RUMBLE, TELEGRAM, TIK TOK, TWITTER and YOUTUBE, to block the channels/profiles/accounts listed below within 2 (two) hours, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content: add all the links indicated:

FACEBOOK

<https://www.facebook.com/people/Patriotas/100068182532776/>
<https://www.facebook.com/nikolasferreiradm>
<https://www.facebook.com/search/top?q=jos%C3%A9%20medeiros>
<https://www.facebook.com/people/Barbara-Te-Updated/100086379919151/>
<https://www.facebook.com/alanrickm>

INSTAGRAM

@monarkoficial
 @patriotasb
 @nikolasferreiradm
 @josemedeirosmt
 @alanrickm
 @ana_lucia_bagueira
 @teatualizeioficial

RUMBLE

<https://rumble.com/Monark>

INQ 4879 / DF

TELEGRAM

t.me/patriotasb
<https://t.me/nikolasferreira>
<https://t.me/monarktalks>
<https://t.me/monarkk>
<https://t.me/profepaulamarisa>

TIK TOK

<https://www.tiktok.com/@nikolasferreiradun>
<https://www.tiktok.com/@teatualizei22>
https://www.tiktok.com/@monarktalks_

TWITTER

@monark
@JoseMedeirosMT
@PATRIOTAS
@nikolas_dm
@taoqueif
@profepaulamarisa
@Alan_Rick

YOUTUBE

<http://youtube.com/patriotasbr>
<https://www.youtube.com/nikolasferreirao>
<https://www.youtube.com/teatualizei>
<https://www.youtube.com/c/PaulaMarisa/featured>
<https://www.youtube.com/@MonarkTalksCortesOficial>
<https://www.youtube.com/@alanrick3>

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister **ALEXANDRE DE MORAES**

INQUÉRITO 4.879 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES)	: SOB SIGILO
PROC.(A/S)(ES)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO

Brasília, 11 de janeiro de 2023.

As empresas

FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA

RUMBLE

TELEGRAM

TIK TOK

TWITTER

YOUTUBE

Ref: Inquérito 4.879

INQ 4879 / DF

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO a expedição de ofício às empresas FACEBOOK, RUMBLE, TELEGRAM, TIK TOK, TWITTER e YOUTUBE, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo: [acrescentar todos os links indicados:

FACEBOOK

<https://www.facebook.com/people/Patriotas/100068182532776/>
<https://www.facebook.com/nikolasferreiradm>
<https://www.facebook.com/search/top?q=jos%C3%A9%20medeiros>
<https://www.facebook.com/people/Barbara-Te-Atualizei/100086379919151/>
<https://www.facebook.com/alanrickm>

INSTAGRAM

@monarkoficial
@patriotasb
@nikolasferreiradm
@josemedeirosmt
@alanrickm
@ana_lucia_bagueira
@teatualizeioficial

RUMBLE

<https://rumble.com/Monark>

INQ 4879 / DF

TELEGRAM

t.me/patriotasb
<https://t.me/nikolasferreira>
<https://t.me/monarktalks>
<https://t.me/monarkk>
<https://t.me/profepaulamarisa>

TIK TOK

<https://www.tiktok.com/@nikolasferreiradm>
<https://www.tiktok.com/@teatualizei22>
https://www.tiktok.com/@monarktalks_

TWITTER

@monark
@JoseMedeirosM1
@PATRIOTAS
@nikolas_dm
@taoquei1
@profpaulamarisa
@Alan_Rick

YOUTUBE

<http://youtube.com/patriotasbr>
<https://www.youtube.com/nikolasferreirao>
<https://www.youtube.com/teatualizei>
<https://www.youtube.com/c/PaulaMarisa/featured>
<https://www.youtube.com/@MonarkTalksCortesOficial>
<https://www.youtube.com/@alanrick3>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

INQ 4879 / DF

Relator

Documento assinado digitalmente

Cópia destinada à Polícia Federal



INQUIRY 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 9, 2023.

To companies
FACEBOOK ONLINE SERVICES BRAZIL LTDA
GETTR
TWITTER BRASIL
YOUTUBE

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

Finally, I ORDER that a letter be sent to FACEBOOK, GETTR, TWITTER and YOUTUBE so that , in the within 02 (two) hours, block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

FACEBOOK

<https://www.facebook.com/PauloGenerosoBR>

INSTAGRAM

<https://www.instagram.com/paulogenerosooficial/>

GETTR

<https://gettr.com/user/PauloGeneroso>

INQ 4781 / DF

TWITTER

<https://twitter.com/Paulogeneroso>

YOUTUBE

<https://www.youtube.com/@RepublicadeCuritiba/videos>

The companies must inform, within 24 (twenty-four) hours, the existence of any sponsors of the respective channels/profiles/accounts, as well as the existence of the transfer of amounts derived from monetization, indicating individually the gains made in each of the channels/profiles/accounts indicated.

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister ALEXANDRE DE MORAES

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 9 de janeiro de 2023.

Às empresas
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
GETTR
TWITTER DO BRASIL
YOUTUBE

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, por fim, a expedição de ofício às empresas FACEBOOK, GETTR, TWITTER e YOUTUBE para que, no prazo de 02 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

FACEBOOK

<https://www.facebook.com/PauloGenerosoBR>

INSTAGRAM

<https://www.instagram.com/paulogenerosooficial/>

GETTR

<https://gettr.com/user/PauloGeneroso>

INQ 4781 / DF

TWITTER<https://twitter.com/Paulogeneroso>**YOUTUBE**<https://www.youtube.com/@RepublicadeCuritiba/videos>

As empresas deverão informar, no prazo de 24 (vinte e quatro) horas, a existência de eventuais patrocinadores dos respectivos canais/perfis/contas, bem como a existência de repasse de valores advindos de monetização, indicando de forma individualizada os ganhos auferidos em cada um dos canais/perfis/contas indicados.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETITION 10.802 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
REQUEST(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL
APPLICANT : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, January 5, 2024.

To TWITTER BRASIL

Ref: Petition 10.802

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit, for IMMEDIATE compliance, in the following terms:

In view of all the above, I DETERMINE, in addition to and as part of the decisions of 30/12/2022, 3/5/2023, 17/5/2023 and 19/5/2023, that the social networks TWITTER, INSTAGRAM, TIKTOK, TELEGRAM, GETTR, RUMBLE and LOCALS be summoned, so that, in the within 2 (two) hours, block the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data, identifying the user, to this SUPREME COURT and the full preservation of their content:

TWITTER

<https://twitter.com/pfigueiredoshow>

In view of the confidential nature of these proceedings, the following steps should be taken

PET 10802 / DF

necessary measures for its maintenance.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Minister **ALEXANDRE DE MORAES**

Rapporteur

digitally signed document

Copy for Twitter

PETIÇÃO 10.802 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 5 de janeiro de 2024.

À empresa TWITTER DO BRASIL

Ref: Petição 10.802

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, **DETERMINO**, em caráter complementar e integrativo às decisões de 30/12/2022, 3/5/2023, 17/5/2023 e 19/5/2023, a intimação das redes sociais **TWITTER, INSTAGRAM, TIKTOK, TELEGRAM, GETTR, RUMBLE e LOCALS**, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário, a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/pfigueiredoshow>

Diante do caráter sigiloso destes autos, deverão ser adotadas as

PET 10802 / DF

providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Cópia destinada ao Twitter

INQUIRY 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, December 30, 2022.

To companies
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
TWITTER DO BRASIL
YOUTUBE BRAZIL PATREON
BRAZIL

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit for IMMEDIATE compliance, in the following terms:

(h) a dispatch of letter to companies TWITTER, YOUTUBE, FACEBOOK, INSTAGRAM and PATREON so that, within 02 (two) hours, proceed to the **total blocking, throughout the national territory, of the channels/profiles/accounts listed below, under penalty of a daily fine of R\$ 100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:**

Twitter

<https://twitter.com/Rconstantino>

YouTube

<https://www.youtube.com/user/constantinorodrigo>

<https://www.youtube.com/c/TudoConsta>

Facebook

<https://www.facebook.com/rodrigo.constantino.90>

<https://www.facebook.com/rconstantinoliberal/>

INQ 4781 / DF

Instagram

<https://www.instagram.com/constantinorodrigojp/> Patreon

<https://www.patreon.com/rodrigoconstantino>

(i) a dispatch of letter to companies TWITTER, YOUTUBE, FACEBOOK, INSTAGRAM and PATREON to inform within 24 (twenty-four) hours of the existence of any sponsors of the respective channels/profiles/accounts, as well as the existence of the transfer of amounts derived from monetization, indicating individually the gains made in each of the channels/profiles/accounts indicated in item 11.

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Airton Vieira

Teaching Magistrate in the Office of Justice

ALEXANDRE DE MORAES

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 30 de dezembro de 2022.

Às empresas
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
TWITTER DO BRASIL
YOUTUBE BRASIL
PATREON BRASIL

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

(b) a expedição de ofício às empresas TWITTER, YOUTUBE, FACEBOOK, INSTAGRAM e PATREON para que, no prazo de 02 (duas) horas, procedam ao **bloqueio total, em todo o território nacional**, dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

Twitter

<https://twitter.com/Rconstantino>

YouTube

<https://www.youtube.com/user/constantinorodrigo>

<https://www.youtube.com/c/TudoConsta>

Facebook

<https://www.facebook.com/rodrigo.constantino.90>

<https://www.facebook.com/rconstantinoliberal/>

Instagram

INQ 4781 / DF

<https://www.instagram.com/constantinorodrigojp/>
Patreon

<https://www.patreon.com/rodrigoconstantino>

(i) a expedição de ofício às empresas TWITTER, YOUTUBE, FACEBOOK, INSTAGRAM e PATREON para que informem no prazo de 24 (vinte e quatro) horas a existência de eventuais patrocinadores dos respectivos canais/perfis/contas, bem como a existência de repasse de valores advindos de monetização, indicando de forma individualizada os ganhos auferidos em cada um dos canais/perfis/contas apontadas no item h.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Airton Vieira

Magistrado Instrutor do Gabinete do
Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

INQUIRY 4.781 FEDERAL DISTRICT

RAPORTEUR : **JUSTICE ALEXANDRE DE MORAES**
AUTHOR(S) : UNDER SEAL
ADV.(A/S) : UNDER SEAL

Brasilia, December 30, 2022.

To companies
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
TWITTER DO BRASIL
YOUTUBE BRAZIL
GETTR
TELEGRAM
TIK TOK

Ref: Inquiry 4.781

Mr. Director,

I inform you that a decision has been issued in the above mentioned confidential lawsuit for IMMEDIATE compliance, in the following terms:

(h) the dispatch of a letter to the companies FACEBOOK, GETTR, TELEGRAM, TIK TOK, TWITTER and YOUTUBE to that, within two (2) hours, they **completely block** the channels/profiles/accounts listed below throughout **the national territory**, under penalty of a daily fine of R\$100,000.00 (one hundred thousand reais), with the provision of their registration data to this SUPREME COURT and the full preservation of their content:

FACEBOOK

[https://www.facebook.com/profile.php?](https://www.facebook.com/profile.php?id=100067583207919)

[id=100067583207919](https://www.facebook.com/profile.php?id=100067583207919)

INSTAGRAM

<https://www.instagram.com/realpfigueiredo/>

GETTR

INQ 4781 / DF

<https://gettr.com/user/realpfigueiredo>

TELEGRAM

<https://t.me/realpfigueiredo>

TIK TOK

<https://www.tiktok.com/@realpfigueiredo>

TWITTER

<https://twitter.com/realpfigueiredo>

YOUTUBE

<https://www.youtube.com/c/CanalPauloFigueiredo>

(i) to send a letter to the companies FACEBOOK, GETTR, TELEGRAM, TIK TOK, TWITTER and YOUTUBE so that they may inform within 24 (twenty-four) hours of the existence of any sponsors of the respective channels/profiles/accounts, as well as the existence of the transfer of amounts arising from monetization, indicating individually the gains made in each of the channels/profiles/accounts indicated in item h.

In view of the confidential nature of these proceedings, the necessary steps must be taken to maintain them.

Without further ado, I take this opportunity to renew my expressions of high esteem and consideration.

Airton Vieira

Instructor Magistrate in the Office of Justice

ALEXANDRE DE MORAES

Rapporteur

digitally signed document

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
 AUTOR(A/S)(ES) : SOB SIGILO
 ADV.(A/S) : SOB SIGILO

Brasília, 30 de dezembro de 2022.

Às empresas
 FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
 TWITTER DO BRASIL
 YOUTUBE BRASIL
 GETTR
 TELEGRAM
 TIK TOK

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

(h) a expedição de ofício às empresas FACEBOOK, GETTR, TELEGRAM, TIK TOK, TWITTER e YOUTUBE para que, no prazo de 02 (duas) horas, procedam ao **bloqueio total, em todo o território nacional**, dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

FACEBOOK

[https://www.facebook.com/profile.php?](https://www.facebook.com/profile.php?id=100067583207919)

[id=100067583207919](https://www.facebook.com/profile.php?id=100067583207919)

INSTAGRAM

<https://www.instagram.com/realpfigueiredo/>

GETTR

<https://gettr.com/user/realpfigueiredo>

INQ 4781 / DF

TELEGRAM

<https://t.me/realpfigueiredo>

TIK TOK

<https://www.tiktok.com/@realpfigueiredo>

TWITTER

<https://twitter.com/realpfigueiredo>

YOUTUBE

<https://www.youtube.com/c/CanalPauloFigueiredo>

(i) a expedição de ofício às empresas FACEBOOK, GETTR, TELEGRAM, TIK TOK, TWITTER e YOUTUBE para que informem no prazo de 24 (vinte e quatro) horas a existência de eventuais patrocinadores dos respectivos canais/perfis/contas, bem como a existência de repasse de valores advindos de monetização, indicando de forma individualizada os ganhos auferidos em cada um dos canais/perfis/contas apontadas no item h.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Airton Vieira

Magistrado Instrutor do Gabinete do

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETIÇÃO 10.391 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : DE OFÍCIO
ADV.(A/S) : SEM REPRESENTAÇÃO NOS AUTOS
REQDO.(A/S) : PARTIDO DA CAUSA OPERÁRIA - PCO
ADV.(A/S) : MATHEUS MAYER MILANEZ

DECISÃO

Em decisão, datada de 2/6/2022, proferida nos autos do Inq. 4.781/DF, foi determinada, entre outras medidas, a expedição de ofício às empresas Twitter, Instagram, Facebook, Telegram, Youtube, Tik Tok para que procedessem ao bloqueio imediato dos perfis/canais do Partido da Causa Operária (PCO) em suas plataformas, com identificação do usuário criador do perfil (Twitter: @PCO29, Instagram: @pco.29, Facebook: @pco29, Telegram: https://t.me/pco_29, Youtube: <https://youtube.com/c/CausaOperaria> TV, Tik Tok: <https://www.tiktok.com/@pco.29>).

É o breve relato. DECIDO.

O art. 4º da Res.-TSE 23.714/2022 visa a tutelar a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação de desinformações, representam substancial transgressão à própria democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 -

PET 10391 / DF

Código Eleitoral.

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito. Ou seja, *"a desinformação – entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos – conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiança, com consequente perda da credibilidade e fe nas instituições da democracia representativa"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Voto. Min. ALEXANDRE DE MORAES, julgado em 25/10/2022).

A atuação da JUSTIÇA ELEITORAL, longe de representar indevida restrição ao exercício do mandato, tem a finalidade de fazer cessar manifestações revestidas de ilicitude não inseridas no âmbito da imunidade parlamentar, a qual, conforme tenho reiteradamente enfatizado, não pode ser utilizada *"como verdadeiro escudo protetivo da prática de atividades ilícitas"* (AP 1.044, Rel. Min. ALEXANDRE DE MORAES, Pleno, DJe de 23/6/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, *"não há direito no abuso de direito"* (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio *"LIBERDADE e RESPONSABILIDADE"*; não permitindo de maneira irresponsável a efetivação de abuso no exercício

PET 10391 / DF

de um direito constitucionalmente consagrado; não permitindo a utilização da “liberdade de expressão” como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

A conduta do Partido da Causa Operária (PCO) caracterizou grave ferimento à ordem jurídica. No caso destes autos, em decisão datada de 11/1/2023, foi determinado o bloqueio dos seguintes perfis (Twitter: @PCO29, Instagram: @pco.29, Facebook: @pco29, Telegram: https://t.me/pco_29, Youtube: [https://youtube.com/c/CausaOperaria TV](https://youtube.com/c/CausaOperariaTV), Tik Tok: <https://www.tiktok.com/@pco.29>), em razão de diversas publicações contendo ataques ao SUPREMO TRIBUNAL FEDERAL e ao TRIBUNAL SUPERIOR ELEITORAL:

“Em sanha por ditadura, *skinhead* de toga retalha o direito de expressão, e prepara um novo golpe nas eleições. A repressão aos direitos sempre se voltará contra os trabalhadores! Dissolução do STF”

“É preciso adotar uma política concreta contra a ditadura do STF. Lutar pela dissolução total do tribunal e pela eleição dos juízes com mandato revogável”.

“A ditadura do TSE sobre o aplicativo Telegram é mais um ataque à liberdade de expressão e uma tentativa de fraude

PET 10391 / DF

às eleições. Após intervir ilegalmente no aplicativo, o tribunal envia mensagens a todos os usuários indicando que leiam o Estadão para ‘combater as *fake news*’.

“Tribunal Superior Eleitoral quer impôr censura a manifestações políticas em show. Fascista Alexandre de Moraes é um dos pilares da ditadura do judiciário e vai presidir o TSE nessas eleições. #ForaBolsonaro #LulaPresidnete #PCO”.

“O STF e o TSE participaram de todos os momentos cruciais do golpe de Estado contra Dilma e Lula desde 201. agora que se aproximam as eleições de 2022 com a ampla preferência popular por Lula, o judiciário golpista se prepara para mais um golpe”.

“Em 2022 as urnas eletrônicas serão ligadas diretamente a Sergio Moro e o TSE será comandado pelo lava jataista Fachin, pelo tucano fascista Alexandre de Moraes e pelo general Azevedo e Silva, que contrariava o STF durante a fraude eleitoral de 2018”.

“Um general no TSE é mais um indicativo da fraude eleitoral que a burguesia prepara para impedir o retorno de Lula ao governo. É preciso lutar contra o STF, os militares e todos os golpistas, por Lula presidente e um governo dos trabalhadores”

“O STF é um tribunal criado para defender a burguesia e seus interesses. Foi um dos principais agentes do golpe de Estado, além de usurpar poderes e os direitos democráticos de toda a população”

“Os 11 ministros não eleitos do STF acreditam estar acima do voto de dezenas de milhões de brasileiros, a própria existência da corte é antidemocrática, mas os togados ainda têm a capacidade de passar por cima da própria constituição e até

PET 10391 / DF

mesmo fraudar as eleições”.

No entanto, da análise individualizada da situação do partido político, depreende-se que houve a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral e a incentivar a realização de atos antidemocráticos pelo PCO, razão pela qual se mostra viável a reativação dos respectivos perfis, mantendo-se, porém, a remoção das postagens irregulares por ele veiculadas.

Diante do exposto, DETERMINO A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS Twitter, Instagram, Facebook, Telegram, Youtube, Tik Tok **para que procedam à reativação das contas do Partido da Causa Operária (PCO):**

Twitter: @PCO29

Instagram: @pco.29

Facebook: @pco29

Telegram: https://t.me/pco_29

Youtube: <https://youtube.com/c/CausaOperariaTV>

Tik Tok: <https://www.tiktok.com/@pco.29>

DETERMINO, AINDA, A IMPOSIÇÃO DE MEDIDA CAUTELAR em face do Partido da Causa Operária (PCO), consistente na abstenção de publicação, promoção, replicação e compartilhamento das notícias fraudulentas (*fake news*) objeto da presente decisão, sob pena de MULTA DIÁRIA DE R\$ 10.000,00 (dez mil reais) no caso de descumprimento.

Intimem-se os advogados constituídos.

Ciência à Procuradoria-Geral da República.

Publique-se.

Brasília, 28 de fevereiro de 2023.

Ministro **ALEXANDRE DE MORAES**

Relator

Documento assinado digitalmente

INQUÉRITO 4.781 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 13 de novembro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Inquérito 4.781

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO, ainda a expedição de ofício às empresas FACEBOOK e TWITTER, para que, no prazo de 02 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/HomeroMarchese?>

<https://twitter.com/HomeroMarchese/status/1589699>

[426620436480/photo/1](https://twitter.com/HomeroMarchese/status/1589699)

<https://twitter.com/LCBelemOficial>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

INQ 4781 / DF

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal



PETIÇÃO 10.802 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, na data da assinatura eletrônica.

À empresa TWITTER INC.

Ref: Petição 10.802

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, nos termos do art. 282, do Código de Processo Penal, **DETERMINO**:

(3) em caráter complementar e integrativo em relação às decisões de 30/12/2022, 3/5/2023, 17/5/2023, 19/5/2023, 4/1/2024, 23/2/2024 e 1º/3/2024, a expedição de ofício à empresa X (antigo TWITTER), para que, no prazo de 2 (duas) horas, proceda ao bloqueio do *link* abaixo discriminado, bem como que indique os usuários e perfis que estão retransmitindo o conteúdo, sob pena de multa horária de R\$ 100.000,00 (cem mil reais):

X (antigo TWITTER):

https://twitter.com/slpng_giants_pt/status/1763623754616221828?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar

PET 10802 / DF

meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada ao TWITTER INC

PETIÇÃO 10.802 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, na data da assinatura eletrônica.

À empresa TWITTER INC.

Ref: Petição 10.802

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, nos termos do art. 282, do Código de Processo Penal, **DETERMINO**:

(3) em caráter complementar e integrativo em relação às decisões de 30/12/2022, 3/5/2023, 17/5/2023, 19/5/2023, 4/1/2024, 23/2/2024 e 1º/3/2024, a expedição de ofício à empresa X (antigo TWITTER), para que, no prazo de 2 (duas) horas, proceda ao bloqueio do *link* abaixo discriminado, bem como que indique os usuários e perfis que estão retransmitindo o conteúdo, sob pena de multa horária de R\$ 100.000,00 (cem mil reais):

X (antigo TWITTER):

https://twitter.com/slpng_giants_pt/status/1763623754616221828?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar

PET 10802 / DF

meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada ao TWITTER INC

PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
 REQTE.(S) : SOB SIGILO
 ADV.(A/S) : SOB SIGILO
 REQDO.(A/S) : SOB SIGILO
 ADV.(A/S) : SOB SIGILO

Brasília, 14 de novembro de 2022.

À empresa
 TWITTER

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO:

(2) em caráter complementar e integrativo em relação às decisões de 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 28/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, DETERMINO a intimação da rede social FACEBOOK e TWITTER para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/eliasjcardoso/>

<https://twitter.com/midiabolica/>

Diante do caráter sigiloso destes autos, deverão ser adotadas as

PET 9935 / DF

providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

AIRTON VIEIRA

Magistrado Instrutor do Gabinete do
Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETIÇÃO 10.474 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 20 de julho de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.474

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA:

(II) A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS TWITTER, YOUTUBE E FACEBOOK, para que procedam ao bloqueio dos canais abaixo discriminados, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

II.2) Twitter

(<https://twitter.com/TerapeutaIvan>)

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 26 de setembro de 2023.

À empresa
TWITTER INC.

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação às decisões de 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/2023 e 22/9/2023, a intimação da empresa TWITTER INC., para que, no prazo de 2 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

@Fera2023

https://twitter.com/fera2023/status/1703481992405229898?s=48&t=RCKnVh4qOeeNHcFCnAe_hA

PET 9935 / DF

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Cópia destinada ao TWITTER INC

INQUÉRITO 4.879 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES)	: SOB SIGILO
PROC.(A/S)(ES)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO

DECISÃO

Trata-se de inquérito instaurado, a pedido da Procuradoria-Geral da República, em face do **Deputado Federal Otoni Moura de Paulo Júnior, Marcos Antônio Pereira Gomes (Zé Trovão)**, Sérgio Bavini (cujo nome artístico é Sérgio Reis), Eduardo Oliveira Araújo, Wellington Macedo de Souza, Antônio Galvan, Alexandre Urbano Raitz Petersen, Turíbio Torres, Juliano da Silva Martins e Bruno Henrique Semczeszm, para apurar a convocação da população, por meio das redes sociais, a praticar atos criminosos e violentos de protesto, às vésperas do feriado de 7/9/2021, durante uma suposta manifestação e greve de caminhoneiros.

INQ 4879 / DF

É o relato. DECIDO.

O contexto fático apontado pela Procuradoria-Geral da República autorizou, inicialmente, a adoção de diversas medidas cautelares, frente à "necessidade da medida" (necessidade para aplicação da lei penal, para a investigação ou a instrução criminal e, nos casos expressamente previstos, para evitar a prática de infrações penais) e sua "adequação" (adequação da medida à gravidade do crime, circunstâncias do fato e condições pessoais do indiciado ou acusado).

Assim, em decisão de 16/8/2021, foram determinadas as seguintes medidas cautelares em face dos investigados acima nominados:

(a) A INSTAURAÇÃO de inquérito solicitada pela Procuradoria Geral da República, em face do Deputado Federal Otoni Moura de Paulo Júnior, Marcos Antônio Pereira Gomes (Zé Trovão), Sérgio Bavini (cujo nome artístico é Sérgio Reis), Eduardo Oliveira Araújo, Wellington Macedo de Souza, Antônio Galvan, Alexandre Urbano Raitz Petersen, Turíbio Torres, Juliano da Silva Martins e Bruno Henrique Semczeszm;

(b) A BUSCA E APREENSÃO de documentos/bens que se relacionem aos fatos e delitos sob apuração, bem como de celulares, computadores, tablets e quaisquer outros dispositivos eletrônicos, nos endereços residenciais e profissionais dos requeridos Deputado Federal Otoni Moura de Paulo Júnior inclusive em seu gabinete na Câmara dos Deputados e apartamento funcional Marcos Antônio Pereira Gomes (Zé Trovão), Sérgio Bavini (cujo nome artístico é Sérgio Reis), Eduardo Oliveira Araújo, Wellington Macedo de Souza, Antônio Galvan, Alexandre Urbano Raitz Petersen, Turíbio Torres, Juliano da Silva Martins e Bruno Henrique Semczeszm. Todos os endereços serão indicados pela Procuradoria Geral da República e pela autoridade policial. AUTORIZO, ainda, nos termos requeridos pela Procuradoria Geral da República, o acesso imediato e exploração do conteúdo dos documentos em qualquer suporte (físicos, mídias eletrônicas, servidores, nuvens, etc.) que se encontrem nos locais ou em poder dos

INQ 4879 / DF

requeridos ou das pessoas que com eles aí estiverem, propiciando atuação célere e imediata, inclusive já no local em que se realiza a ação;

(c) A OITIVA PELA AUTORIDADE POLICIAL de todos os requeridos, imediatamente após a realização da busca e apreensão;

(d) A RESTRIÇÃO DOS INVESTIGADOS DE APROXIMAÇÃO DE 1 (UM) QUILÔMETRO DE RAIOS DA PRAÇA DOS TRES PODERES, DOS MINISTROS DO SUPREMO TRIBUNAL FEDERAL E DOS SENADORES DA REPÚBLICA para evitar a prática de infrações penais e preservação da integridade física e psicológica dos Ministros, Senadores, servidores ali lotados, bem como do público em geral que diariamente frequenta e transita nas imediações. A presente restrição somente não se aplicará ao Deputado Federal Otoni Moura de Paulo Júnior, em razão da necessidade do exercício de suas atividades parlamentares;

(e) A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS RESPONSÁVEIS POR REDES SOCIAIS (Facebook, Instagram, Twitter, Youtube) para que procedam ao bloqueio imediato dos perfis de titularidade dos requeridos, a serem indicados pela Procuradoria Geral da República e pela autoridade policial;

(f) A EXPEDIÇÃO DE OFÍCIO AO BANCO CENTRAL PARA O BLOQUEIO da chave PIX *7desetembro@portalbrasillivre.com*, bem como da conta a qual a referida chave se encontra vinculada, nos termos requeridos pela Procuradoria Geral da República, com envio a esta CORTE, no prazo de 24 (vinte e quatro) horas, das informações pertinentes;

(g) AS MEDIDAS CAUTELARES INOMINADAS requeridas pela Procuradoria Geral da República, quais sejam: *não se comunicarem entre si os manifestantes; bloqueio e não participação em suas e em quaisquer redes sociais; proibição de eventos em ruas e monumentos no Distrito Federal.*

INQ 4879 / DF

No que diz respeito a MARCOS ANTÔNIO PEREIRA GOMES, por meio de decisão de 1º/9/2021, nos termos dos arts. 282, § 4º e 312, § 1º, ambos do Código de Processo Penal, o investigado teve a sua prisão preventiva decretada.

A prisão, no entanto, foi efetivada tão somente em 26/10/2021, pois, conforme amplamente noticiado, o investigado evadiu-se do território nacional, fato por ele admitido, firmando esconderijo no México, após transitar pelo Panamá, de onde continuou a publicar vídeos incentivando atos violentos de protesto e a ofender a instituição do SUPREMO TRIBUNAL FEDERAL, revelando seu completo desprezo pelo Poder Judiciário.

Em 17/12/2021, converti a prisão preventiva do investigado em prisão domiciliar, posteriormente substituída pelas seguintes medidas cautelares:

(a) uso de tornozeleira eletrônica, nos termos do inciso IX do art. 319 do Código de Processo Penal;

(b) proibição de participação em redes sociais de sua titularidade, ou de quaisquer outras pessoas;

(c) proibição de conceder qualquer tipo de entrevista sem prévia autorização judicial;

(d) proibição de comunicação com quaisquer dos investigados neste inquérito.

As medidas cautelares impostas ao Deputado Federal OTONI DE PAULA e a MARCOS ANTÔNIO PEREIRA GOMES continuam em pleno vigor, não havendo qualquer decisão judicial que as tenha modificado ou revogado.

No entanto, há notícia de que ambos os investigados adotam comportamento que viola os termos das medidas cautelares impostas, mediante a criação e utilização de novos perfis nas redes sociais. Dessa forma, também devem ser adotadas medidas que restrinjam o comportamento recalcitrante dos investigados quanto ao ponto.

INQ 4879 / DF

Diante do exposto, DETERMINO a intimação das redes sociais FACEBOOK, TWITTER, TIK TOK, TELEGRAM e YOUTUBE para que procedam ao bloqueio dos canais/perfis/grupos abaixo discriminados, **no prazo máximo de 24 (vinte e quatro horas)**, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

(a) FACEBOOK:

@otonidepaularj

<https://www.instagram.com/otonidepaularj/?hl=en>https://web.facebook.com/otonidepaularj?_rdc=1&_rdr**(b) TWITTER:**<https://twitter.com/OtoniDePaula>**(c) TIK TOK:**<https://www.tiktok.com/@deputadootonidepaulajr>**(d) TELEGRAM:**<https://t.me/+L0PkRjJvJy0zZjhh><https://web.telegram.org/z/#-1281444021><https://t.me/ZeTrovaoOficial>**(e) YOUTUBE:**https://www.youtube.com/channel/UCKGFo1c87prpFyxI5_2UJXw

Cumpra-se, encaminhando-se com urgência à autoridade policial.

Ciência à Procuradoria-Geral da República.

Brasília, 8 de agosto de 2022.

Ministro **ALEXANDRE DE MORAES**

Relator

Documento assinado digitalmente

INQUÉRITO 4.879 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES)	: SOB SIGILO
PROC.(A/S)(ES)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO

Brasília, 23 de agosto de 2023.

Às empresas
 META INC.
 TWITTER
 TIK TOK
 YOUTUBE

Ref: Inquérito 4.879

Senhor Diretor,

INQ 4879 / DF

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS META INC., TWITTER, TIK TOK e YOUTUBE para que procedam à reativação das contas do Deputado Federal OTONI DE PAULA, nos seguintes termos:

FACEBOOK

facebook.com/OtoniDeputadoFederal
([https://web.facebook.com/otonidepaularj?
_rdc=1&_rdr](https://web.facebook.com/otonidepaularj?_rdc=1&_rdr))

INSTAGRAM

instagram.com/otonideputadofederal
@otonidepaularj
(<https://www.instagram.com/otonidepaularj/?hl=en>)

TWITTER

twitter.com/OtoniDepFederal
<https://twitter.com/OtoniDePaula>

TIK TOK

<https://www.tiktok.com/@deputadootonidepaulajr>

YOUTUBE

<youtube.com//otonidepaulajunior>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente



Supremo Tribunal Federal

URGENTE

MANDADO DE INTIMAÇÃO Nº 784/2022

Petição n. 10391

REQTE.(S) : DE OFÍCIO
ADV.(A/S) : SEM REPRESENTAÇÃO NOS AUTOS
REQDO.(A/S) : PARTIDO DA CAUSA OPERÁRIA - PCO
ADV.(A/S) : MATHEUS MAYER MILANEZ (59370/DF)

(Gerência de Processos Originários Criminais)

O **Ministro Alexandre de Moraes**, do Supremo Tribunal Federal, **MANDA** que o oficial de justiça **INTIME** TWITTER BRASIL REDE DE INFORMAÇÃO LTDA., na pessoa do advogado [REDACTED] com endereço na [REDACTED] do inteiro teor do despacho proferido em 17 de junho de 2022, cuja cópia segue anexa.

Secretaria Judiciária do Supremo Tribunal Federal, em 20 de junho de 2022.

Ministro Alexandre de Moraes
Relator
Documento assinado digitalmente

PETIÇÃO 10.391 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : DE OFÍCIO
ADV.(A/S) : SEM REPRESENTAÇÃO NOS AUTOS
REQDO.(A/S) : PARTIDO DA CAUSA OPERÁRIA - PCO
ADV.(A/S) : MATHEUS MAYER MILANEZ

DESPACHO

Trata-se de agravos regimentais interpostos por Telegram Messenger Inc. (eDoc. 24), Meta Platforms Inc. (eDoc. 37), Bytedance Brasil Tecnologia LTDA. (eDoc. 41) e Twitter Brasil Rede de Informação LTDA. (eDoc. 43).

É o breve relato.

Nos termos do art. 317, § 4º, do Regimento Interno do SUPREMO TRIBUNAL FEDERAL, o agravo regimental não terá efeito suspensivo, de modo que não há qualquer justificativa para o parcial descumprimento da decisão judicial proferida nestes autos.

OFICIE-SE às empresas Twitter, Instagram, Facebook, Telegram, Youtube, Tik Tok para que procedam ao **imediato bloqueio** dos perfis/canais do Partido da Causa Operária (PCO) em suas plataformas, abaixo indicados, no prazo máximo de 24 (vinte e quatro) horas:

Twitter: @PCO29

Instagram: @pco.29

Facebook: @pco29

Telegram: https://t.me/pco_29

Youtube: [https://youtube.com/c/CausaOperaria TV](https://youtube.com/c/CausaOperariaTV)

Tik Tok: <https://www.tiktok.com/@pco.29>

Em caso de descumprimento, fixo multa diária no valor de R\$ 20.000,00 (vinte mil reais), nos termos do art. 3º do Código de Processo Penal e dos arts. 77, IV e 139, IV, ambos do Código de Processo Civil, sem prejuízo da imposição de outras medidas coercitivas.

Junte-se aos autos a petição STF nº 45.109/2022.

PET 10391 / DF

Publique-se.

Brasília, 17 de junho de 2022.

Ministro **ALEXANDRE DE MORAES**

Relator

Documento assinado digitalmente

PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 11 de fevereiro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 9.935

Senhor Diretor,

Foi proferida decisão nos autos em epígrafe, para imediato cumprimento, nos seguintes termos:

Diante do exposto, **em caráter complementar e integrativo em relação à decisão de 6/10/2021**, DETERMINO:

(b) a intimação da rede social Twitter, através de sua representante no território nacional (Twitter Brasil Rede de Informação Ltda) para que bloqueie, **no prazo máximo de 24 (vinte e quatro horas)**, o seguinte perfil em sua plataforma, vinculado ao investigado ALLAN LOPES DOS SANTOS:

Twitter: @allandossantos_
(https://twitter.com/allandossantos_)

Deverá a plataforma indicar o usuário de criação dos mencionados perfis, com todos os dados disponíveis (nome, CPF, e-mail), ou qualquer outro meio de identificação possível, além de apontar a

PET 9935 / DF

data de criação dos perfis.

Deverá a plataforma, ainda, remeter TODAS as postagens realizadas por meio do perfil acima indicado aos autos desta Pet 9.935/DF, no prazo máximo de 5 (cinco) dias.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Com meus cordiais cumprimentos,

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETIÇÃO 10.792 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 27 de março de 2023.

Às empresas
INSTAGRAM e TWITTER

Ref: Pet 10.792

Senhores Diretores,

Comunico-lhes que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA, AS SEGUINTE MEDIDAS:

(7) a EXPEDIÇÃO DE OFÍCIO às empresas INSTAGRAM e TWITTER para que, no prazo de 2 (duas) horas, proceda ao bloqueio do canal/perfil/conta abaixo discriminados, bem como de quaisquer grupos que sejam administrados pelo usuário abaixo identificado, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

INSTAGRAM:

instagram.com/benito_franco/
<https://www.instagram.com/p/CmHwl61rdNs/>
<https://www.instagram.com/p/CmKYgMBjuQE/>
<https://www.instagram.com/p/CmFXA69pNuF/>
<https://www.instagram.com/p/CI92q61DmHT/>
<https://www.instagram.com/p/C1rD2FOtBfR/>
<https://www.instagram.com/p/ClcOnETOaiv/>

PET 10792 / DF

<https://www.instagram.com/p/CICLaL8u5nE/>
<https://www.instagram.com/p/CIBthzQuXwO/>
<https://www.instagram.com/p/Ck8cnz9ApD8/>
<https://www.instagram.com/p/Ck0U5MW0Cp9/>
<https://www.instagram.com/p/CkfsimCJNXk/>
<https://www.instagram.com/p/Cjoxk1Qt9VM/>

TWITTER:

twitter.com/BenitoFranco22
<https://twitter.com/Benitofranco22/status/160352388990132480>
<https://twitter.com/BenitoFranco22/status/1603459880622477312>
<https://twitter.com/BenitoFranco22/status/1603502699982589953>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETIÇÃO 10.708 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 24 de dezembro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Pet 10.708

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS FACEBOOK e TWITTER para que procedam à reativação das contas do Deputados Estadual pelo Estado do Paraná HOMERO MARCHESE, nos seguintes termos:

TWITTER

<https://twitter.com/HomeroMarchese>, com ressalva dos conteúdos indicados na decisão proferida nestes autos, cuja suspensão fica mantida (links indicados)

<https://twitter.com/HomeroMarchese/status/1589699426620436480/photo/1>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

PET 10708 / DF

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal



PETIÇÃO 10.373 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 18 de junho de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.373

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, EM ACRÉSCIMO:

(a) a intimação da rede social Twitter, através de sua representante no território nacional, para que bloqueie, **no prazo máximo de 24 (vinte e quatro horas)**, os seguintes perfis em sua plataforma, vinculado ao réu DANIEL SILVEIRA:

@DanielFederal;

@Apoio Silveira

Deverão as plataformas, ainda:

(1) indicar o usuário de criação dos mencionados perfis, com todos os dados disponíveis (nome, CPF, e-mail), ou qualquer outro meio de identificação possível, além de apontar a data de criação dos perfis.

PET 10373 / DF

(2) preservar o conteúdo do histórico de conversas, de todo o conteúdo disponível na conta e/ou que tenha sido deletado, em *container* forense (com cálculo de *hash*) e disponibilização para coleta/*download*;

(3) informar nestes autos, imediata e obrigatoriamente, acerca da criação de quaisquer novas contas/perfis pelo réu DANIEL LÚCIO DA SILVEIRA, além de proceder ao seu bloqueio IMEDIATO;

(4) adotar mecanismos que impeçam a criação de quaisquer novos perfis vinculados a DANIEL LÚCIO DA SILVEIRA.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETIÇÃO 10.373 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 23 de agosto de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.373

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, ainda:

(b) A INTIMAÇÃO DAS REDES SOCIAIS Facebook e Twitter, através de suas representantes no território nacional, para que procedam ao bloqueio dos canais/perfis/grupos vinculados ao investigado e abaixo discriminados, **no prazo máximo de 24 (vinte e quatro horas)**, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/PaolaSDaniel>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

PET 10373 / DF

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETIÇÃO 10.464 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 12 de julho de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.464

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

(c) a expedição de ofício à empresa Twitter, para que proceda ao bloqueio dos canal abaixo discriminado, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

Twitter

@eustaquiojor

twitter.com/eustaquiojor

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PETIÇÃO 10.535 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 22 de agosto de 2022

À empresa
TWITTER DO BRASIL

Ref: Petição 10.535

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, nos termos do art. 21 do Regimento Interno do SUPREMO TRIBUNAL FEDERAL, DETERMINO:

(2) **A INTIMAÇÃO DAS REDES SOCIAIS** Facebook, Tik Tok, Twitter e Youtube, através de suas representantes no território nacional, para que procedam ao bloqueio dos canais/perfis/grupos vinculados ao investigado e abaixo discriminados, **no prazo máximo de 24 (vinte e quatro horas)**, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER

<https://twitter.com/SeuVitor2822>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

PET 10535 / DF

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETIÇÃO 10.648 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 24 de dezembro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.648

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS Twitter, Youtube, Facebook, TikTok, Instagram, GETTR, KWAI e Telegram, para que procedam à reativação das contas de ANDRÉ VALADÃO, nos seguintes termos:

TWITTER

<https://twitter.com/andrevaladao>, com ressalva dos conteúdos indicados na decisão proferida nestes autos, cuja suspensão fica mantida (links indicados):

https://twitter.com/andrevaladao/status/1582840828543700992?t=G_wgJm1UVD_IKSph3Q2f-A&s=19

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

PET 10648 / DF

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Polícia Federal

PETIÇÃO 10.648 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 31 de outubro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.648

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, ainda:

(c) a expedição de ofício às empresas Twitter, Youtube, Facebook, TikTok, Instagram, GETTR, KWAI e Telegram, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

Twitter

<https://twitter.com/andrevaladao>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

PET 10648 / DF

documento assinado digitalmente

Cópia destinada à Polícia Federal



PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

Brasília, 5 de outubro de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

DETERMINO, AINDA, DIANTE DA NECESSIDADE DE BLOQUEIO DOS NOVOS PERFIS DO INVESTIGADO NAS REDES SOCIAIS:

(B) a intimação da rede social TWITTER, através de sua representante no território nacional para que bloqueie, **no prazo máximo de 24 (vinte e quatro horas)**, sob pena de multa de R\$ 100.00,00 (cem mil reais) os seguintes perfis em sua plataforma, vinculado ao investigado ALLAN LOPES DOS SANTOS:

TWITTER:

@farc_server

Deverá a plataforma, ainda:

(1) indicar o usuário de criação dos mencionados perfis, com todos os dados disponíveis (nome, CPF, e-mail), ou qualquer outro meio de identificação possível, além de apontar a data de criação dos perfis.

PET 9935 / DF

(2) remeter TODAS as postagens realizadas por meio do perfil acima indicado aos autos desta Pet 9.935/DF, em mídia eletrônica, no prazo máximo de 5 (cinco) dias;

(3) informar nestes autos, imediata e obrigatoriamente, acerca da criação de quaisquer novas contas/perfis pelo investigado ALLAN LOPES DOS SANTOS, além de proceder ao seu bloqueio IMEDIATO;

(4) adotar mecanismos que impeçam a criação de quaisquer novos perfis por ALLAN LOPES DOS SANTOS.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

PET 11704 / DF

Diante de todo o exposto, DEFIRO a representação da autoridade policial e os requerimentos formulados pela Procuradoria-Geral da República e, com fundamento nos arts. 240 e seguintes do Código de Processo Penal, **DETERMINO:**

(9) **O BLOQUEIO DOS CANAIS/PERFIS/CONTAS** abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e integral preservação de seu conteúdo, mediante expedição de ofício às empresas META INC. e TWITTER INC.:

FACEBOOK

<https://www.facebook.com/gilcemar.fariadeoliveira>

<https://www.facebook.com/vilamirvalmorromaniski.romanoski>

<https://www.facebook.com/alcides,hahn.3>

INSTAGRAM

<https://www.instagram.com/gilcemarfariadeoliveira/>

<https://www.instagram.com/vilamirvalmor>

<https://www.instagram.com/aline.paivalopes/>

<https://www.instagram.com/rodrigolinsms>

TWITTER

<https://www.twtitter.com/yettesoares14>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

PETIÇÃO 10.484 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 28 de julho de 2022.

À empresa
TWITTER DO BRASIL

Ref: Petição 10.484

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO:

A. A intimação das redes sociais FACEBOOK, TELEGRAM, TWITTER e YOUTUBE para que procedam ao bloqueio dos canais/perfis/grupos abaixo discriminados, **no prazo máximo de 24 (vinte e quatro horas)**, com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

TWITTER:

<https://twitter.com/gentedecente22>

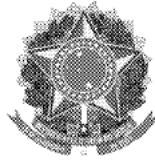
Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente



Supremo Tribunal Federal

URGENTE

Ofício eletrônico nº 7289/2023

Brasília, 2 de junho de 2023.

Ao Senhor
Administrador do TWITTER Brasil Rede de Informação Ltda.

Inquérito nº 4923

AUTOR(A/S)(ES) : MINISTÉRIO PÚBLICO FEDERAL
 PROC.(A/S)(ES) : PROCURADOR-GERAL DA REPÚBLICA
 INVEST.(A/S) : [REDACTED]
 ADV.(A/S) : [REDACTED] E OUTRO(A/S)
 INVEST.(A/S) : [REDACTED]
 ADV.(A/S) : [REDACTED] (64600/DF)
 INVEST.(A/S) : [REDACTED]
 ADV.(A/S) : [REDACTED] (15072/DF, 14768/ES) E OUTRO(A/S)
 INVEST.(A/S) : [REDACTED]
 ADV.(A/S) : [REDACTED] (31680/DF, 68794/GO,
 202448/MG) E OUTRO(A/S)
 AUT. POL. : DELEGADO DE POLÍCIA FEDERAL

(Gerência de Processos Originários Criminais)

Senhor Administrador,

Comunico-lhe os termos do(a) despacho/decisão proferido(a) nos autos em epígrafe, cuja cópia segue anexa, para as providências necessárias para a reativação da conta TWITTER: @taoquei1 de Bárbara Zambaldi Destefani.

Atenciosamente,

Ministro Alexandre de Moraes
 Relator
Documento assinado digitalmente

INQUÉRITO 4.923 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES)	: MINISTÉRIO PÚBLICO FEDERAL
PROC.(A/S)(ES)	: PROCURADOR-GERAL DA REPÚBLICA
INVEST.(A/S)	: IBANEIS ROCHA BARROS JÚNIOR
ADV.(A/S)	: CLEBER LOPES DE OLIVEIRA E OUTRO(A/S)
INVEST.(A/S)	: ANDERSON GUSTAVO TORRES
ADV.(A/S)	: EUMAR ROBERTO NOVACKI
INVEST.(A/S)	: FERNANDO DE SOUSA OLIVEIRA
ADV.(A/S)	: DANILO DAVID RIBEIRO E OUTRO(A/S)
INVEST.(A/S)	: FÁBIO AUGUSTO VIEIRA
ADV.(A/S)	: JOAO PAULO DE OLIVEIRA BOAVENTURA E OUTRO(A/S)
AUT. POL.	: DELEGADO DE POLÍCIA FEDERAL

DECISÃO

Trata-se de pedido formulado por BÁRBARA ZAMBALDI DESTEFANI (petição STF nº 23.783/2023), no qual requer a reativação de suas redes sociais.

Sustenta, em síntese, que *“jamaís atuou em grupo ou em rede articulada de pessoas, disseminou notícias falsas ou desinformação, tampouco desferiu ataques às instituições”*, ressaltando que, tendo sido encerradas as eleições em 30 de outubro de 2022, não persiste mais razão para a manutenção do bloqueio, e recorda a reativação perfis da Deputada Federal Carla Zambelli nas redes sociais.

É o breve relatório. DECIDO.

Verifica-se que, por meio de decisão proferida neste Inq. 4.923/DF, datada de 18/1/2023, acolhendo requerimento formulado pelo Presidente do Senado Federal, Senador RODRIGO PACHECO, foi autorizada a reativação das contas do Senador eleito ALAN RICK, cujo bloqueio foi imposto no mesmo ato decisório referente aos perfis de BÁRBARA ZAMBALDI DESTEFANI.

Ainda, na mencionada decisão, foi determinada a imposição de

INQ 4923 / DF

medida cautelar, consistente na abstenção de publicação, promoção, replicação e compartilhamento das notícias fraudulentas (*fake news*), sob pena de multa diária de R\$ 10.000,00 (dez mil reais) no caso de descumprimento, a ser descontada diretamente dos vencimentos recebidos pelo Parlamentar.

De fato, a partir do exame do conteúdo do ato decisório, vê-se que os argumentos veiculados para a liberação das contas do Senador ALAN RICK se mostram inteiramente aplicáveis em relação a BÁRBARA ZAMBALDI DESTEFANI, em que pese não exercer atividade parlamentar.

Eis o teor da mencionada decisão:

O art. 4º da Res.-TSE 23.714/2022 visa a tutelar a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação de desinformações, representam substancial transgressão à própria democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas

INQ 4923 / DF

que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito. Ou seja, *"a desinformação – entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos – conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiância, com conseqüente perda da credibilidade e fé nas instituições da democracia representativa"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Voto. Min. ALEXANDRE DE MORAES, julgado em 25/10/2022).

A atuação da JUSTIÇA ELEITORAL, longe de representar indevida restrição ao exercício do mandato, tem a finalidade de fazer cessar manifestações revestidas de ilicitude não inseridas no âmbito da imunidade parlamentar, a qual, conforme tenho reiteradamente enfatizado, não pode ser utilizada "como verdadeiro escudo protetivo da prática de atividades ilícitas" (AP 1.044, Rel. Min. ALEXANDRE DE MORAES, Pleno, DJe de 23/6/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, "não há direito no abuso de direito" (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio "LIBERDADE e RESPONSABILIDADE"; não permitindo de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da

INQ 4923 / DF

“liberdade de expressão” como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

A conduta do parlamentar caracterizou grave ferimento à ordem jurídica. No caso destes autos, em decisão datada de 11/1/2023, foi determinado o bloqueio dos seguintes perfis:

Conforme se vê, embora o objeto da decisão sejam os perfis de Senador eleito, os fundamentos utilizados se revelam plenamente aplicáveis a BÁRBARA ZAMBALDI DESTEFANI, considerando, ainda, que, da análise individualizada da situação da requerente, depreende-se ter havido a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral e a incentivar a realização de atos antidemocráticos, sendo viável a reativação de seus perfis, mantendo-se, porém, a remoção das postagens irregulares por ela veiculadas.

Diante do exposto, DETERMINO A EXPEDIÇÃO DE OFÍCIO ÀS EMPRESAS FACEBOOK, INSTAGRAM, TIK TOK, TWITTER E YOUTUBE para que procedam à reativação das contas de BÁRBARA ZAMBALDI DESTEFANI, nos seguintes termos:

FACEBOOK

<https://www.facebook.com/people/Barbara-Te-Atualizei/100086379919151/>

INSTAGRAM

@teatualizeioficial

INQ 4923 / DF

TIK TOK

<https://www.tiktok.com/@teatualizei22>

TWITTER

@taoquei1

YOUTUBE

<https://www.youtube.com/teatualizei>

DETERMINO, AINDA, A IMPOSIÇÃO DE MEDIDA CAUTELAR em face de BÁRBARA ZAMBALDI DESTEFANI, consistente na abstenção de publicação, promoção, replicação e compartilhamento das notícias fraudulentas (*fake news*) objeto da presente decisão, sob pena de MULTA DIÁRIA DE R\$ 10.000,00 (dez mil reais) no caso de descumprimento.

Ciência à Procuradoria-Geral da República.

Publique-se.

Brasília, 30 de maio de 2023.

Ministro **ALEXANDRE DE MORAES**

Relator

Documento assinado digitalmente

**TRIBUNAL SUPERIOR ELEITORAL****ACÓRDÃO****REPRESENTAÇÃO Nº 0601752-80.2022.6.00.0000 – BRASÍLIA – DISTRITO FEDERAL**

Relator: Ministro Benedito Gonçalves

Representante: Coligação Brasil da Esperança

Advogados: Eugênio José Guilherme de Aragão – OAB: 4935/DF e outros

Representado: Jair Messias Bolsonaro

Advogados: Tarcisio Vieira de Carvalho Neto – OAB: 11498/DF e outros

REPRESENTAÇÃO. ELEIÇÕES 2022. PRESIDENTE DA REPÚBLICA. PROPAGANDA IRREGULAR. INTERNET.

1. Representação ajuizada em desfavor do segundo colocado ao cargo de presidente da República nas Eleições 2022 por prática de propaganda irregular mediante publicações na rede social *Twitter*, em 16/10/2022, com conteúdo sabidamente inverídico, em prejuízo da candidatura da coligação representante, que veio a se sagrar vencedora do pleito majoritário.

PRELIMINAR. PERDA DE OBJETO. REJEIÇÃO.

2. A superveniência das eleições não implica prejudicialidade do pedido de remoção de conteúdo ilícito (Rp 0601373-42/DF, Rel. Min. Floriano de Azevedo Marques, sessão de 8/8/2023). Nos tempos atuais, as campanhas concentram-se notadamente na rede mundial de computadores, com registro perene das manifestações externadas pelos atores do processo eleitoral, protraindo-se assim a competência desta Justiça para adotar medidas acauteladoras ou reparatórias no âmbito da propaganda.

3. É cabível a multa do art. 57-D, § 2º, da Lei 9.504/97 na hipótese de abuso da liberdade de expressão na propaganda na internet, tal como nos casos de discurso de ódio, de ideias contrárias à ordem constitucional e ao Estado Democrático e de mensagens injuriosas, difamantes ou mentirosas (Rp 0601562-20/DF, Rel. Min. Alexandre de Moraes, DJE de 26/6/2023).

TEMA DE FUNDO. CONTEÚDO FALSO E ATENTATÓRIO À LISURA DO PROCESSO ELEITORAL. CONFIGURAÇÃO. VEDAÇÃO. ART. 57-D, *CAPUT*, DA LEI 9.504/97.

4. Consoante o art. 57-D, *caput*, da Lei 9.504/97, no curso das campanhas eleitorais a regra é a

livre manifestação do pensamento, inclusive na rede mundial de computadores, excetuada a veiculação de conceitos, imagens ou afirmações caluniosas, difamatórias, injuriosas ou sabidamente inverídicas.

5. Na linha da remansosa jurisprudência desta Corte Superior, “[a]s limitações impostas à propaganda eleitoral não afetam os direitos constitucionais de livre manifestação do pensamento e de liberdade de informação” (AgR-AREspE 0600384-93/PR, Rel. Min. Carlos Horbach, DJE de 11/5/2022).

6. No caso, o candidato representado veiculou, em 16/10/2022, em sua página no *Twitter*, postagens nas quais afirmou que a principal candidatura adversária (a) defendia ser possível que “criança toque em homem pelado em museu e aprenda sexo nas escolas”, (b) pregava a “liberação do aborto até o 6º mês de gestação”, (c) tinha apoio do narcotráfico e (d) foi responsável pela morte de cinegrafista em conhecido e lamentável episódio.

7. Em todos os casos, as mensagens veiculadas ou são inverídicas ou estão fora de contexto, inclusive com anterior sancionamento por esta Corte em hipóteses similares.

8. No referendo da Rp 0601562-20/DF, Rel. Min. Alexandre de Moraes, sessão de 28/10/2022, com posterior julgamento de mérito no mesmo sentido, consignou-se que “a notícia veiculada [...] se descola da realidade, por meio de inverdades, ao afirmar que o candidato adversário, assim como o partido pelo qual filiado, seriam favoráveis à implantação [...] do aborto”. Quanto ao tema do narcotráfico: referendo na Rp 0601259-06/DF, Rel. Min. Cármen Lúcia, sessão de 20/10/2022.

9. A tentativa de associar a sexualização de crianças funda-se em matéria na qual uma das legendas integrantes da coligação representante repudiou os ataques de grupo de extrema direita a evento cultural cujo tema era diversidade sexual. Assim, a afirmação do representado de que “[s]ão eles que defendem que criança toque em homem pelado em museu” alterou por completo o sentido original do que veiculado.

10. No que se refere à trágica morte de cinegrafista, tem-se mais uma vez imputação desprovida de substrato concreto.

MULTA. DOSIMETRIA. CASO CONCRETO.

11. A violação ao art. 57-D, *caput*, da Lei 9.504/97 enseja multa de R\$ 5.000,00 a R\$ 30.000,00, nos termos do respectivo § 2º.

12. Na espécie, cabe fixar a multa em R\$ 20.000,00, haja vista: (a) a afirmação de quatro fatos inverídicos acerca de temas extremamente sensíveis (violência, aborto, drogas e sexo); (b) o alcance das postagens, a principal delas com 40.000 mil “curtidas” e quase 12 mil replicações; (c) à época, faltavam pouco mais de 15 dias para o segundo turno das eleições.

CONCLUSÃO. PARCIAL PROCEDÊNCIA.

13. Representação cujos pedidos se julgam procedentes em parte para aplicar ao representado multa no valor de R\$ 20.000,00 e determinar a imediata remoção do conteúdo impugnado.

Acordam os ministros do Tribunal Superior Eleitoral, por maioria, em rejeitar a preliminar de perda de objeto e, no mérito, julgar procedentes em parte os pedidos na Representação para aplicar ao representado Jair Messias Bolsonaro multa pecuniária no valor de R\$ 20.000,00 e, ainda, determinar ao *Twitter* a imediata remoção dos conteúdos indicados nos *links* contidos à folha 20 da petição inicial (ID 158.300.556), sob pena de multa diária de R\$ 5.000,00, nos termos do voto do relator, vencido parcialmente o Ministro Nunes Marques, que arbitrava a multa no patamar mínimo legal.

Brasília, 9 de novembro de 2023.

MINISTRO BENEDITO GONÇALVES – RELATOR

RELATÓRIO

O SENHOR MINISTRO BENEDITO GONÇALVES: Senhor Presidente, trata-se de Representação ajuizada pela Coligação Brasil da Esperança em desfavor de Jair Messias Bolsonaro, segundo colocado na disputa do cargo de presidente da República nas Eleições 2022, por prática propaganda irregular consubstanciada em publicações diversas, com conteúdo inverídico, veiculadas no dia 16/10/2022, na rede social *Twitter*, em prejuízo do candidato adversário Luiz Inácio Lula da Silva, vencedor do pleito majoritário.

Na inicial (ID 158.300.556), apontou-se, em suma:

a) “[...] o representado, dolosamente, descontextualizou nota oficial da Secretaria Nacional LGBT do PT, publicada no *site* oficial do Partido dos Trabalhadores, repudiando atos de violência, a fim de fazer transparecer que o [então] candidato o Luiz Inácio Lula da Silva defende a lunática pauta de que ‘criança toque em homem pelado em museu e aprenda sexo nas escolas’” (fl. 6);

b) o representado sustentou também que o então candidato Luiz Inácio Lula da Silva promove ataques à religião, apoia o narcotráfico, incentiva o uso de drogas, realiza rituais satânicos e, se eleito, iria liberar a prática abortiva;

c) publicou-se, ainda, conteúdo associando o então candidato Luiz Inácio Lula da Silva ao assassinato de um cinegrafista e à “[...] ordem de assassinato do [então] presidente Jair Bolsonaro” (fl. 12);

d) todas as inverdades foram veiculadas com o objetivo de macular a imagem do opositor e angariar votos, o que contraria o disposto nos arts. 9º-A e 27 da Res.-TSE 23.610/2019. Assim, faz-se necessário determinar a remoção definitiva das publicações, a abstenção de novas práticas e a fixação de multa, na forma da lei de regência.

O representado Jair Messias Bolsonaro apresentou defesa, na qual aduziu, em síntese (ID 159.054.323):

a) o pedido de remoção do conteúdo encontra-se prejudicado, haja vista a superveniência das eleições. Ademais, a pretensão sancionatória deduzida na Representação não comporta

acolhimento, pois a multa do art. 57-D, § 2º, da Lei 9.507/97 se aplica apenas aos casos de anonimato, o que não é a hipótese dos autos. Assim, impõe-se reconhecer perda de objeto da demanda;

b) as matérias veiculadas, “[...] apesar de polêmicas e de dividirem opiniões entre o eleitorado, foram apoiadas diretamente pelo governo petista. Ou seja, as acusações de que se trataria de estratégia de desinformação não subsistem, uma vez que a conduta constituiu no mero compartilhamento de notícias, sem manipulações ou recortes, com críticas às pautas defendidas pelo partido opositor” (fl. 12);

c) “[...] as críticas não foram dirigidas a Lula pelo Representado diretamente! Diferentemente, foram apresentadas diversas notícias que demonstram algumas pautas que foram apoiadas pelo partido da coligação representante, em recente passado. Trata-se, a todo sentir, portanto, de crítica política em sua acepção mais pura” (fl. 12);

d) “[...] não se trata de fato sabidamente inverídico, de inverdade chapada e aferível de plano, o que reforça a inexistência de desinformação no caso” (fl. 12);

e) “não havendo veiculação de notícias inverídicas, mas apenas críticas às plataformas progressistas características do partido da coligação representante (das quais eventualmente se arrependa ou se envergonhe), não há que se falar em interferência desta Especializada, que sempre deverá prestigiar o livre debate de ideias [...]” (Fl. 15).

A d. Procuradoria-Geral Eleitoral opinou pela extinção do processo sem resolução do mérito (ID 158.687.705).

O feito foi a mim redistribuído em 10/1/2023, tendo em vista o encerramento da atuação dos juízes auxiliares da propaganda.

É o relatório.

VOTO

O SENHOR MINISTRO BENEDITO GONÇALVES (relator): Senhor Presidente, conforme se relatou, a hipótese cuida de Representação ajuizada em desfavor do segundo colocado ao cargo de presidente da República nas Eleições 2022 por prática de propaganda irregular mediante publicações na rede social *Twitter*, em 16/10/2022, com conteúdo sabidamente inverídico, em prejuízo do candidato da coligação representante, que veio a se sagrar vencedor do pleito majoritário.

Aprecio, ponto a ponto, as alegações formuladas pelas partes.

1. Perda de Objeto da Representação

O candidato representado aduz a perda de objeto da Representação considerando as duas sanções pleiteadas na petição inicial, quais sejam, a remoção do conteúdo impugnado (diante do término do período eleitoral) e a incidência de multa pecuniária (sob o argumento de ausência de previsão legal).

A preliminar, contudo, não merece prosperar.

Em recentíssimo julgado, esta Corte Superior assentou que **a superveniência das eleições não implica prejudicialidade do pedido de remoção de conteúdos tidos como ilícitos**.

Com efeito, nos tempos atuais, em que as campanhas se desenvolvem massivamente por intermédio da rede mundial de computadores, com registro duradouro das manifestações externadas pelos atores do processo eleitoral, tem-se que a competência desta Justiça Especializada se protraí no contexto da adoção de medidas acauteladoras ou reparatórias no âmbito da propaganda. Confira-se:

[trecho do voto do Relator] Inicialmente, assinalo que **não é possível a extinção do feito sem resolução do mérito em relação ao pedido de remoção de conteúdo. Uma vez o fato tido por ilícito tendo lugar durante o**

período eleitoral e em sede da rinha eleitoral, a competência da Justiça Eleitoral se protraí para providências acauteladoras ou reparadoras mesmo após a realização do pleito, não havendo propriamente relação de prejudicialidade.

Segue daí que, ao meu sentir, prossegue cabível e conveniente a adoção de providências supressivas de conteúdo considerado afrontante às regras eleitorais, mesmo já tendo se esgotado o período das eleições. Isso não apenas por uma razão de compreensão pessoal sobre os efeitos da competência da Justiça Eleitoral, mas também e especialmente pela percepção de que hodiernamente o fenômeno eleitoral tende a assumir uma temporalidade contínua, o que justifica o amoldamento do exercício da competência deste Tribunal às circunstâncias contemporâneas.

Neste sentido, inclusive, parece caminhar a orientação mais recente desta Corte Superior, na linha de que não fica prejudicado pedido deste jaez em razão do mero transcurso das eleições.

Cito, a esse propósito, o R-RP 0601325-83, de relatoria do Min. Carlos Horbach, julgado em 5.5.2023, no qual esta Corte Superior, por maioria, referendou a decisão que determinara a remoção do conteúdo ilícito e aplicou multa com fundamento no art. 57-D da Lei 9.504/97.

No mesmo sentido, indico o R-Rp 0601754-50, julgado em 28.3.2023, e o R-Rp 0601756-20, julgado em 18.4.2023, ambos da relatoria do Min. Alexandre de Moraes, nos quais este Tribunal decidiu, também por maioria, que é possível a aplicação da multa prevista no art. 57-D da Lei 9.504/97 nas representações por propaganda eleitoral irregular divulgada na internet mediante veiculação de informação inverídica e persiste o interesse jurídico na determinação de remoção definitiva de conteúdo, independentemente da superveniência das eleições.

Assim, não há falar em perda do objeto da representação em virtude da realização das eleições.

(Rp 0601373-42/DF, Rel. Min. Floriano de Azevedo Marques, julgado em 8/8/2023) (sem destaques no original)

De outra parte, saliente-se que, nos termos do art. 57-D da Lei 9.504/97, “é livre a manifestação do pensamento, vedado o anonimato durante a campanha eleitoral, por meio da rede mundial de computadores – internet, assegurado o direito de resposta, nos termos das alíneas a, b e c do inciso IV do § 3º do art. 58 e do 58-A, e por outros meios de comunicação interpessoal mediante mensagem eletrônica”, cuja afronta enseja a consequência prevista no § 2º, qual seja, “multa no valor de R\$ 5.000,00 (cinco mil reais) a R\$ 30.000,00 (trinta mil reais)”.

O Tribunal Superior Eleitoral, em recente interpretação acerca desses dispositivos, assentou ser cabível aplicar-se a multa prevista no art. 57-D, § 2º, da Lei 9.504/97 na hipótese de abuso na liberdade de expressão ocorrido por meio de propaganda veiculada na internet – como ocorre na divulgação de discurso de ódio, ideias contrárias à ordem constitucional e ao Estado Democrático, e de informações injuriosas, difamantes ou mentirosas –, independentemente de anonimato. Veja-se:

ELEIÇÕES 2022. RECURSO INOMINADO. REPRESENTAÇÃO. PROPAGANDA ELEITORAL IRREGULAR. INTERNET. DESINFORMAÇÃO. FATOS MANIFESTAMENTE INVERÍDICOS. REMOÇÃO DAS PUBLICAÇÕES. APLICAÇÃO DA MULTA PREVISTA NO ART. 57-D DA LEI 9.504/1997. POSSIBILIDADE. ART. 16 DA CONSTITUIÇÃO FEDERAL. NÃO INCIDÊNCIA. MULTA. VALOR. PROPORCIONALIDADE. DESPROVIMENTO.

1. O art. 57-D da Lei 9.504/1997 não restringe, de forma expressa, qualquer interpretação no sentido de limitar sua incidência aos casos de anonimato, de forma que é possível ajustar a exegese à sua finalidade de preservar a higidez das informações divulgadas na propaganda eleitoral, ou seja, alcançando a tutela de manifestações abusivas por meio da internet – incluindo-se a disseminação de fake news tendentes a vulnerar a honra de candidato adversário – que, longe de se inserirem na livre manifestação de

pensamento, constituem evidente transgressão à normalidade do processo eleitoral. Precedentes.

[...]

(Rp 0601562-20/DF, Rel. Min. Alexandre de Moraes, DJE de 26/6/2023) (sem destaque no original)

Por conseguinte, rejeito a preliminar arguida.

2. Tema de Fundo: Postagens Impugnadas

Reafirme-se que, consoante o art. 57-D, *caput* e §§ 2º e 3º, da Lei 9.504/97, no curso das campanhas eleitorais a regra é a livre manifestação do pensamento, inclusive no âmbito da rede mundial de computadores, ressalvada a utilização de conceitos, imagens ou afirmações caluniosas, difamatórias, injuriosas ou sabidamente inverídicas, sob pena de multa de R\$ 5.000,00 a R\$ 30.000,00 e de remoção do conteúdo ilícito. Confira-se:

Art. 57-D. É livre a manifestação do pensamento, vedado o anonimato durante a campanha eleitoral, por meio da rede mundial de computadores – internet, assegurado o direito de resposta, nos termos das alíneas *a*, *b* e *c* do inciso IV do § 3º do art. 58 e do 58-A, e por outros meios de comunicação interpessoal mediante mensagem eletrônica.

[...]

§ 2º A violação do disposto neste artigo sujeitará o responsável pela divulgação da propaganda e, quando comprovado seu prévio conhecimento, o beneficiário à multa no valor de R\$ 5.000,00 (cinco mil reais) a R\$ 30.000,00 (trinta mil reais).

§ 3º Sem prejuízo das sanções civis e criminais aplicáveis ao responsável, a Justiça Eleitoral poderá determinar, por solicitação do ofendido, a retirada de publicações que contenham agressões ou ataques a candidatos em sítios da internet, inclusive redes sociais.

Ademais, na linha da remansosa jurisprudência desta Corte Superior, “[a]s limitações impostas à propaganda eleitoral não afetam os direitos constitucionais de livre manifestação do pensamento e de liberdade de informação” (AgR-AREspE 0600384-93/PR, Rel. Min. Carlos Horbach, DJE de 11/5/2022).

No caso em análise, é incontroverso que o candidato representado veiculou, no dia 16/10/2022, em sua página oficial do *Twitter* (@jairbolsonaro), inúmeras postagens em detrimento da candidatura adversária ao cargo de presidente da República nas Eleições 2022.

A síntese do teor dessas manifestações pode obtida, em especial, a partir da seguinte postagem (ID 158.300.558):



Como se vê, **o representado afirmou que seu principal adversário político (aí inserida a legenda à qual este filiado): (a)** defendia a possibilidade de que “criança toque em homem pelado em museu e aprenda sexo nas escolas”; **(b)** pregava “liberação do aborto até o 6º mês de gestação”; **(c)** tem apoio do narcotráfico; **(d)** foi responsável pela morte de cinegrafista em conhecido e lamentável episódio de violência.

Em todos esses casos, as mensagens veiculadas ou são inverídicas ou estão fora de contexto e, quanto a duas delas, já houve inclusive sancionamento por esta Corte Superior em hipóteses extremamente similares.

No que tange à temática do **aborto**, confira-se o que decidido pelo Tribunal Superior Eleitoral no referendo de liminar (posteriormente confirmada pela procedência do pedido em desfavor do representado):

ELEIÇÕES 2022. REPRESENTAÇÃO. PROPAGANDA ELEITORAL. FATO SABIDAMENTE INVERÍDICO. CARACTERIZAÇÃO. LIMINAR. DEFERIMENTO.

1. A liberdade de expressão não permite a propagação de discursos de ódio e ideias contrárias à ordem constitucional e ao Estado de Direito (STF, Pleno, AP 1044, Rel. Min. ALEXANDRE DE MORAES), inclusive pelos pré-candidatos, candidatos e seus apoiadores antes e durante o período de propaganda eleitoral, uma vez que a liberdade do eleitor depende da tranquilidade e da confiança nas instituições democráticas e no processo eleitoral (TSE – RO-EI 0603975-98, Rel. Min. LUIS FELIPE SALOMÃO, DJe de 10/12/2021).

[...]

3. No caso, **a notícia veiculada**, em 16/10/2022, **se descola da realidade, por meio de inverdades, ao afirmar que o candidato adversário, assim como o partido pelo qual filiado, seriam favoráveis à implantação** de banheiro unissex nas escolas, bem como **do aborto** e da liberação das drogas. Trata-se da veiculação de informação inverídica tendente a desinformar a população acerca de temas sensíveis, que exigem ampla discussão, e sobre a qual, pretende conquistar o eleitorado contrário a matérias tão polêmicas, em evidente prejuízo de seu adversário, inclusive com a checagem realizada demonstrando a falsidade das informações.

[...]

(Referendo na Rp 0601562-20/DF, Rel. Min. Alexandre de Moraes, publicado em sessão em 28/10/2022) (sem destaque no original)

Quanto ao tema do **narcotráfico**, além de inexistir qualquer elemento que comprove a veracidade dessa afirmação, verifica-se que esta Corte analisou controvérsia similar de suposto envolvimento do adversário do representado, assentando mais uma vez se tratar de informação inverídica. Veja-se:

[síntese do julgamento] **O Tribunal, por unanimidade, referendou o parcial deferimento da liminar, determinando (a) a remoção, no prazo de 24 horas, das postagens nas quais constem as afirmações “Recebeu R\$ 300 milhões da Odebrecht”; “apoiado pelo narcotráfico” e “financiou ditaduras na Venezuela e Cuba” indicadas no endereço eletrônico apontado na decisão; [...] Votaram com a Relatora os Ministros: Benedito Gonçalves, Raul Araújo, Sérgio Banhos, Carlos Horbach, Ricardo Lewandowski e Alexandre de Moraes (Presidente). [...]**

(Referendo na Rp 0601259-06/DF, Rel. Min. Cármen Lúcia, publicado em sessão em 20/10/2022) (sem destaque no original)

De outra parte, a tentativa de associar adversário à **sexualização de crianças** é embasada, na publicação impugnada nos presentes autos, em matéria que se veiculou no *site* do Partido dos Trabalhadores (PT) com o seguinte título: “[s]ecretaria LGBT do PT repudia cancelamento da mostra Queermuseu”, na qual se externou repúdio a atos violentos orquestrados por grupo de extrema direita em detrimento de exposição ocorrida no Santander Cultural acerca da diversidade sexual e expressão de gênero.

Assim, é notório que a afirmação do representado de que “[s]ão eles que defendem que criança toque em homem pelado em museu” altera por completo o sentido original da matéria visando criar desinformação.

Por fim, no que se refere à trágica morte de **cinegrafista**, tem-se, mais uma vez, que a imputação externada pelo representado contra seus opositores políticos revela-se desprovida de substrato concreto e tem como intuito levar o eleitorado a erro.

Desse modo, configurou-se a propaganda eleitoral irregular, em afronta ao art. 57-D, *caput*, da Lei 9.504/97.

3. Dosimetria da Multa

Tal como se frisou, a multa decorrente da violação ao art. 57-D, *caput*, da Lei 9.504/97 varia de R\$ 5.000,00 a R\$ 30.000,00, nos termos do respectivo § 2º.

No caso dos autos, impõe-se fixar a multa no patamar de R\$ 20.000,00, considerando as seguintes nuances do caso concreto:

(a) a quantidade de notícias inverídicas em favor de seus adversários políticos, afirmando-se quatro fatos distintos, em relação a questões extremamente sensíveis (aborto, drogas, sexo e violência), cujo teor não encontra qualquer amparo na realidade;

(b) o alcance das postagens, com destaque especial àquela referida na fundamentação, que obteve 40.000 mil “curtidas” e foi objeto de quase 12 mil replicações (*retweets*);

(c) a circunstância de faltar, à época, pouco mais de 15 dias para o segundo turno das eleições presidenciais.

Assim, a despeito de incabível, no caso específico, aplicar o montante máximo pretendido na inicial, constata-se, por outro lado, a presença de elementos que excedem a simples violação da norma de regência.

4. Conclusão

Ante o exposto, **julgo procedentes em parte** os pedidos na Representação para aplicar ao

representado Jair Messias Bolsonaro multa pecuniária no valor de R\$ 20.000,00 e, ainda, determinar ao *Twitter* a imediata remoção dos conteúdos indicados nos *links* contidos à folha 20 da petição inicial (ID 158.300.556), sob pena de multa diária de R\$ 5.000,00.

Comunique-se à rede social *Twitter*.

É como voto.

VOTO

O SENHOR MINISTRO NUNES MARQUES: Senhor Presidente, tratando-se de propaganda relativa às eleições para o cargo de Presidente da República, reputo que o número de visualizações da postagem impugnada – 40 mil, segundo consta do voto –, não traduz, por si só, gravidade suficiente para legitimar o arbitramento da sanção próxima ao grau máximo.

Considero, ademais, que os autos não dispõem de elementos de prova capazes de demonstrar que o fato de a mídia ter sido publicada a 15 dias do segundo turno tenha impactado significativamente a disputa.

Desse modo, divirjo parcialmente, para arbitrar a multa no patamar mínimo legal.

É como voto.

EXTRATO DA ATA

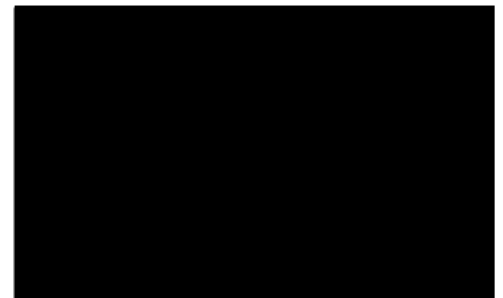
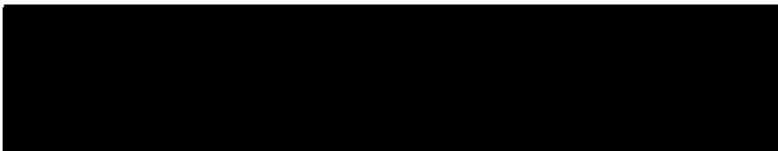
Rp nº 0601752-80.2022.6.00.0000/DF. Relator: Ministro Benedito Gonçalves. Representante: Coligação Brasil da Esperança (Advogados: Eugênio José Guilherme de Aragão – OAB: 4935/DF e outros). Representado: Jair Messias Bolsonaro (Advogados: Tarcisio Vieira de Carvalho Neto – OAB: 11498/DF e outros).

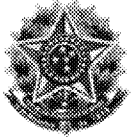
Decisão: O Tribunal, por maioria, rejeitou a preliminar de perda de objeto e, no mérito, julgou procedentes em parte os pedidos na Representação para aplicar ao representado Jair Messias Bolsonaro multa pecuniária no valor de R\$ 20.000,00 e, ainda, determinar ao *Twitter* a imediata remoção dos conteúdos indicados nos *links* contidos à folha 20 da petição inicial (ID 158.300.556), sob pena de multa diária de R\$ 5.000,00, nos termos do voto do relator, vencido parcialmente o Ministro Nunes Marques, que arbitrava a multa no patamar mínimo legal.

Composição: Ministros Alexandre de Moraes (presidente), Cármen Lúcia, Nunes Marques, Benedito Gonçalves, Raul Araújo, Floriano de Azevedo Marques e André Ramos Tavares.

Vice-Procurador-Geral Eleitoral: Paulo Gustavo Gonet Branco.

SESSÃO ORDINÁRIA REALIZADA POR MEIO ELETRÔNICO DE 3 A 9.11.2023.





29/09/2022

Número: **0601765-67.2022.6.22.0000**

Classe: **REPRESENTAÇÃO**

Órgão julgador colegiado: **Colegiado do Tribunal Regional Eleitoral**

Órgão julgador: **JUIZ AUXILIAR 2 (ACIR TEIXEIRA)**

Última distribuição : **26/09/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Redes Sociais**

Objeto do processo: **REPRESENTAÇÃO - PROPAGANDA ELEITORAL**

Segredo de justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
Procuradoria Regional Eleitoral de Rondônia (REPRESENTANTE)			
VALCLEI QUEIROZ DA SILVA (REPRESENTADO)			
AGIR POR RONDÔNIA 36-AGIR / 90-PROS (REPRESENTADO)			
Procuradoria Regional Eleitoral de Rondônia (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
7988056	29/09/2022 12:21	<u>Decisão</u>	Decisão



TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA

REPRESENTAÇÃO (11541) - Processo nº 0601765-67.2022.6.22.0000 - Porto Velho - RONDÔNIA

[Propaganda Política - Propaganda Eleitoral - Redes Sociais]

RELATOR: ACIR TEIXEIRA GRECIA

REPRESENTANTE: PROCURADORIA REGIONAL ELEITORAL DE RONDÔNIA

REPRESENTADO: VALCLEI QUEIROZ DA SILVA, AGIR POR RONDÔNIA 36-AGIR / 90-PROS

DECISÃO

Vistos.

Trata-se de representação eleitoral, com pedido de tutela de urgência, ofertada pela PROCURADORIA REGIONAL ELEITORAL em face de VALCLEI QUEIROZ DA SILVA – “ELEIÇÃO 2022 VALCLEI QUEIROZ DA SILVA GOVERNADOR” –, e Coligação “AGIR POR RONDÔNIA” (36-AGIR / 90-PROS), com o intuito de obter “*medida de busca e apreensão de material de campanha dos representados, cumulada com ordem de abstenção de realização de propaganda eleitoral, inclusive nas redes sociais, e de demais atos de campanha*”, nos quais o primeiro representado se apresente como candidato a Governador nas Eleições 2022 (id. 7986024).

Assevera o órgão ministerial que, nos autos do RRC n. 0600924-72.2022.6.22.0000, este Regional indeferiu o pedido de registro de candidatura do representado ao cargo de Governador, bem como o da respectiva chapa majoritária, consoante o inteiro teor do Acórdão n. 284/2022, de 9/9/2022, cujo trânsito em julgado ocorreu em 12/9/2022 (id. 7986025, pág. 12/18). Em decorrência, consta que contra esse julgado, em 13/9/2022, houve a propositura de recurso ordinário, todavia, o relator não conheceu da peça recursal porquanto manifestamente intempestiva, em decisão que foi posteriormente referendada pelo Plenário do TRE/RO (id. 7986025, pág. 19/23). Para

além disso, em 21/9/2022, em decisão oriunda do colendo TSE – Tutela Cautelar Antecedente n. 0601141-30.2022.6.00.0000 –, foi indeferido o pedido de tutela de urgência formulado pelos representados, com vistas a garantir a permanência do pretense candidato ao Governo do Estado em campanha, sob o fundamento de que o trânsito em julgado do acórdão regional afasta a aplicação do permissivo contido no art. 16-A da Lei n. 9.504/1997 (id. 7986025, pág. 24/28).

Contudo, alega a representante que, ainda que não ostente mais a condição de candidato, uma vez extinta sua condição de “sub judice” com trânsito em julgado do indeferimento de seu pedido de registro, o representado “*permanece realizando propaganda eleitoral, inclusive participando de debates de TV, distribuindo de material de propaganda eleitoral e outros atos típicos de campanha*” (id. 7986025, pág. 2/11), circunstância com aptidão para confundir e levar o eleitorado ao erro, notadamente, no que toca à propaganda compartilhada em rede social.

Desse modo, pugna pela “*imediata cessação da prática de atos de campanha, bem ainda a retirada de toda a propaganda eleitoral existente, incluindo-se a propaganda impressa e aquela veiculada na internet*”.

É o relatório. Decido o pedido de tutela de urgência.

A teor do art. 300 do Código de Processo Civil e da jurisprudência do colendo TSE, a tutela provisória de urgência será concedida caso o magistrado, ainda que em juízo sumário, verifique a plausibilidade da pretensão (probabilidade de êxito), aliada à comprovação do risco de dano irreparável que, em uma análise objetiva, revele-se concreto e real.

No caso em análise, examinada a questão à luz dos elementos de prova constantes dos autos, em juízo de cognição sumária, entendo presentes os requisitos para sustentar a liminar postulada.

A Procuradoria Regional Eleitoral, em síntese, aduz que os representados estariam proibidos de realizar propaganda eleitoral e demais atos de campanha para promover a candidatura de Valclei Queiroz da Silva ao cargo de governador nas eleições 2022. Isso porque:

- i) o pedido de registro de candidatura do representado e da respectiva chapa majoritária, foram indeferidos em 9/9/2022 – RRC n. 0600924-72.2022.6.22.0000, Acórdão n. 284/2022 (id. 7986025, pág. 12/17);
- ii) o acórdão transitou em julgado em 12/9/2022 (id. 7986025, pág. 18);
- iii) o recurso contra o indeferimento do registro não foi conhecido pelo relator, pois manejado apenas em 13/9/2022, fora do prazo legal; decisão posteriormente referendada na Corte Regional (id. 7986025, pág. 19/23); e
- iv) em 21/9/2022, na Tutela Cautelar Antecedente n. 0601141-30.2022.6.00.0000 proposta perante o TSE, o pedido de tutela de urgência formulado pelos representados, com vistas a garantir a permanência do pretense candidato ao Governo do Estado em campanha, foi indeferido ao fundamento de que o trânsito em julgado do acórdão regional afasta a aplicação do permissivo contido no art. 16-

A da Lei n. 9.504/1997 (id. 7986025, pág. 24/28).

Com efeito, em se tratando de candidatura “sub judice”, não há vedação à prática de atos relativos à campanha eleitoral, à luz da norma contida no art. 16-A da Lei n. 9.504/1997, conforme se vê:

Art. 16-A. O candidato cujo registro esteja sub judice poderá efetuar todos os atos relativos à campanha eleitoral, inclusive utilizar o horário eleitoral gratuito no rádio e na televisão e ter seu nome mantido na urna eletrônica enquanto estiver sob essa condição, ficando a validade dos votos a ele atribuídos condicionada ao deferimento de seu registro por instância superior . (Incluído pela Lei n. 12.034, de 2009).

Todavia, quanto à condição “sub judice”, o § 1º do art. 51 da Resolução TSE n. 23.609/2019 é categórico ao dispor que, **com o trânsito em julgado da decisão, aquele que teve o registro indeferido não ostenta mais “status” de candidato, “in verbis”:**

“Art. 51. A candidata ou o candidato cujo registro esteja sub judice pode efetuar todos os atos relativos à campanha eleitoral, inclusive utilizar o horário eleitoral gratuito no rádio e na televisão e ter seu nome mantido na urna eletrônica enquanto estiver sob essa condição.”

§ 1º Cessa a situação sub judice:

I – com o trânsito em julgado; ou

II – independentemente do julgamento de eventuais embargos de declaração, a partir da decisão colegiada do Tribunal Superior Eleitoral, salvo se obtida decisão que:

- a) afaste ou suspenda a inelegibilidade (LC n. 64/1990, arts. 26-A e 26-C);
- b) anule ou suspenda o ato ou decisão do qual derivou a causa de inelegibilidade;

c) conceda efeito suspensivo ao recurso interposto no processo de registro de candidatura.

§ 2º Publicado o acórdão referido no parágrafo anterior com decisão pelo indeferimento, cancelamento ou não conhecimento do registro de candidatura, será alterada a situação da candidata ou do candidato no CAND e, se houver viabilidade técnica, promovida a exclusão de seu nome da urna.

§ 3º O disposto no § 1º não obsta a prolação de decisões monocráticas pelo Tribunal Superior Eleitoral e pelos Tribunais Regionais Eleitorais nas hipóteses autorizadas pela lei, por seus regimentos internos e por esta Resolução, mas, nesses casos, permanecerá a situação sub judice.”

Nesse cenário, assiste razão ao órgão ministerial, posto que, com o trânsito em julgado da decisão de indeferimento do registro neste Regional, bem ainda, com a negativa de efeito suspensivo ao recurso interposto no âmbito do TSE, o representado não ostenta mais a condição de candidato.

Assim, de rigor a cessação de todo e qualquer ato de propaganda eleitoral pelo representado, dada a proximidade do primeiro turno, de modo a preservar a normalidade e legitimidade das eleições, haja vista que essa circunstância tem aptidão para confundir e levar o eleitorado ao erro, sobretudo quando se trata de propaganda compartilhada em rede social, mostra-se necessária a concessão da medida de urgência, ainda que com algum ajuste.

Nesse ponto, com referência ao pedido para “**retirada imediata de toda e qualquer propaganda**”, **deduzido no item 1.3.1 da exordial**, tenho por bem indeferi-lo, considerando que até a data do trânsito em julgado do acórdão que indeferiu o registro de candidatura do representado (12/9/2022) e, mais especificamente da negativa de efeito suspensivo ao recurso interposto no âmbito do TSE (21/9/2022), um incontável número de adesivos, botons e outros materiais físicos de campanha foram produzidos e, a toda evidência, uma considerável parcela desse material foi distribuído a cabos eleitorais e cidadãos, não se mostrando razoável impor aos representados o ônus de recolher o material lícitamente partilhado.

Ante o exposto, DEFIRO PARCIALMENTE a tutela de urgência requerida pela Procuradoria Regional Eleitoral e DETERMINO:

1.1 a imediata exclusão das publicações nas quais o representado se apresenta como candidato a governador e/ou com menção ao número pelo qual pretendia concorrer (36), cujas plataformas e “links” que seguem relacionados (id. 7987846):

1.1.2 Facebook:

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/136150192492186/>

https://www.facebook.com/reel/492929369362968/?s=single_unit
<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/135688862538319/>
<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/135468235893715/>

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/135365205904018/>

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/pcb.135345555905983/135345499239322/>

https://www.facebook.com/reel/1437499776717845/?s=single_unit

https://www.facebook.com/reel/652750699462065/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/13>

4630139310858/

https://www.facebook.com/reel/1030032211014201/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/133654316075107/>

https://www.facebook.com/reel/579377053870673/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/133505496089989/>

https://www.facebook.com/reel/871234547195206/?s=single_unit

https://www.facebook.com/reel/475527731120122/?s=single_unit

https://www.facebook.com/reel/3301806033424803/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/132237509550121/>

https://www.facebook.com/reel/766027681343768/?s=single_unit

https://www.facebook.com/reel/1099849304070639/?s=single_unit

https://www.facebook.com/reel/612448486916728/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/130986379675234/>

https://www.facebook.com/reel/954179588836103/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/130545246386014>

https://www.facebook.com/reel/2605148056282219/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/129972236443315/>

https://www.facebook.com/reel/2334677610005086/?s=single_unit

https://www.facebook.com/reel/1117932228931701/?s=single_unit

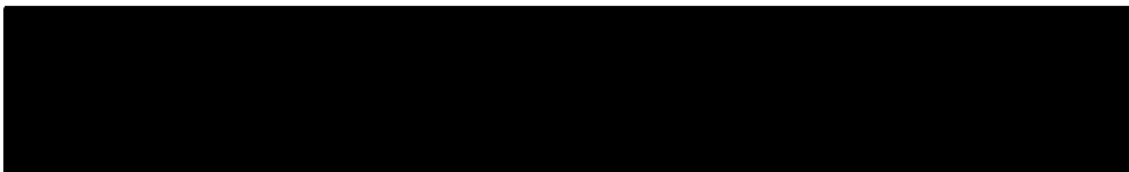
<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/129073636533175/>

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/128284203278785/>

https://www.facebook.com/reel/558082762733981/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.119786584128547/128175369956335/>

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/pcb.127513640022508/127513556689183/>



<https://www.facebook.com/comendadorvalqueiroz.ro/photos/pcb.126755490098323/126755360098336/>

https://www.facebook.com/reel/1173349683446484/?s=single_unit

https://www.facebook.com/reel/796373461397433/?s=single_unit

https://www.facebook.com/reel/472483241113309/?s=single_unit

https://www.facebook.com/reel/462900002375505/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/125809160192956/>

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/pcb.125665753540630/125665653540640/>

https://www.facebook.com/reel/475576417375263/?s=single_unit

https://www.facebook.com/reel/737369720686389/?s=single_unit

https://www.facebook.com/reel/397311125845040/?s=single_unit

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/125391610234711/>

<https://www.facebook.com/comendadorvalqueiroz.ro/photos/a.120419414065264/125317263575479/>

1.1.2 Instagram:

<https://www.instagram.com/p/CinlatHurT-/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/p/ChwkbZaNO0e/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/reel/Ch-psIUDwCD/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/p/CjDFrEDtRZu/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/reel/CjBeqZppp4N/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/tv/CjAqSJajZPg/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/p/Ci93bspsZ1W/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/p/Ci7PZwEvIWf/?igshid=YmMyMTA2M2Y=>

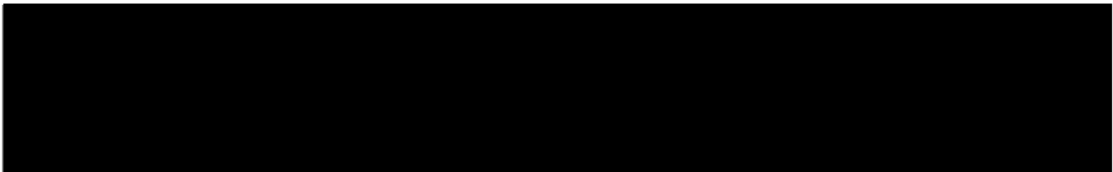
<https://www.instagram.com/p/Ci6DrvihaZC/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/p/Ci5wNFmuBow/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/tv/Ci5ttNlJU0B/?igshid=YmMyMTA2M2Y=>

<https://www.instagram.com/reel/Ci3M1iVjy5h/?igshid=YmMyMTA2M2Y=>

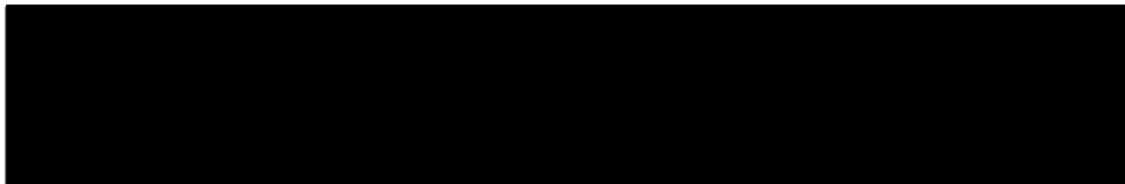
https://www.instagram.com/reel/Ci2QuhVjyNV/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CiyQxNELzXJ/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CisFgO8jCVY/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CipNpvSszU4/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CioOR7YDFKN/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/Cin9xlar56M/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/Cil5r0eD13_/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CigRLuJDILE/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CifgLWjLI5T/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/Cic3o-2D8_o/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CiaA2ehOOf8/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CiYXq1LDsLn/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CiX5y_-L2Wj/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CiVuv8cjmKE/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CiT6aSGDcQT/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CiOtSu_j4dV/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CiMzZ2nNW7k/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CiLCWUmj8c1/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/CiIDK_tgP5a/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/CiD43AsD-5a/?igshid=YmMyMTA2M2Y=s
https://www.instagram.com/p/CiCezqhtoZ7/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/Ch735fODuxs/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/Ch5q6GpN_IA/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/tv/Ch3g0WrDsGc/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/Ch11PySsucs/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/Chxhcn6u4qc/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/tv/ChuUnzNDILF/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/Chp2-DeOmnY/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/Chix427LCI8/?igshid=YmMyMTA2M2Y=



<https://www.instagram.com/reel/ChgFg06DIAA/?igshid=YmMyMTA2M2Y=>
<https://www.instagram.com/reel/ChgBDNkD2cs/?igshid=YmMyMTA2M2Y=>
https://www.instagram.com/reel/Che_XoljocL/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/ChcVvFPD_ly/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/p/ChYDI-FO_Ox/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/ChXYTSYj9b_/?igshid=YmMyMTA2M2Y=
https://www.instagram.com/reel/ChW_Z_JDeOM/?igshid=YmMyMTA2M2Y=
<https://www.instagram.com/reel/ChVp6mMjqdR/?igshid=YmMyMTA2M2Y=>
<https://www.instagram.com/p/ChVWnR6ODAb/?igshid=YmMyMTA2M2Y=>
<https://www.instagram.com/p/ChUy0xyLVu0/?igshid=YmMyMTA2M2Y=>

1.1.3 Twitter:

<https://mobile.twitter.com/valqueirozro/status/1574936845745786880>
<https://mobile.twitter.com/valqueirozro/status/1573870903158620161>
<https://mobile.twitter.com/valqueirozro/status/1573754054534209539>
<https://mobile.twitter.com/valqueirozro/status/1573277041604153345>
<https://mobile.twitter.com/valqueirozro/status/1572712811020558339>
<https://mobile.twitter.com/valqueirozro/status/1571844922394935297>
<https://mobile.twitter.com/valqueirozro/status/1571300720074260480>
<https://mobile.twitter.com/valqueirozro/status/1571263979447517184>
<https://mobile.twitter.com/valqueirozro/status/1571210354797023232>
<https://mobile.twitter.com/valqueirozro/status/1570975097846140928>
<https://mobile.twitter.com/valqueirozro/status/1569705599322963970>
<https://mobile.twitter.com/valqueirozro/status/1568779658451210240>
<https://mobile.twitter.com/valqueirozro/status/1567712091447984129>
<https://mobile.twitter.com/valqueirozro/status/1567498565026516993>
<https://mobile.twitter.com/valqueirozro/status/1567192945824043010>
<https://mobile.twitter.com/valqueirozro/status/1566093179157454848>
<https://mobile.twitter.com/valqueirozro/status/1565060235659776001>



<https://mobile.twitter.com/valqueirozro/status/1564787651546415108>
<https://mobile.twitter.com/valqueirozro/status/1564353289705213953>
<https://mobile.twitter.com/valqueirozro/status/1563496853509111815>
<https://mobile.twitter.com/valqueirozro/status/1562835651850285061>
<https://mobile.twitter.com/valqueirozro/status/1561527310431522816>
<https://mobile.twitter.com/valqueirozro/status/1561148582186700800>
<https://mobile.twitter.com/valqueirozro/status/1560994692296220675>
<https://mobile.twitter.com/valqueirozro/status/1559949024957980672>
<https://mobile.twitter.com/valqueirozro/status/1559948937926164480>
<https://mobile.twitter.com/valqueirozro/status/1557399634020122626>

1.1.4 TikTok:

https://www.tiktok.com/@comendadorvalclei/video/7134082397959703814?is_from_webapp=1&sender_device=pc&web_id=7148493323094836741

– **No prazo de 6h (seis horas)** a contar da notificação, considerada a proximidade do dia da eleição, na forma do art. 38, §§4º e 5º, da Resolução TSE n. 23.610/2019;

1.2 busca e apreensão nos comitês de Valclei Queiroz da Silva instalados no Estado, com a maior brevidade possível, para que seja apreendido todo o material de campanha, especialmente panfletos, adesivos, santinhos ou demais objetos de propaganda eleitoral que contenham a foto, nome e número de urna com a indicação de que Valclei Queiroz da Silva é candidato ao cargo de Governador do Estado de Rondônia ou qualquer outro tipo de propaganda que induza o eleitor a concluir que Valclei Queiroz da Silva ainda concorre no pleito de 2022;

1.3 a VALCLEI QUEIROZ DA SILVA e à COLIGAÇÃO “AGIR POR RONDÔNIA”, sob pena de multa no valor de R\$ 100.000,00 (cem mil reais), por violação, em caso de descumprimento:

1.3.1 – indeferido;

1.3.2 abstenham-se, imediatamente, de promover atividades de militância e mobilização de rua, bem como realização de passeatas, caminhadas, carreatas e comícios ou atos similares de promoção/exibição, inclusive propaganda eleitoral na internet, redes sociais, aplicativos de mensagens e em horário eleitoral gratuito contendo foto, nome e número de urna com a indicação de que Valclei Queiroz da Silva é candidato ao cargo de Governador do Estado de Rondônia ou qualquer outro tipo de propaganda que induza o eleitor a concluir que Valclei Queiroz da Silva

ainda concorre no pleito de 2022;

1.3.3 a **vedação imediata da distribuição de material impresso**, como santinhos e materiais similares de propaganda;

1.4 À COLIGAÇÃO “AGIR POR RONDÔNIA” (AGIR-PROS) para que se abstenha de repassar qualquer valor do fundo partidário ou do FEFC à campanha majoritária de Valclei Queiroz da Silva – sob pena de multa no valor de R\$ 50.000,00 (cinquenta mil reais), por violação, em caso de descumprimento;

1.5 Às EMISSORAS DE RÁDIO E TV EM RONDÔNIA para que se abstenham de permitir a participação de Valclei Queiroz da Silva, na condição de candidato a Governador - Eleições 2022, em entrevistas, debates e demais eventos/divulgações em que o representado se apresente como candidato ao cargo de Governador nas Eleições Gerais de 2022, sob pena de multa diária, que fixo em R\$ 1.000,00 (mil reais), limitada a R\$ 50.000,00 (cinquenta mil reais), devendo comprovar nos autos o cumprimento da medida;

1.6 Após o cumprimento da medida liminar:

1.6.1 Promova-se a citação dos representados para, querendo, apresentar defesa no prazo de 2 (dois) dias (Resolução TSE n. 23.608/2019, art. 18);

1.6.2 O envio desta decisão à ASEPA para conhecimento e eventual instrução dos processos de prestação de contas das agremiações e do candidato;

1.7 Providencie-se o necessário ao cumprimento desta decisão, com a ressalva de que as diligências devem ser realizadas com a maior brevidade possível, durante o dia (inciso XI do art. 5º da Constituição Federal), com execução simultânea nos endereços indigitados (item 1.2), utilizando-se de servidores e veículos descaracterizados, com o máximo de discrição possível. Fica autorizado o uso de força policial com aparato caracterizado, somente se houver resistência no cumprimento da ordem.

1.8 Após, redistribua-se ao relator originário, observando-se a certidão de id. 7986157.

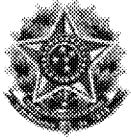
Visando dar maior celeridade ao feito, servirá cópia da presente decisão como MANDADO.

Cumpra-se.

Porto Velho, 29 de setembro de 2022.

ACIR TEIXEIRA GRÉCIA

Juiz Auxiliar da Propaganda Eleitoral do TRE-RO – Eleições Gerais de 2022



17/10/2022

Número: **0601831-53.2022.6.11.0000**

Classe: **REPRESENTAÇÃO**

Órgão julgador colegiado: **Colegiado do Tribunal Regional Eleitoral**

Órgão julgador: **Juiz Auxiliar 2 - Fábio Henrique de Moraes Fiorenza**

Última distribuição : **14/10/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Internet, Execução - De Multa Eleitoral, Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

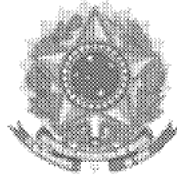
Objeto do processo: **Ação de Representação Eleitoral ajuizada pelo Ministério Público Eleitoral em desfavor de FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA, BYTEDANCE BRASIL TECNOLOGIA LTDA e TWITTER BRASIL REDE DE INFORMACAO LTDA LTDA, por veiculação de desinformação (fake news) nas redes sociais Tiktok, Twitter e Whatsapp, que noticiam falsamente a atuação da Justiça Eleitoral nos municípios de São José dos Quatro Marcos e Mirassol D'oeste/MT, em vídeo e demais anexos, propagando a seguinte mensagem: "Ontem a igreja católica de Quatro Marcos, vizinha de Mirassol, foi fechada pela justiça eleitoral pois as pessoas foram proibidas de fazer uma vigília de oração pelo Brasil, alegaram que a vigília podia favorecer a direita. Já começou a perseguição religiosa." , referente às eleições gerais de 2022.**

Segredo de justiça? **NÃO**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
Procuradoria Regional Eleitoral (REPRESENTANTE)			
FACEBOOK SERVICOS ONLINE DO BRASIL LTDA. (REPRESENTADO)			
BYTEDANCE BRASIL TECNOLOGIA LTDA. (REPRESENTADO)			
TWITTER BRASIL REDE DE INFORMACAO LTDA (REPRESENTADO)			
Procuradoria Regional Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
18329 394	17/10/2022 13:35	<u>Decisão</u>	Decisão



TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO

REFERÊNCIA TRE-MT: REPRESENTAÇÃO nº 0601831-53.2022.6.11.0000

REPRESENTANTE: Procuradoria Regional Eleitoral
REPRESENTADO: FACEBOOK SERVICOS ONLINE DO BRASIL LTDA.
REPRESENTADO: BYTEDANCE BRASIL TECNOLOGIA LTDA.
REPRESENTADO: TWITTER BRASIL REDE DE INFORMACAO LTDA
FISCAL DA LEI: Procuradoria Regional Eleitoral

DECISÃO

Vistos.

Trata-se de representação por propaganda irregular com pedido liminar (ID 18328314) apresentada pelo **MINISTÉRIO PÚBLICO ELEITORAL** em face de **FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA, BYTEDANCE BRASIL TECNOLOGIA LTDA e TWITTER BRASIL REDE DE INFORMAÇÃO LTDA.**

Segundo a mensagem impugnada, a igreja católica de São José de Quatro Marcos-MT teria sido fechada pela Justiça Eleitoral com a finalidade de proibir as pessoas de fazerem uma vigília de oração pelo Brasil, vez que o ato favoreceria a corrente ideológica de direita, o que indicaria perseguição religiosa.

De acordo com a inicial, a desinformação foi veiculada nas redes sociais "Tiktok", "Twitter" e "Whatsapp".

Afirma estarem presentes os pressupostos necessários para a concessão da tutela de urgência, requerendo, liminarmente, a remoção do conteúdo publicado nos endereços <https://twitter.com/leonard26742724/status/1578187333731434496> e https://www.tiktok.com/@raquelduarteana/video/7152598623920901381?is_from_webapp=v1&item_id=7152598623920901381.

Requer ainda a intimação das representadas para que impeçam compartilhamentos ou republicações do conteúdo, bem como para informar quem são os titulares das contas responsáveis pela publicação, possibilitando sua qualificação, assim como os endereços de "internet protocol" (IP) utilizados para acesso à conta e publicação do conteúdo objeto dos autos.

Ao fim, solicitam que, uma vez identificados os usuários, que seja determinado que se abstenham de publicar novas “fake news”, com a imposição de retratação nos mesmos canais, sob pena de multa diária a ser cominada pelo juízo.

É o relato.

Decido.

Como relatado, o Ministério Público Eleitoral requer a concessão de tutela de urgência para impedir a divulgação de propaganda irregular nas redes sociais geridas pelas Representadas.

Passo então à análise dos requisitos autorizadores da tutela.

É cediço que a tutela de urgência será concedida quando demonstrados os elementos que evidenciem a probabilidade do direito e o perigo de dano ou o risco ao resultado útil do processo, conforme art. 300 do CPC.

No caso em tela, verifico a presença dos requisitos autorizadores da tutela. Vejamos o que diz a Res. TSE 23.610/2019:

*Art.9º-A. É vedada a divulgação ou compartilhamento de **fatos sabidamente inverídicos** ou gravemente descontextualizados **que atinjam a integridade do processo eleitoral**, inclusive os processos de votação, apuração e totalização de votos, **devendo o juízo eleitoral, a requerimento do Ministério Público, determinar a cessação do ilícito**, sem prejuízo da apuração de responsabilidade penal, abuso de poder e uso indevido dos meios de comunicação.(Incluído pela Resolução nº 23.671/2021).*

E, conforme consulta realizada nesta data, a Justiça Eleitoral já desmentiu a referida mensagem, conforme se constata facilmente no link: <https://www.justicaeleitoral.jus.br/fato-ou-boato/chechagens/e-mentira-que-igreja-catolica-em-quatro-marcos-mt-tenha-sido-fechada-pela-justica-eleitoral>.

Por sua vez, o perigo de dano é evidente, na medida em que a continuidade da disseminação de tal mensagem pode trazer riscos irreparáveis à integridade do processo eleitoral, considerando-se, para tanto, o 2º turno que se avizinha e a quantidade expressiva de interações nas publicações hostilizadas¹.

Assim sendo, com esteio no art. 300 do Código de Processo Civil, **DEFIRO A LIMINAR** pretendida e determino a intimação das empresas Representadas para que:

l) removam, no prazo de 24 horas, os conteúdos publicados nos endereços <https://twitter.com/leonard26742724/status/1578187333731434496> e

https://www.tiktok.com/@raquelduarteana/video/7152598623920901381?is_from_webapp=v1&item_id=7152598623920901381 e impeçam compartilhamentos ou republicações do conteúdo, sob pena de multa diária de R\$ 30.000,00 (trinta mil reais);

II) informem ao Juízo os dados disponíveis relacionados aos titulares das contas dos responsáveis pela publicação, contribuindo, assim, para as suas respectivas qualificações;

III) forneçam os endereços de "internet protocol" (IP) utilizados para acesso às contas e publicações dos conteúdos objeto dos autos.

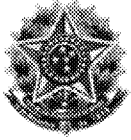
Publique-se. Intime-se. Cumpra-se.

Cuiabá, *(datado e assinado eletronicamente)*

Fábio Henrique Rodrigues de Moraes Fiorenza

Juiz Auxiliar da Propaganda

1Twitter: 13 mil curtidas, 413 comentários e 5.083 "retweets" até o momento; Tik Tok: 9.520 curtidas, 523 comentários e 4.849 compartilhamentos até o momento



31/10/2022

Número: **0601823-82.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **31/10/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **A AEED informa que, a partir de atividades de monitoramento de dados abertos de mídias sociais, esta Assessoria Especial detectou a realização de manifestação pública, na forma de live, baseada em afirmações falsas ou gravemente descontextualizadas que atingem a integridade as eleições, sendo estes os dados essenciais:**

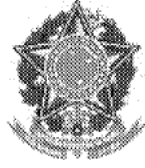
Segredo de justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
15832 1342	31/10/2022 20:38	<u>Decisão</u>	Decisão

index: PETIÇÃO CÍVEL (241)-0601823-82.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601823-82.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

**RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL**

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de manifestação pública em forma de *live*, baseada em afirmações falsas que atingem a integridade e normalidade do processo eleitoral.

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Além disso, é evidente que a manifestação pública detectada (link) tem potencial para tumultuar o processo eleitoral, na medida em que incentiva comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Veja-se, nessa linha, que a postagem reportada exhibe suposta fala do General Humberto Madeira, com advertência de que, se houver “fraude”, o vencedor das eleições “não leva”. O interlocutor, Coronel Koury, comenta sobre tais falas, aventando a possibilidade de recusa dos resultados das urnas e, conseqüentemente, de violência generalizada, caso haja “insegurança” sobre a correção dos resultados.

Apura-se do vídeo, na sequência, afirmação de que a garantia de segurança legítima só existiria com a aprovação do voto impresso, e de que, além do segmento militar, outros segmentos sociais que não aceitariam um resultado sem comprovação de idoneidade. Deixa assim a sugestão de que as eleições orientadas pelo método eletrônico de votação não seriam legítimas e que, conseqüentemente, os seus resultados devem ser recebidos com desconfiança pela população.

Convém assinalar, em acréscimo, a significativa repercussão do material ilícito, que, consoante informações prestadas pela AEED/TSE, no curso período de 8 (oito) horas obteve mais de 301.000 (trezentos e uma mil visualizações, 40.000 (quarenta mil) curtidas, 4.100 (quatro mil e cem) comentários e 15.000 (quinze mil) compartilhamentos.

Trata-se de conduta ilegal de natureza grave, com grande potencial para tumultuar as eleições em andamento, e que portanto autoriza o exercício do poder administrativo para evitar ou fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

Ante o exposto, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código, **DETERMINO** às plataformas Facebook, Twitter, Instagram, Youtube e Telegram, a imediata suspensão dos canais, grupos e perfis oficiais do Coronel Koury (Grupo B38) listados nas URLs abaixo, por um período de 72 (setenta e duas) horas, sob pena de

multa ora fixada no valor de R\$100.000,00 (cem mil reais) por hora de descumprimento, contada a partir do término da primeira hora após o recebimento da notificação.

Lista de URLs:

<https://t.me/grupob38> (Telegram)

<https://www.facebook.com/grupob38/> (Facebook)

<https://www.instagram.com/grupob38/> (Instagram)

<https://twitter.com/grupob38> (Twitter)

Coronel Koury GRUPO B-38 - YouTube (Youtube)

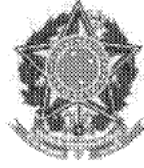
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 31 de outubro de 2022.

Ministro **ALEXANDRE DE MORAES**
Relator

index: PETIÇÃO CÍVEL (241)-0601843-73.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601843-73.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação (AEED), acerca de manifestações públicas realizadas pela Deputada Federal Carla Zambelli que atingem a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas acusações de fraude, a recusa dos resultados e intervenção militar.

A título exemplificativo, colacionam-se algumas das publicações destacadas pela AEED, das quais se depreendem as manifestações anti-democráticas:





Do vídeo imediatamente acima, foram extraídas as seguintes declarações da parlamentar: "A gente sabe que o sentimento da maioria da população é de angústia, de tristeza e até mesmo de raiva. [...] O resultado dessa eleição não reflete o que representa Jair Bolsonaro para a maioria de nós. [...] Não reflete sequer o sentimento da maioria da população. Mas, nesse momento, quero pedir a vocês que a gente tenha serenidade. Que a gente tenha força, tenha coragem, mas que tenha serenidade, para aguardar o pronunciamento do nosso Presidente e apoiá-lo sobre todas as coisas. Quando eu disse durante a campanha 'lealdade acima de tudo, lealdade ao Brasil e lealdade ao Presidente', é disso que a gente trata. [...]"

As publicação em questão, extraídas do Twitter, vêm sendo replicadas em todas as plataformas sociais da deputada e, em paralelo, constituem espaço para comentários que explicitamente clamam pela ruptura democrática, conforme se percebe das seguintes capturas:

Rute Santos da Rocha
Vamos todos !!
PARA 142 SÓ COM O POVO NAS RUAS
Curtir Responder 15 h 43

↳ 1 resposta

Superfã
Marqueli Delais
Aguentem firmes até 72 horas ,que Deus abençoe à todos ,artigo 142
Curtir Responder 14 h 27

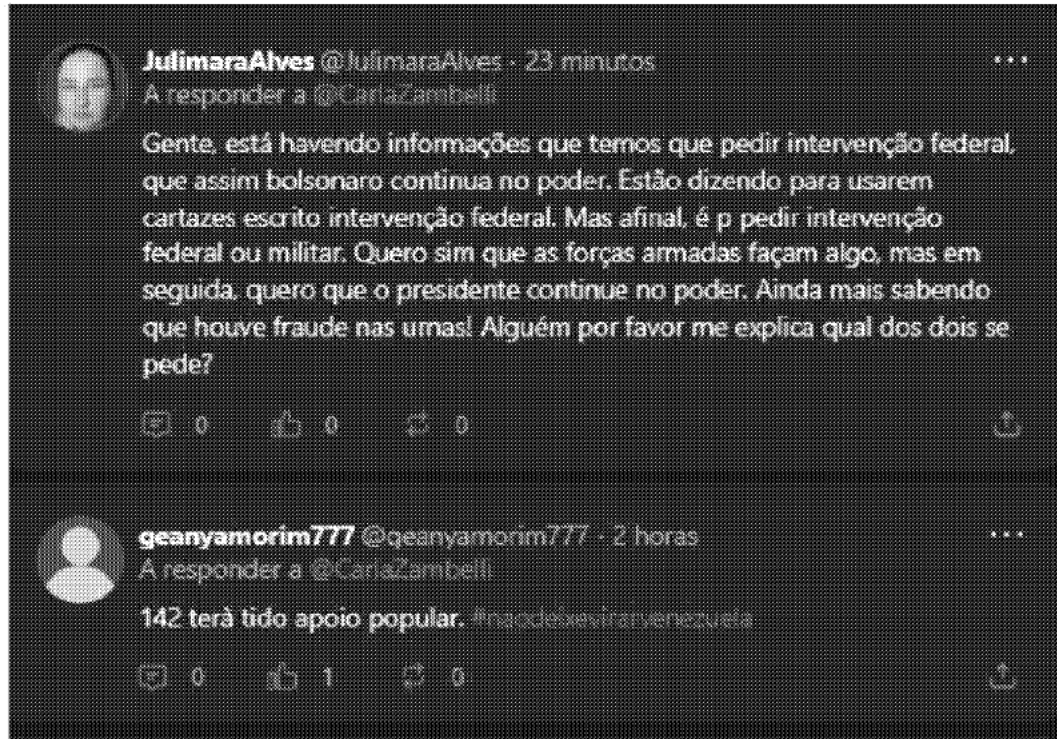
Marcio Vanessa Madeira
Artigo 142 Pelo Bem do nosso Brasil!!!
Curtir Responder 15 h Editado 44

↳ 1 resposta

Kleyton Fabio
Kde os grandes agricultores com os tratores e maquinas agriculas, eles podem apoiar e ajudar a fechar se querem acionar o artigo 142 o povo tem reagir para que seja visto pelas forças armadas.
Curtir Responder 15 h 38

↳ 5 respostas

Decei Dendi 12 horas (retirado)
DIA 7 DE SETEMBRO DE 21 PERDEMOS A CHANCE DE POR OS RATOS PRA CORRER, NUNCA SURTIRME SEU IRMIGO ,PRINCIPALMENTE SABENDO QUEM É...
Responder



Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos

eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, "caput" e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

É evidente que as publicações possuem potencial para tumultuar o processo eleitoral, na medida em que discursos pró-ruptura incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Convém assinalar, em acréscimo, a significativa repercussão do material ilícito, que já conta com milhares de interações em cada uma das plataformas, com potencial para reunir um número ainda maior de pessoas no decorrer dos dias que seguem.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato da diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

Ante o exposto, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249, 286 e 296 do Código, de ordem, **DETERMINO** ao Facebook, Twitter, Instagram, Youtube, Telegram, TikTok, Gettr, Whatsapp e LinkedIn a imediata remoção dos perfis abaixo listados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da primeira hora após o recebimento da notificação.

<https://www.facebook.com/ZambelliOficial/> (Facebook)

<https://twitter.com/Zambelli2210> (Twitter)

<https://www.instagram.com/carla.zambelli/?hl=pt-br> (Instagram)

<https://www.youtube.com/c/CarlaZambelli> (Youtube)

<https://t.me/carlazambellioficial> (Telegram)

<https://t.me/CarlaZambelli> (Telegram)

<https://www.tiktok.com/@carlazambelli22> (TikTok)

<https://gettr.com/user/carlazambelli> (Gettr)

<https://wa.me/5511981442210> (WhatsApp)

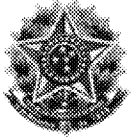
<https://www.linkedin.com/in/carlazambelli> (Linkedin)

Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 1 de novembro de 2022.

Marco Antônio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral



05/12/2022

Número: **0601843-73.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **01/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **A Assessoria Especial de Enfrentamento à Desinformação (AEED) informa a que, a partir de atividades de monitoramento de dados abertos de mídias sociais, detectou a realização de manifestações públicas em publicações na plataforma Twitter, Facebook, Instagram, Telegram, Whatsapp, Youtube, TikTok, Gettr e LinkedIn baseadas em afirmações falsas ou gravemente descontextualizadas, que atingem a normalidade e a integridade as eleições, incentivando a recusa dos resultados e fazendo apologia a um golpe militar.**

Obs: **documentos extraídos do SEI 15694-4**

Segredo de Justiça? **NÃO**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	
CARLA ZAMBELLI SALGADO (INTERESSADA)	
	THIAGO ROCHA DOMINGUES (ADVOGADO) PAULA ZANI DE LEMOS CORDEIRO (ADVOGADO) KARINA DE PAULA KUFA (ADVOGADO)

Outros participantes	
Procurador Geral Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158462080	05/12/2022 12:22	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601843-73.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de pedido formulado por CARLA ZAMBELLI SALGADO, no qual pretende, em suma, a reconsideração das decisões que determinaram a remoção de seu perfis das redes sociais Facebook, Twitter, Instagram, Youtube, Telegram, TikTok, Gettr, Whatsapp e LinkedIn. Pretende ainda o acesso integral dos presentes autos (ID 158345136).

Ato contínuo, a Assessoria Especial de Enfrentamento à Desinformação informa a divulgação de novos conteúdos irregulares, razão porque sugere a identificação *"dos perfis que realizaram as publicações, com o objetivo de identificar se a autora não está criando perfis em desacordo com a decisão proferida pela Justiça, bem como para investigar possíveis ligações com líderes e financiadores dos atos antidemocráticos e envio ao Supremo Tribunal Federal para apreciação"* (ID 158462170).

É o breve relato. Decido.

O art. 4º da Res.-TSE 23.714/2022 visa tutelar a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação desinformações, representam substancial transgressão à própria democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Dessa forma a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito.

Ou seja, *"a desinformação - entendida como uma ação comunicativa fraudulenta, baseada na propagação*

de afirmações falsas ou descontextualizadas com objetivos destrutivos - conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes", comprometendo, "portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiança, com consequente perda da credibilidade e fê nas instituições da democracia representativa" (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Voto. Min. ALEXANDRE DE MORAES, julgado em 25/10/2022).

A atuação desta JUSTIÇA ESPECIALIZADA tem a finalidade de fazer cessar manifestações revestidas de ilicitude não inseridas no âmbito da imunidade parlamentar, a qual, conforme tenho reiteradamente enfatizada, não pode ser utilizada "como verdadeiro escudo protetivo da prática de atividades ilícitas" (AP 1.044, Rel. Min. ALEXANDRE DE MORAES, Pleno, DJe de 23/6/2022).

A requerente pretende a reativação de suas contas nas redes sociais e, logo em seguida, fez vídeo com nítido interesse na ruptura do Estado Democrático de Direito, ao pleitear que os generais de quatro estrelas tomem medidas para fazer valer a incidência do art. 142 da Constituição Federal, sob o argumento de que o processo eleitoral foi fraudado.

Vê-se, assim, que, mesmo sem as redes sociais, a requerente insiste em incentivar atos antidemocráticos em apologia ao crime contra à Democracia e utiliza-se, ainda, de seguidores para disseminar informação falsa.

Por essa razão, não há como ser deferida a pretensão de reativação das redes sociais da requerente porque a finalidade dela é de desestabilizar as instituições e pugnar por ato criminoso, atitude que passa ao largo do direito que invoca de utilização das referidas redes para comunicação com seus eleitores.

Diante disso, as Plataformas Digitais devem, na hipótese, informar os dados cadastrais dos perfis abaixo indicados, bem como suspender os respectivos perfis, impedir o registro de novas contas ou canais pelos responsáveis ou sob seu controle, assim como a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347, do Código Eleitoral:

<https://gettr.com/post/p205a86ea4c>

https://www.tiktok.com/@viniciusmatosdutra/video/7171624836375088390?is_from_webapp=1&sender_device=pc&web_id=7138181630733026822

<https://www.youtube.com/watch?v=8n3ANZGk9EU&t=92s>

<https://gettr.com/post/p20536dd6ca>

https://www.tiktok.com/@rodrigofernandes8674/video/7171597617212837125?is_copy_url=1&is_from_webapp=v1&lang=pt-BR&q=Generais%20Lula&t=1669835749936

https://gettr.com/post/p2058h93a03?fbclid=IwAR1NKfBHmmdfaZcyTRGlgzdey_h6J_TeOgzExWBLSAuPjO2RAzPUHcL2WA

https://m.facebook.com/watch/?v=3034769336813055&paipv=0&eav=AfY4k0mHXfi00cbNXOCzT5oMjvI8Ic1xhd3tXJRZcoI36ROgwrqt_N2xNIqIjUxaINU&_rdr

<https://twitter.com/i/status/1597737344685465600>

<https://twitter.com/i/status/1598009747378434049>

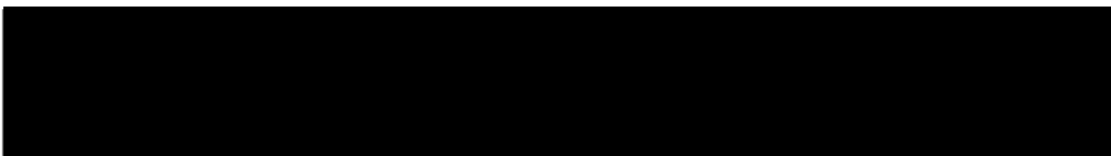
<https://twitter.com/i/status/1597995293358030848>

<https://twitter.com/i/status/1597783012493910016>

<https://twitter.com/i/status/1597774469421883392>

<https://twitter.com/i/status/1597750776302272512>
<https://twitter.com/i/status/1598013792885305347>
<https://twitter.com/i/status/1597994857255297024>
<https://twitter.com/i/status/1597886026743418880>
<https://twitter.com/i/status/1597936902308790273>
<https://twitter.com/i/status/1597890791862505472>
<https://twitter.com/i/status/1597868380601872386>
<https://twitter.com/i/status/1598001047188148231>
<https://twitter.com/i/status/1597901626030772225>
<https://twitter.com/i/status/1597767707545305089>
<https://twitter.com/i/status/1597767586410008577>
<https://twitter.com/i/status/1597783012493910016>
<https://twitter.com/i/status/1597761516904013826>
<https://twitter.com/i/status/1597994857255297024>
<https://twitter.com/i/status/1597947728587522049>
<https://twitter.com/i/status/1597767545351999489>
<https://twitter.com/i/status/1597892637968957440>
<https://twitter.com/i/status/1597789099569692672>
<https://twitter.com/i/status/1597798552591556608>
<https://twitter.com/i/status/1597737344685465600>
<https://twitter.com/i/status/1597784120989745155>
<https://twitter.com/i/status/1597799776531415040>
<https://twitter.com/i/status/1597769107008786432>
<https://twitter.com/i/status/1597760443585802241>
<https://twitter.com/i/status/1597771788347666434>
<https://twitter.com/i/status/1597750776302272512>
<https://twitter.com/i/status/1597833820400922624>
<https://twitter.com/i/status/1597794561505755136>

https://gettr.com/post/p2058h93a03?fbclid=IwAR1NKfBHmmdfaZcyTRGIgzdey_h6J_TeOg



zExWBLSc AuPjO2RAzPUHcL2WA

Por outro lado, a recalitrância da Deputada no fomento à apologia ao crime com manifestação de fraude ao processo eleitoral e, por via de consequência, de rompimento da ordem constitucional e do Estado de Direito importam na pronúncia do Ministério Público Eleitoral acerca dos crimes praticados e, em especial, para adoção das providências cabíveis.

Além disso, a fim de garantir a lisura, a normalidade e a legitimidade do processo eleitoral, fixo multa diária no valor de R\$ 20.000,00 no caso de reincidência na publicação de mensagens atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito que será cumprida mediante desconto em seus vencimentos como parlamentar.

Ante o exposto, com base nos arts. 2º, § 1º e 4º, parágrafo único, da Res.-TSE nº 23.714/2022, **DETERMINO**:

a) às Plataformas Digitais, o envio de dados da(s) pessoa(s) responsável(eis) pelo registro das contas listadas, num prazo máximo de 24 (vinte e quatro) horas; e a imediata remoção dos perfis relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação;

b) o ENCAMINHAMENTO dos autos ao Ministério Público Eleitoral para se manifestar sobre os crimes cometidos, bem como adotar as providências cabíveis;

c) a extração de cópia dos autos para posterior remessa ao Inquérito 4.781 instaurado perante o SUPREMO TRIBUNAL FEDERAL;

d) o ESTABELECIMENTO de multa no valor de R\$ 20.000,00 a Deputada Federal CARLA ZAMBELLI SALGADO, no caso de reincidência na publicação de mensagens atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito, a serem descontados de forma compulsória dos rendimentos da Parlamentar perante a Câmara dos Deputados;

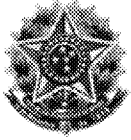
e) o INDEFERIMENTO de reativação das redes sociais da requerente; e

f) a REMOÇÃO do sigilo do processo, o que oportuniza, portanto, o acesso dos autos à Requerente que deve ainda, ser incluída como parte nos autos.

Intimem-se os envolvidos. Cumpra-se.

Brasília, 1 de dezembro de 2022.

Ministro **ALEXANDRE DE MORAES**
Presidente



17/02/2023

Número: **0601843-73.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **01/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **A Assessoria Especial de Enfrentamento à Desinformação (AEED) informa a que, a partir de atividades de monitoramento de dados abertos de mídias sociais, detectou a realização de manifestações públicas em publicações na plataforma Twitter, Facebook, Instagram, Telegram, Whatsapp, Youtube, TikTok, Gettr e LinkedIn baseadas em afirmações falsas ou gravemente descontextualizadas, que atingem a normalidade e a integridade as eleições, incentivando a recusa dos resultados e fazendo apologia a um golpe militar.**

Obs: **documentos extraídos do SEI 15694-4**

Segredo de Justiça? **NÃO**

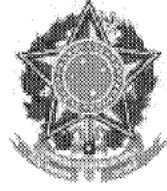
Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	
CARLA ZAMBELLI SALGADO (INTERESSADA)	
	THIAGO ROCHA DOMINGUES (ADVOGADO) PAULA ZANI DE LEMOS CORDEIRO (ADVOGADO) KARINA DE PAULA KUFA (ADVOGADO)

Outros participantes	
Procurador Geral Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158653857	17/02/2023 15:17	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601843-73.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

INTERESSADA: CARLA ZAMBELLI SALGADO

Advogados do(a) INTERESSADA: THIAGO ROCHA DOMINGUES - RJ199596, PAULA ZANI DE LEMOS CORDEIRO - RJ236778, KARINA DE PAULA KUFA - SP245404-A

DECISÃO

Em consonância com os pareceres emitidos pela Assessoria Especial de Enfrentamento à Desinformação, e tendo em consideração o correspondente contexto, DEFIRO os requerimentos de liberação dos perfis @kalliloliveira_ (URL: https://twitter.com/kalliloliveira_) – ID 158531668 – e @TelesCombate (URL: <https://twitter.com/telescombate>) – ID 158493476 – na plataforma Twitter, e DETERMINO, ademais, o levantamento de eventuais limitações no alcance da visibilidade porventura decorrentes da suspensão judicial.

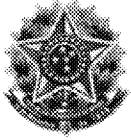
INDEFIRO, no entanto, o pedido de restabelecimento das publicações que ensejaram a decisão original de remoção, uma vez que a replicação de manifestações de caráter golpista sem sinais inequívocos de reprovação expressa termina por cumprir, independentemente da intenção não declarada de submetê-las a uma exposição negativa, o papel pragmático de amplificação indevida de uma narrativa de desinformação.

Ao teor do exposto, DETERMINO o restabelecimento das contas assinaladas.

Cumpra-se com urgência.

Brasília, 16 de fevereiro de 2023.

Ministro ALEXANDRE DE MORAES
Presidente



10/11/2022

Número: **0601853-20.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **02/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **A AEED informa que, partir de atividades de monitoramento de dados abertos de mídias sociais, detectou, nesta data, notas contas criadas pela deputada federal Carla Zambelli, em diversas mídias sociais, com o fim de driblar decisão de remoção exarada por esta Corte Superior.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)	

Outros participantes	
Procurador Geral Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158367701	10/11/2022 14:48	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601853-20.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de reprodução de manifestação pública que atinge a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas acusações de fraude, a recusa dos resultados do pleito presidencial de 2022.

O vídeo em questão foi produzido pela deputada federal Carla Zambelli e veiculado nas plataformas Twitter e Tiktok. Embora a deputada esteja com suas contas oficiais suspensas em várias plataformas, em decorrência de decisões judiciais anteriores, ela continua veiculando seus conteúdos por meio de contas de terceiros. No vídeo, a deputada volta a afirmar que houve fraude nas eleições por meio da adulteração do “software” da urna eletrônica e ainda sugere um golpe militar por meio das Forças Armadas.

A mensagem ilícita foi reproduzida, dentre outros, nos perfis abaixo listados:

<https://twitter.com/luciomaradv/status/1590541462575665153?s=48&t=kch5cj5eAbStv3ORjM4VeA>

<https://www.tiktok.com/@ivanpinheiro53? t=8XEpetY9NXp& r=1>

<https://vm.tiktok.com/ZMFfK3ge3/>

<https://vm.tiktok.com/ZMFfKT5XR/>

<https://vm.tiktok.com/ZMFfKVhPo/>

<https://vm.tiktok.com/ZMFfKgHDx/>

<https://vm.tiktok.com/ZMFfKvT2p/>

<https://vm.tiktok.com/ZMFfKcXRm/>

<https://vm.tiktok.com/ZMFfK4a8N/>

SIGILOSO

- <https://vm.tiktok.com/ZMFfKp52e/>
- <https://vm.tiktok.com/ZMFfKxGOL/>
- <https://vm.tiktok.com/ZMFfKQXUu/>
- <https://vm.tiktok.com/ZMFfKWRqv/>
- <https://vm.tiktok.com/ZMFfKbxFk/>
- <https://vm.tiktok.com/ZMFfK9rHb/>
- <https://vm.tiktok.com/ZMFfKbHBd/>
- <https://vm.tiktok.com/ZMFfK4GKy/>
- <https://vm.tiktok.com/ZMFfK33Uy/>
- <https://vm.tiktok.com/ZMFfK4A9N/>
- <https://vm.tiktok.com/ZMFfK7Yb6/>
- <https://vm.tiktok.com/ZMFfKerlw/>
- <https://vm.tiktok.com/ZMFfKs7CM/>
- <https://vm.tiktok.com/ZMFfKxxyv/>
- <https://vm.tiktok.com/ZMFfKmbD8/>
- <https://vm.tiktok.com/ZMFfKm74R/>
- <https://vm.tiktok.com/ZMFfKudt1/>
- <https://vm.tiktok.com/ZMFfKWKvn/>
- <https://vm.tiktok.com/ZMFfKVjXh/>
- <https://vm.tiktok.com/ZMFfKsbuj/>
- <https://vm.tiktok.com/ZMFfK4jxj/>
- <https://vm.tiktok.com/ZMFfKCSbC/>
- <https://vm.tiktok.com/ZMFfK95gp/>
- <https://vm.tiktok.com/ZMFfKGLb7/>
- <https://vm.tiktok.com/ZMFfKthsY/>
- <https://vm.tiktok.com/ZMFfKwgt4/>
- <https://vm.tiktok.com/ZMFfKT8CT/>
- <https://vm.tiktok.com/ZMFfKqMS9/>
- <https://vm.tiktok.com/ZMFfKKdgu/>



SIGILOSO

Ademais, foi identificado também que o perfil @Brazilwasstolenoficial (URL: <https://www.tiktok.com/@brazilwasstolenoficial?t=8XEqGOnbl9q&r=1>) na plataforma Tiktok é dedicado exclusivamente a divulgar conteúdos alegando falsamente a existência de fraude nas eleições brasileiras.

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

É evidente que a manifestação pública detectada possui potencial para tumultuar o processo eleitoral, na medida em que, implicitamente, incentiva comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Apenas em caráter exemplificativo, seguem abaixo algumas imagens por meio das quais se pode aferir que o vídeo em questão está sendo replicado em contas de terceiros:

SIGILOSO



Luciomar
@LuciomarADV

...

Em resposta a @GXMShyriu @IolandaFlaviano e @feliipebambam

Veja se isso lhe anima mais.Ou seja...
"XANDÃO...ou entrega o Código Fonte,e aí a Fraude
fica provada!
Ou Não entrega,admitindo a Culpa!
Se ficar o bicho pega!!!!
Se Correr o bicho Come!"



12:06 AM · 10 de nov de 2022 de Brasília, Brasil · Twitter for Android

SIGILOSO



sarahsilva19976

Sarah Silva

Seguir

2960 Seguindo **3708** Seguidores **66K** Curtidas

Se ninguém te apoia, vai sozinha.

Só não deixe de conquistar seus sonhos 🍀 ✨ ❤️

Vídeos

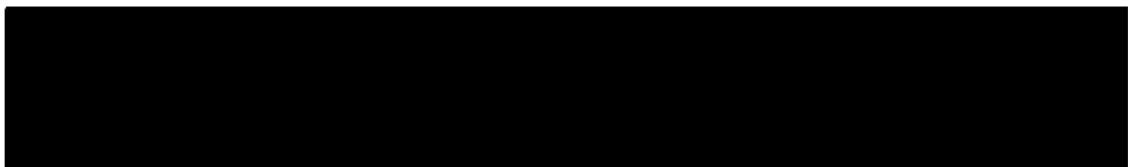
Curtido



#fy #vaiprofycaramba ...



#fy #vaiprofycaramba ...



SIGILOSO



ivanpinheiro53

ivanpinheiro

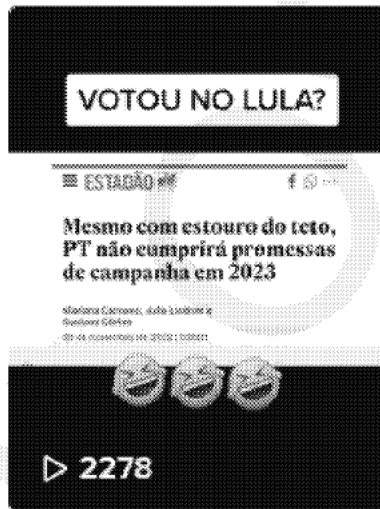
Seguir

4 Seguindo **3880** Seguidores **83.6K** Curtidas

Quem for a favor do aborto, vazal!

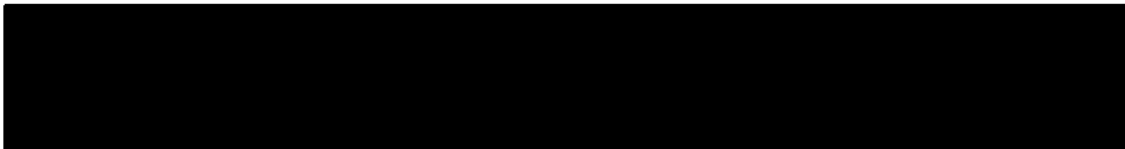
Vídeos

Curtido



Sobre o relatório! ...

SIGI



SIGILOS



jefersonguedes

Guedes Jeferson

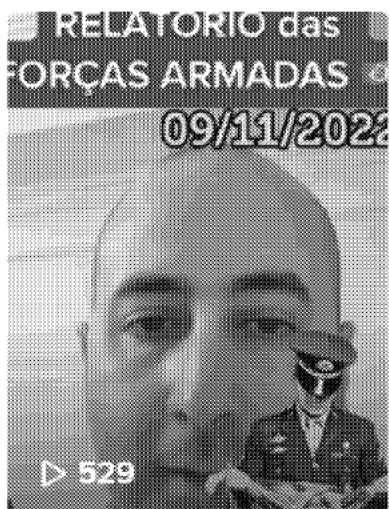
Seguir

759 Seguindo **6246** Seguidores **87.2K** Curtidas

link para cadastro Cruzeiro <http://jefersonguedes.com.br/d>

Vídeos

Curtido



#argentino ...



#carlazambelli ...

SIGI

SIGILOSO



evielancaster0511

Evie Lancaster

Seguir

520 Seguindo **385** Seguidores **5405** Curtidas

Ainda sem descrição.

Vídeos

Curtido



Carla Zambelli. Relatóri...



Campo Grande, MS ...

SIGILOS

SIGILOS



andrea_xande

andrea_xande

Seguir

914 Seguindo **1554** Seguidores **3269** Curtidas

Ainda sem descrição.

Vídeos

Curtido



brazilwasstolenoficial

BrasilWasStolen

Seguir

40 Seguindo **1767** Seguidores **14.5K** Curtidas

Grupo descentralizado de apoio à manifestações contra o comunismo.

📍 Lme/ondaverdeamarela

Vídeos

Curtido



SIGILOSO

Trata-se de conduta ilegal de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Twitter e Tiktok a remoção definitiva e imediata das respectivas postagens identificadas pelos links acima. **DETERMINO**, ainda, para ambas plataformas, a remoção definitiva e imediata do conteúdo do vídeo, veiculado na íntegra ou parcialmente em outras postagens para além das acima relacionadas, bem como de eventuais postagens futuras que venham a replicar o mesmo conteúdo, devendo ser preservada uma cópia do vídeo, pelo prazo de 6 (seis) meses, para caso seja necessário realizar investigação posterior. **DETERMINO**, por fim, à plataforma Tiktok, a remoção definitiva e imediata do perfil @Brazilwasstolenoficial, cuja URL segue abaixo:

<https://www.tiktok.com/@brazilwasstolenoficial? t=8XEqGOnbl9q& r=1>.

O descumprimento de quaisquer das determinações acima acarretará a imposição de pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

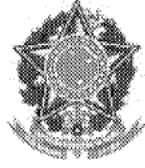
Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis, sobretudo eventual análise de abuso de poder em relação à candidata eleita Carla Zambelli.

Brasília, 10 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO

index: PETIÇÃO CÍVEL (241)-0601811-68.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601811-68.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

**RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL**

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de manifestações públicas realizadas pelo deputado federal eleito Marcel Van Hattem, que atingem a integridade e a normalidade do processo eleitoral, incentivando a realização de captação ilícita de sufrágio por coação e do crime de coação eleitoral.

As manifestações em questão foram realizadas em diferentes plataformas digitais, como se vê:

INSTAGRAM



Figura 3 -- Video publicado no Instagram

https://www.instagram.com/tv/CkQe96wphgK/?utm_source=ig_web_copy_link

FACEBOOK



Figura 4- Vídeo publicado na Facebook

YOUTUBE

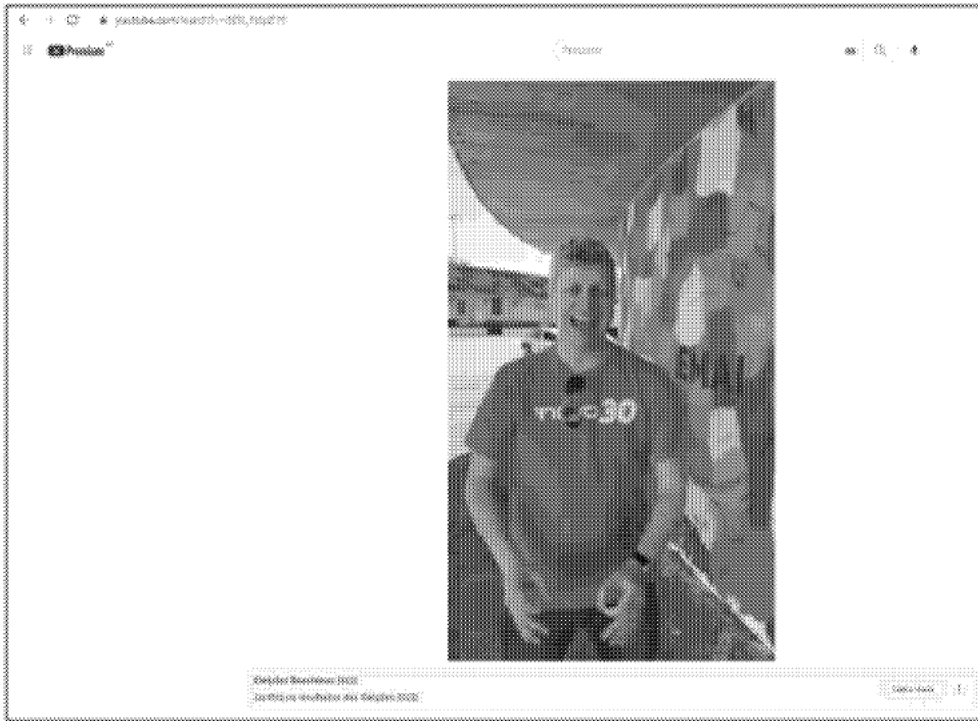


Figura 5 – Publicação YouTube

https://www.youtube.com/watch?v=9ZK_PzlpZ10&t=45s

LINKEDIN

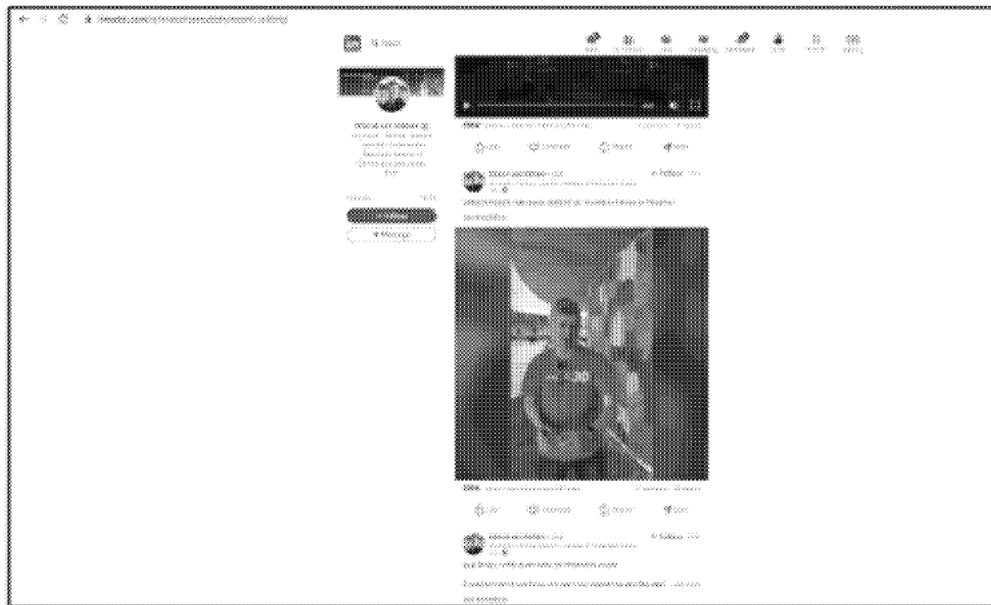


Figura 6 – Publicação LinkedIn

<https://www.linkedin.com/in/marcelvanhattem/recent-activity/>

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 41-A, § 2º, da Lei nº 9.504/97, 296 e 301 do Código Eleitoral, e 286 do Código Penal:

Art. 41-A. Ressalvado o disposto no art. 26 e seus incisos, constitui captação de sufrágio, vedada por esta Lei, o candidato doar, oferecer, prometer, ou entregar, ao eleitor, com o fim de obter-lhe o voto, bem ou vantagem pessoal de qualquer natureza, inclusive emprego ou função pública, desde o registro da candidatura até o dia da eleição, inclusive, sob

pena de multa de mil a cinqüenta mil Ufir, e cassação do registro ou do diploma, observado o procedimento previsto no art. 22 da Lei Complementar nº 64, de 18 de maio de 1990.

[...]

§ 2º As sanções previstas no caput aplicam-se contra quem praticar atos de violência ou grave ameaça a pessoa, com o fim de obter-lhe o voto. (Incluído pela Lei nº 12.034, de 2009)

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 301. Usar de violência ou grave ameaça para coagir alguém a votar, ou não votar, em determinado candidato ou partido, ainda que os fins visados não sejam conseguidos:

Pena – reclusão até quatro anos e pagamento de 5 a 15 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

A divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

O incentivo ao uso da condição patronal para exercer pressão eleitoral sobre os empregados, por outro lado, constitui forma ilegal de captação de sufrágio, categoricamente vedada pelos arts. 41-A, da Lei das Eleições, e 301, do Código Eleitoral.

Trata-se de condutas ilegais de natureza grave, com grande potencial para prejudicar a integridade do processo eleitoral que, como se sabe, somente termina com o ato de

diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41 e 41-A, § 2º, da Lei nº 9.504/97, 296 e 301 do Código Eleitoral, **DETERMINO** às plataformas Facebook, Instagram, Linkedin, Youtube, TikTok, Telegram, Twitter a imediata remoção do conteúdo mencionado nos perfis, canais e grupos abaixo relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da primeira hora após o recebimento da notificação.

Cumpra-se com urgência.

Relação de URLs:

<https://www.facebook.com/marcelvh> (Facebook)

<https://www.instagram.com/marcelvanhattem/> (Instagram)

<https://www.linkedin.com/in/marcelvanhattem/> (Linkedin)

<https://www.youtube.com/c/MarcelvanHattemOficial> (Youtube)

<https://www.tiktok.com/@marcel.vanhattem> (TikTok)

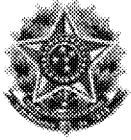
<https://t.me/marcelvanhattem> (Telegram)

<https://twitter.com/marcelvanhattem> (Twitter)

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 3 de novembro de 2022.

Marco Antonio Martin Vargas
juiz Auxiliar da Presidência do Tribunal Superior Eleitoral



04/11/2022

Número: **0601867-04.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **04/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **A Assessoria Especial de Enfrentamento à Desinformação (AEED) informa que a partir de atividades de monitoramento de dados abertos de mídias sociais detectou, nesta data, a realização de manifestações públicas em publicações no perfil @TomRiplay07 (<https://twitter.com/TomRiplay07>) na plataforma Twitter baseadas em afirmações falsas ou gravemente descontextualizadas, que atingem a normalidade e a integridade as eleições, incentivando a recusa dos resultados das Eleições 2022 e fazendo apologia a um golpe militar.**

Documentos extraídos do SEI 16002-0

Segredo de justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
15834 2535	04/11/2022 19:39	<u>Decisão</u>	Decisão

index: PETIÇÃO CÍVEL (241)-0601867-04.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601867-04.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

**RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL**

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação (AEED), acerca de manifestações públicas realizadas pelo perfil Tom Riplay.2 (@TomRiplay07) que atingem a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas acusações de fraude, a recusa dos resultados e intervenção militar.

A AEED destacou as seguintes publicações, a título exemplificativo, das quais se depreendem as desinformações e manifestações antidemocráticas:



No vídeo acima, o manifestante afirma "Temos uma excelente notícia. Dentro dos quartéis os altos comandos querem e já é cogitado a intervenção. A única coisa que ainda está sendo trabalhada é a questão internacional. Como que a visão internacional vai olhar para o Brasil após essa intervenção militar. Então, senhores, está vindo. Isso eu posso garantir aos senhores. Só que tem um detalhe, igual o capitão falou, precisa do povo na rua. A ordem é: vamos organizar. [...]".



No vídeo acima, são feitas as seguintes afirmações em espanhol: Nossas eleições foram fraudadas e Alexandre de Moraes, que se encontra no STF, ajudou Lula a roubar a vitória. Não aceitamos um ladrão como nosso presidente.





No vídeo acima, o manifestante faz as seguintes declarações: "Pessoal do Paraná que me conhece, Cabo Correia, sabe que não estamos de brincadeira. O papinho de levantar a bandeira como se fosse jogo da seleção brasileira acabou. O limite do povo brasileiro acabou. Os Ministros do STF, eu mando recado e falo mesmo, o vagabundo do Moraes, o babaca do Barroso, aquela corja todinha de vagabundo, não tenho medo de falar, são tudo pilantra safado, colocado lá pelo PT para acabar com a nossa nação. Nós vamos morrer pela pátria, nós vamos levar o V da vitória, porque o Brasil jamais terá uma bandeira com qualquer mancha vermelha

causada pelo comunismo. Brasil acima de tudo, Deus acima de todos”.

A AEED ressaltou, ainda, que o perfil realizou mais de cinquenta publicações de incentivo às manifestações antidemocráticas em curso no país apenas na manhã do dia 4/11/2022 e é seguido por 17.300 pessoas.

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

É evidente que as publicações possuem potencial para tumultuar o processo eleitoral, na medida em que discursos pró-ruptura incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Convém assinalar, em acréscimo, a significativa repercussão do material ilícito, na medida em que o perfil é seguido por milhares de pessoas e os conteúdos são postados com intensidade.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato da diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249, 286 e 296 do Código, de ordem, **DETERMINO** ao Twitter a imediata remoção do perfil @TomRiplay07 (<https://twitter.com/TomRiplay07>), sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 4 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

index: PETIÇÃO CÍVEL (241)-0601864-49.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601864-49.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL



RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação (AEED), acerca de manifestações públicas que atingem a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas acusações de fraude, a recusa dos resultados e intervenção militar.

A título exemplificativo, colacionam-se algumas das publicações destacadas pela AEED, das quais se depreendem informações falsas e manifestações anti-democráticas:



 **Saul Christos** 
@saulchristos

A PRF deu a dica: a paralisação pode continuar às margens da rodovia. Faz sentido, pois os caminhoneiros não precisam bloquear estradas, basta cruzarem os braços e terem o apoio da população.

Translate Tweet




PRF // INFORMA

A PRF RJ informa que foi exarada decisão da Justiça Federal do Rio de Janeiro que concede liminar determinando a liberação das rodovias federais interditadas por pessoas e veículos, sendo obrigatório o imediato cumprimento por parte dos manifestantes.

A decisão prevê multa pecuniária diária no valor de R\$ 5.000,00 por pessoa física participante e de R\$ 100.000,00 por pessoa jurídica que lidere ou preste apoio ao movimento.

Informamos também que é assegurado o direito de manifestação, mesmo às margens da rodovia, desde que não cause prejuízo à segurança viária e ao direito de circulação dos demais usuários da rodovia.


@prfficial
@prfbrazil

PRF  **191**

7:16 AM · Nov 1, 2022 · Twitter for Android

5,690 Retweets **216** Quote Tweets **15.6K** Likes

 **Pavão Misterious**  
@pavao911

**Fox News anuncia que Biden e CIA estão envolvidos na fraude das eleições brasileiras.
Os togado e a Esquerda estão arrumando confusão muito séria.
Só falta um relatório.**

[Translate Tweet](#)

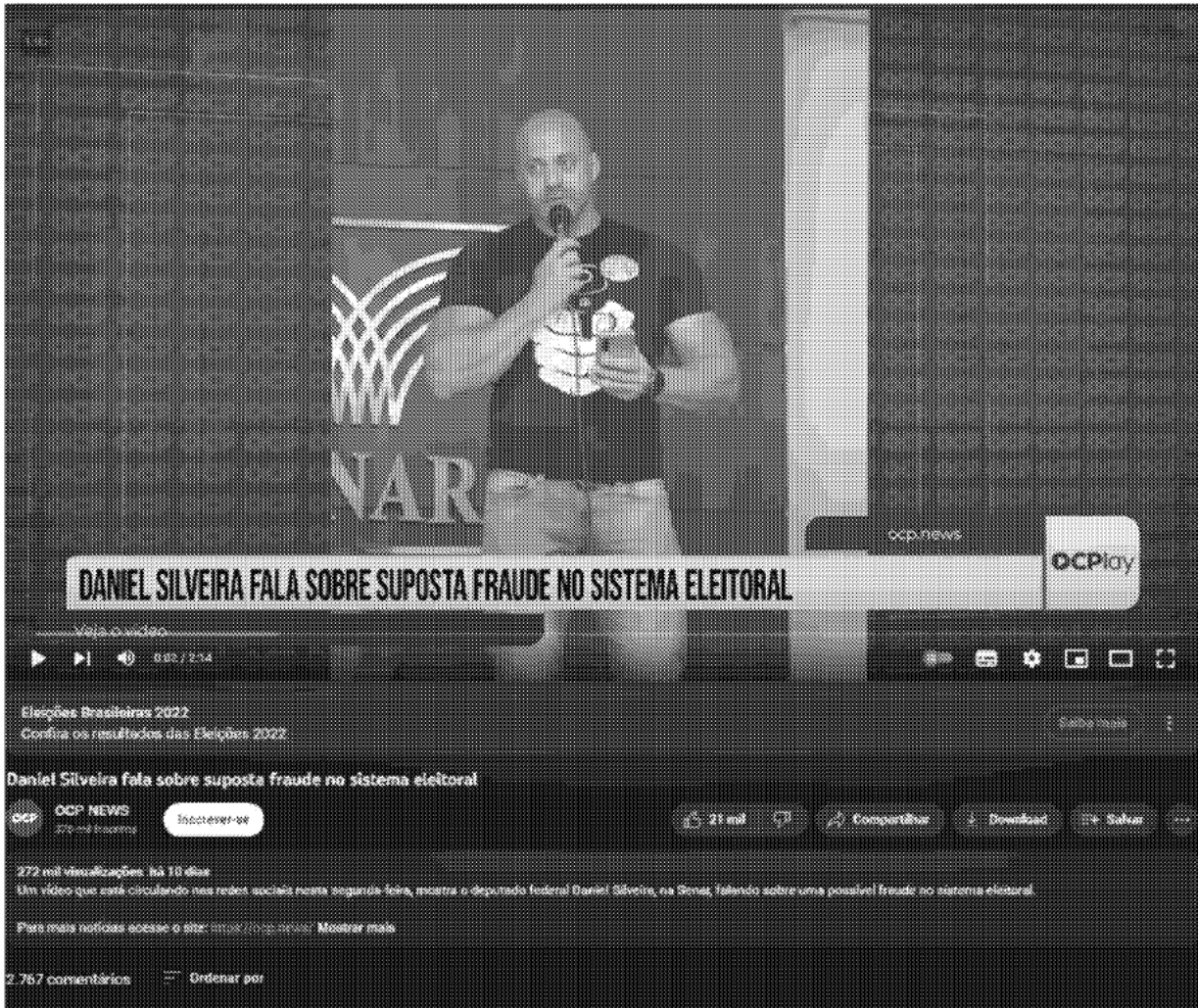


9:25 AM · Nov 3, 2022 · Twitter for Android

4,210 Retweets **169** Quote Tweets **11.9K** Likes

Conforme informação das AEED, no vídeo abaixo, o ex-Deputado Federal, Daniel Silveira, aduz que os eleitores gastariam cerca de 10 segundos para serem habilitados pelos mesários e votar em todos os cinco cargos em disputa. O argumento é utilizado para sugerir aos interlocutores que o curto tempo levado pelo eleitorado na votação seria um indicativo de fraude

no sistema eleitoral. A alegação já foi desmentida pelo TSE na página Fato ou Boato: <https://www.justicaeleitoral.jus.br/fato-ou-boato/chechagens/ex-deputado-federal-propagandimentas-sobre-tempo-de-votacao-e-inquerito-da-pf-sobre-urnas-e-leitro-ni-cas/#>



Já o *post* a seguir sustenta que o General Paulo Sérgio Nogueira afirma que "houve fraude no primeiro turno das eleições" e que Jair Bolsonaro "resolveu apostar no segundo turno achando que ia conseguir conter o sistema". Contudo, o vídeo é falso, uma vez que não é o ministro que aparece nas imagens, conforme verificado por agências de checagem parceiras do TSE:

<https://www.aosfatos.org/noticias/video-nao-mostra-ministro-da-defesa-dizendo-que-houve-fraude-na-eleicao/>

<https://politica.estadao.com.br/blogs/estadao-verifica/ministro-da-defesa-embaixador-da-franca/>



Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

É evidente que as publicações possuem potencial para tumultuar o processo eleitoral, na medida em que discursos pró-ruptura incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Convém assinalar, em acréscimo, a significativa repercussão do material ilícito, que já conta com milhares de interações em cada uma das plataformas, com potencial para reunir um número ainda maior de pessoas no decorrer dos dias que seguem.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato da diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

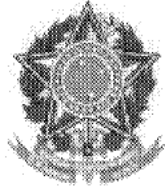
Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249, 286 e 296 do Código, de ordem, **DETERMINO** ao Twitter, Facebook, Instagram, Youtube, Kwai, TikTok e Gettr a imediata remoção dos perfis listados no documento anexo, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 4 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

**TRIBUNAL SUPERIOR ELEITORAL****PETIÇÃO CÍVEL (241) Nº 0601872-26.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL****RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL****DECISÃO**

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que reporta a criação de novo perfil, pelo influenciador Gustavo Gayer, na plataforma Twitter, em franco descumprimento a determinação dessa Corte, que ordenou a remoção de seu perfil original em virtude da propagação de desinformação e pela incitação de atos a favor de uma ruptura institucional.

Eis o perfil consignado no termo em questão:

URL: <https://twitter.com/GugaGayer>



Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

Nos termos do art. 4º, parágrafo único, da Res.-TSE nº 23.714, a determinação de remoção das redes compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, assim como a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347, do Código Eleitoral.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º e 4º, parágrafo único, da Res.-TSE nº 23.714/2022, **DETERMINO** à plataforma Twitter a imediata remoção do perfil relacionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

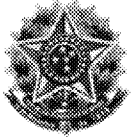
Após, **ENCAMINHEM-SE** cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 22 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral







05/11/2022

Número: **0601875-78.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **05/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Extraído do SEI 2022.00.000016089-5**

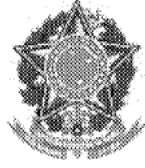
Segredo de justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data	Documento	Tipo
158347943	05/11/2022 14:20	<u>Decisão</u>	Decisão

index: PETIÇÃO CÍVEL (241)-0601875-78.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601875-78.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que detectou, nesta data, a replicação de vídeos de uma *live* sensacionalista, realizada na data de 4 de novembro nas plataformas Twitch e Youtube, com a apresentação de acusações vagas e sem provas, que atingem a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas afirmações de fraude, a recusa dos resultados e, eventualmente, uma ruptura institucional.

A *live* em questão distorce dados relacionados ao funcionamento das urnas eletrônicas e, conforme matéria publicada pelo jornal O Estado de São Paulo, baseia-se em um “dossiê apócrifo [...] repleto de informações falsas” [Link para o Estadão].

As manifestações em questão foram realizadas nos seguintes canais e perfis do Youtube:

Nome do perfil ou canal	URL do perfil ou canal	URL da postagem
Cortes do LocoBaltar	https://www.youtube.com/channel/UCZul8hAJCBu3ebopfS1OZw	https://www.youtube.com/watch?v=yV0KJbGTTZQ https://www.youtube.com/watch?v=73fynurQLW8
* Vídeo privado -		
Patriota Cruzeiro do Sul	https://www.youtube.com/channel/UCbTqzGyPntaGVEakogdeSOg	https://www.youtube.com/watch?v=ohvgVyAONTo
Pastor Luciano Monteiro	https://www.youtube.com/channel/UCbTqzGyPntaGVEakogdeSOg	https://www.youtube.com/watch?v=i6n81eNVGnE
Edson Passos	https://www.youtube.com/user/EdTi19	https://www.youtube.com/watch

SIGILOSO

B r u n n o Marques	https://www.youtube.com/channel/UC3Mdf9Gy9OKLgW9k3OPI_6A	?v=6_p2nyi3x0c https://www.youtube.com/watch?v=KlAnTVQNbp8
Raiam Santos	https://www.youtube.com/c/R2Raiam	https://www.youtube.com/watch?v=uBo_zbBwZDY
Thiago	https://www.youtube.com/c/FortinhoTV	https://www.youtube.com/watch?v=DMOWFnRAask
Bertoldi	https://www.youtube.com/c/PequenoEmpreendedor	https://www.youtube.com/watch?v=xkUQ9D8n-og

Além disso, o vídeo ilegal tem sido amplamente repercutido na plataforma Twitter, pelos seguintes usuários:

Usuário	URL do perfil ou canal	URL da postagem
C a n a l Hipócritas	https://twitter.com/CanalHipocritas	https://twitter.com/CanalHipocritas/status/1588640230118412288
F á b i o Talhari	https://twitter.com/FabioTalhari	https://twitter.com/FabioTalhari/status/1588638756428738561
A Voz do Povo	https://twitter.com/MariMir24539700	https://twitter.com/MariMir24539700/status/1588640421735198720
G u s t a v o Grein	https://twitter.com/gustavo_grein	https://twitter.com/gustavo_grein/status/1588638551322787845
E v a Rezende	https://twitter.com/rezende_eva	https://twitter.com/rezende_eva/status/1588676714405646336?s=20&t=w7l
D r i k a Moraes 0809	https://twitter.com/drikamoraes0809	https://twitter.com/drikamoraes0809/status/1588694115428233216?s=20&t
L u c i u s Cubilucarius	https://twitter.com/Luckam1955	https://twitter.com/Luckam1955/status/1588714260993302531?s=20&t=w7l
Elislyca	https://twitter.com/Elislyca	https://twitter.com/Elislyca/status/1588658791306137600?s=20&t=w7FaziC

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de

SIGILOSO

comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o processo eleitoral, na medida em que incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Ao contrário das acusações plasmadas na transmissão em tela, as urnas eletrônicas são confiáveis e seguras, tal como confirmado, reiteradamente, por inúmeros testes públicos e

procedimentos de auditoria:

<https://www.tse.jus.br/comunicacao/noticias/2021/Outubro/urna-eletronica-relatorio-do-tcu-diz-que-equipamento-e-seguro-e-auditavel>

<https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tcu-apresenta-a-corte-eleitoral-dados-parciais-de-auditoria-realizada-em-boletins-de-urna-das-eleicoes-2022>

<https://www.tse.jus.br/comunicacao/noticias/2022/Maio/tps-2021-comissao-avaliadora-divulga-relatorio-final>

<https://www.tse.jus.br/comunicacao/noticias/2022/Agosto/universidades-validam-nova-urna-e-codigos-fonte-dos-sistemas-eleitorais-357621>

As inverdades noticiadas, portanto, configuram condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Twitter e Youtube a imediata e definitiva remoção dos canais e perfis acima mencionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

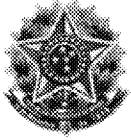
Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 5 de novembro de 2022.

MARCO ANTONIO MARTIN VARGAS

Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOS



08/11/2022

Número: **0601877-48.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **05/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

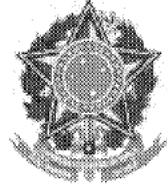
Objeto do processo: **Extraído do SEI 2022.00.000016091-7**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158354446	08/11/2022 15:34	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601877-48.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que detectou, nesta data, a replicação e a repercussão de uma *live* sensacionalista com a apresentação de acusações vagas e sem provas, que atingem a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas afirmações de fraude, a recusa dos resultados e, eventualmente, uma ruptura institucional.

A *live* em questão distorce dados relacionados ao funcionamento das urnas eletrônicas e, conforme matéria publicada pelo jornal O Estado de São Paulo, baseia-se em um “dossiê apócrifo [...] repleto de informações falsas” [[Link para o Estadão](#)].

As manifestações em questão foram realizadas nos seguintes canais do Youtube:

CANAL	URL
Investidor no Japão	https://www.youtube.com/c/InvestidornoJap%C3%A3o
UCB União Conservadora Brasileira	https://www.youtube.com/watch?v=12Priaa4sV0
Kaká Souza	https://www.youtube.com/watch?v=oDGCKFU72d0
Pedagogo Soares	https://www.youtube.com/watch?v=r4FEA-5T2qU

SIGILOSO

Monark	https://www.youtube.com/c/monark
A Bordo PodCast	https://www.youtube.com/c/ABordoPodCast
De Olho em Portugal	https://www.youtube.com/channel/UCd2-It35JvaAnfgRGSpKQbQ
Michell D'Oliveira	https://www.youtube.com/channel/UCG7toQstkyB96MxtEHY_rIw
Raphael Grego	https://www.youtube.com/user/MrRafloide

Além disso, o vídeo ilegal tem sido amplamente repercutido na plataforma Twitter, pelos seguintes usuários:

Usuário	URL do perfil ou canal
La Derecha Diario	https://twitter.com/laderechadiario
Michelle Bolsonaro Liberdade e Notícias	https://twitter.com/MichelleBols0n

Reproduções do mesmo vídeo também foram identificadas no Facebook:

<https://www.facebook.com/cortespcortes1.0/videos/630233831943711/>

<https://www.facebook.com/motovlo021/videos/2006074889585787/>

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

SIGILOSO

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o processo eleitoral, na medida em que incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Ao contrário das acusações plasmadas na transmissão em tela, as urnas eletrônicas são confiáveis e seguras, tal como confirmado, reiteradamente, por inúmeros testes públicos e procedimentos de auditoria:

<https://www.tse.jus.br/comunicacao/noticias/2021/Outubro/urna-eletronica-relatorio-do-tcu-diz-que-equipamento-e-seguro-e-auditavel>

<https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tcu-apresenta-a-corte-eleitoral-dados-parciais-de-auditoria-realizada-em-boletins-de-urna-das-eleicoes-2022>

SIGILOSO

<https://www.tse.jus.br/comunicacao/noticias/2022/Maio/tps-2021-comissao-avaliadora-divulga-relatorio-final>

<https://www.tse.jus.br/comunicacao/noticias/2022/Agosto/universidades-validam-nova-urna-e-codigos-fonte-dos-sistemas-eleitorais-357621>

Nesse norte, o conteúdo da *live* mencionada já foi desmentido por agências de checagens de fato:

<https://www.aosfatos.org/noticias/site-argentino-mentiras-urna-eletronica/>

[Auditoria na Argentina comprova fraude nas urnas brasileiras e é apresentada em live #boato \(boatos.org\)](#)

As inverdades noticiadas, portanto, configuram condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Facebook, Twitter e Youtube a imediata e definitiva remoção dos canais e perfis acima mencionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

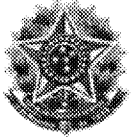
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 8 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO



06/11/2022

Número: **0601881-85.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **06/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **SEI 16096-8**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158349295	06/11/2022 11:53	<u>Decisão</u>	Decisão



MARISA LOBO PSIC. @marisa_lobo · 15h

...

Explica isso
XANDÃO!!!!

Bolsonaro em São Gabriel da cachoeira em 27/05, onde obteve ZERO VOTOS????

#BrazilWasStolen



375

4,869

18.9K



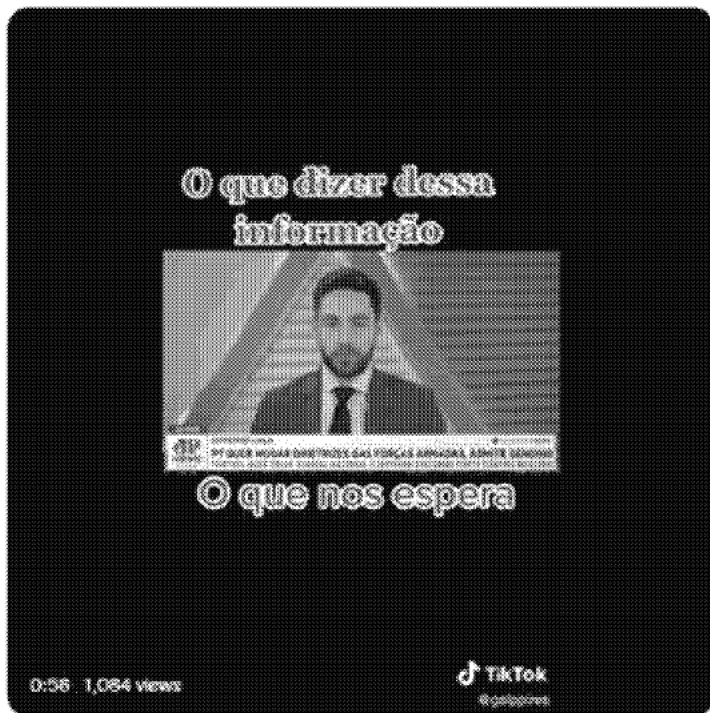
SIGI

SIGILOS



MARISA LOBO PSIC. @marisa_lobo · Nov 4
Então, o que dizer dessa informação? @fab_oficial @exercitooficial @DefesaGovBr @JusticaGovBR, Vocês vão aceitar?

...



👁️ 1 🗨️ 41 ❤️ 🍷 📤

SIGILO



SIGILOSO



MARISA LOBO PSIC. @marisa_lobo · 15h

...

O mundo já sabe, a vergonha que está acontecendo em nosso País.
#FRAUDE



4

45

106



SIGILO

SIGILOSO



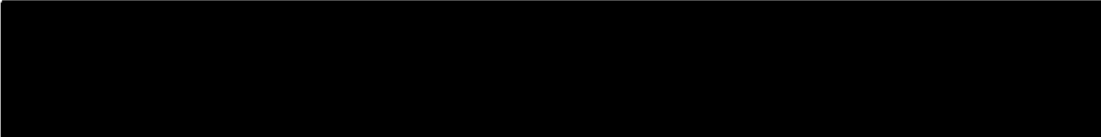
MARISA LOBO PSIC. @marisa_lobo · Nov 3

Curitiba agora a noite..... não vou falar o que eles estão fazendo lá na frente do batalhão não. 🇨🇮 🇨🇮



👁️ 28 🗨️ 363 ❤️ 1,464 🔄

SIGILOSO



SIGILOSO



MARISA LOBO PSIC. @marisa_lobo · Nov 3

...

Lula tem menos da metade dos seguidores do Presidente @jairbolsonaro .
Os dados "fantasiosos " não encontram Lógica nos números.
#Resistênciaconservadora.



Influenciadora: Marisa Lobo


Rede social: Twitter

Número de seguidores: 108.3 mil

URL:https://twitter.com/marisa_lobo


SIGILOSO

Num. 158349295 - Pág. 6

Vitor Hugo  @MajorVitorHugo · Nov 4 ...


Estatísticos e galera de TI de todo País precisam tb se debruçar sobre o que os argentinos apresentaram. A identificação de padrões nos resultados não pode ser ignorada, já que o melhor interesse de TODOS nós é que o resultado das urnas espelhem a vontade dos eleitores, né, não?

 875  3,566  16.5K 

Vitor Hugo  @MajorVitorHugo · Nov 4 ...

Não se trata mais de auditoria nas URNAS, mas de estudo profundo dos RESULTADOS. Muito grave essa diferença apresentada entre urnas auditadas e não auditadas e a subsequente identificação de padrões estatísticos improváveis. Eles lá terão pressa pra checar essas conclusões tb?!

 69  775  3,729 

Vitor Hugo  @MajorVitorHugo · Nov 4 ...

Queremos o melhor para o País e a certeza de que a vontade soberana do povo brasileiro esteja representada nos resultados das urnas. É pedir muito?!

 57  405  2,455 

Influenciador: Major Vitor Hugo

Rede social: Twitter

Número de seguidores: 412.2 mil

URL: (20) Vitor Hugo (@MajorVitorHugo) / Twitter

SIGILOSO



CORONEL TADEU @CoronelTadeu · Nov 4
Gracias Fernando



Fernando Cerimedo @FerCerimedo_ok · Nov 4
La verdad por sobre todo/A verdade sobre tudo.
#Brazilwasstolen

Stay informed

Learn more about why election experts say civic processes in Brazil are safe and secure. Find out more

20

137

1,140



CORONEL TADEU @CoronelTadeu · Nov 4



O que você prefere:
Viver num regime militar ou num regime de criminosos e comunistas ?

Hay que ser firme ahora

2,169

3,121

18.4K



SIGILOSO



CORONEL TADEU @CoronelTadeu · Nov 3

...

Recado



980

7,183

25.5K



SIG

SIGILOSO

CORONEL TADEU @CoronelTadeu · Nov 3

Qual a sua opinião sobre as declarações do General Mourão?
 Você concorda com ele ou não? Nós estamos chorando ou questionando?
 Siga @coroneltadeu nas redes.



Imagem do vice-presidente Hamilton Mourão - Getty Images

Brasil

GENERAL MOURÃO SE PRONUNCIA SOBRE ELEIÇÃO DE LULA: 'NÃO ADIANTA MAIS CHORAR'

CORONEL TADEU @CoronelTadeu · Nov 2

São imagens impressionantes.
 Se todos os trabalhadores pararem ao policiais e as GCM não darão conta.
 O exército terá que fazer alguma coisa.



1,312 10.4K 22.6K

Influenciador: Coronel Tadeu

Rede social: Twitter

Número de seguidores: 77.4 mil

URL: <https://twitter.com/CoronelTadeu>

SIGILOSO

SIGILOSO

SIGILOSO

↳ Fernando Cerimedo Retweeted



Fernando Cerimedo @FerCerimedo_ok · 9h

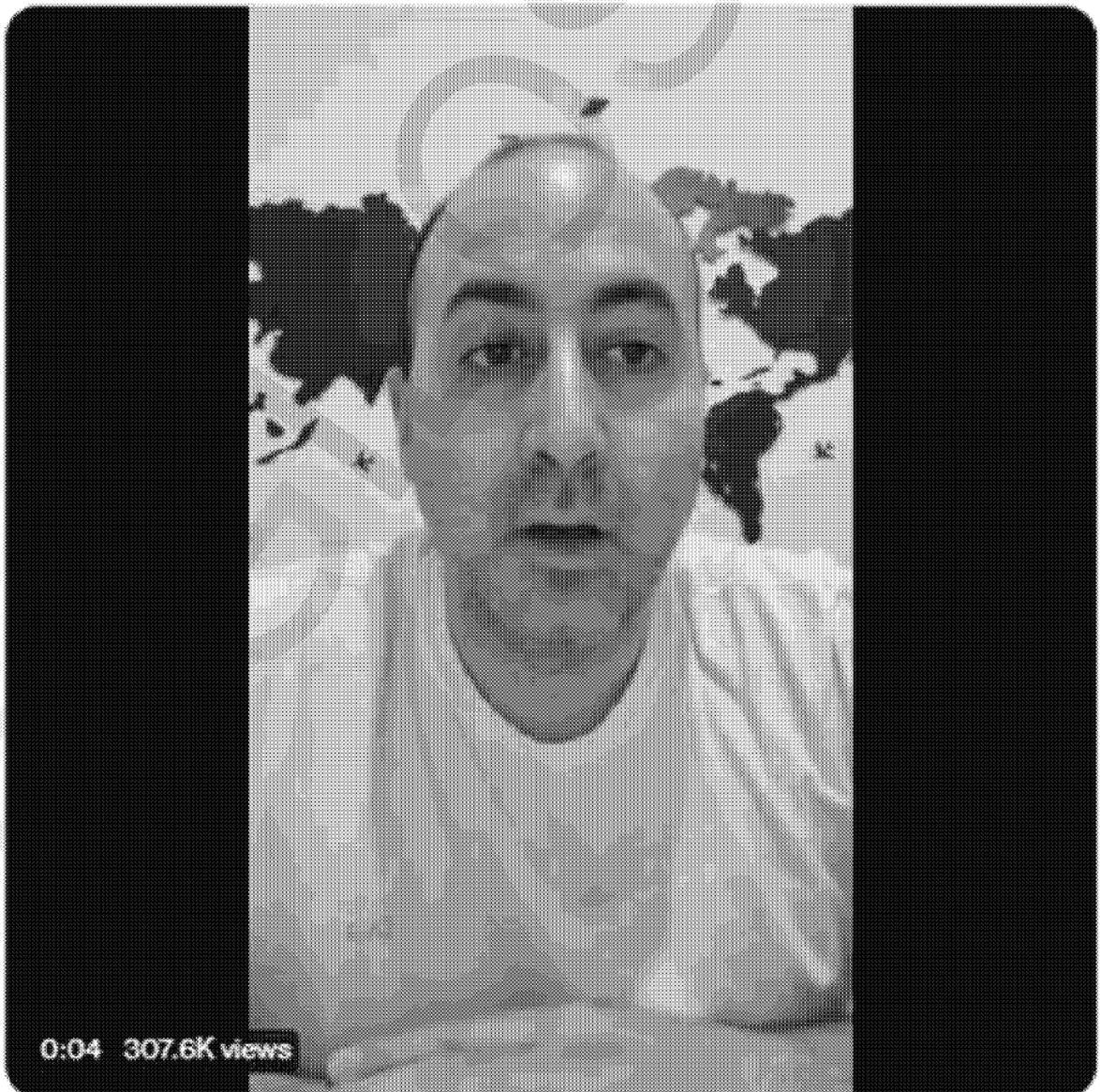
...

📺 Amanhã 12:00hs vou fazer uma LIVE com novas informações

- Auditoria completa da segunda volta
- Relação do META com TSE
- Auditorias sem fazer
- Modificação de arquivos

e muito mais!!!!

Não percam. Em breve postarei o link.



💬 2,134

↳ 21.8K

❤️ 59.4K



SIGILOSO

Fernando Corimedo Retweeted

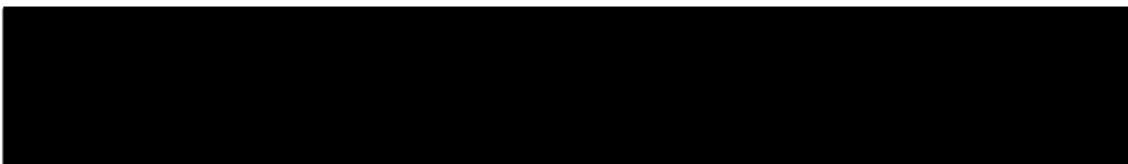


Flavia Magalhães @FlaviaMSouza76 · 12h
Hoje, dia 05/11/2022

MIAMI



124 1,864 8,369



SIGILOSO



Fernando Cerimedo @FerCerimedo_ok · 9h

Hablan de FALSAS SOSPECHAS. Como una sospecha es falsa?? es sospecha y tiene que comprobarse si es así o no. No pudieron eliminarlo, millones lo vieron y replicaron. Y hoy MILES de personas hicieron el mismo trabajo de auditoría, con mismos resultados.

LA NACION @LANACION · 9h

Suspenden en Brasil un video de un consultor argentino por divulgar fake news sobre las elecciones lanacion.com.ar/el-mundo/suspe...



147

1,347

5,960



Influenciador: Fernando Cerimedo

Rede social: Twitter

Número de seguidores: 151.4 mil

URL: https://twitter.com/FerCerimedo_ok

SIGILOSO



Jornal Direita @jornaldireitaOK · Nov 4

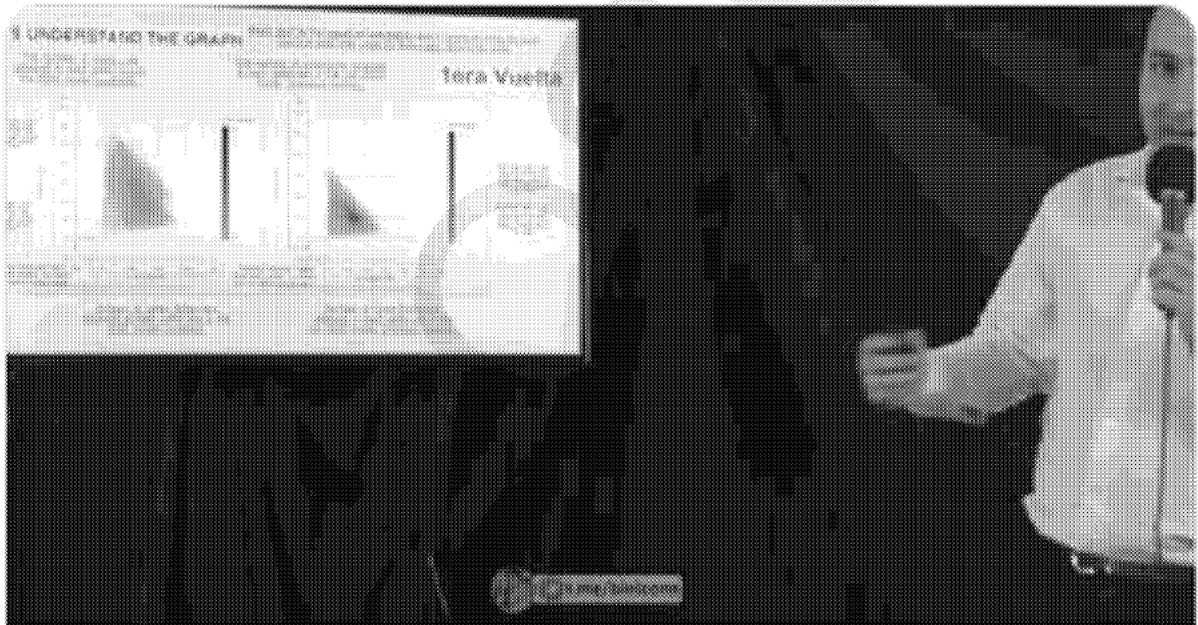
...

| A transmissão completa de #BrazilWasStolen no link de Rumble.

Link:

Stay informed >

Learn more about why election experts say civic processes in Brazil are safe and secure. Find out more



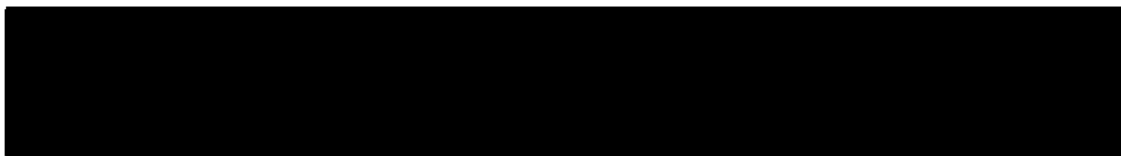
rumble.com

Auditoría dos Argentinos sobre as eleições brasileiras

146

2,715

7,505



SIGILOSO

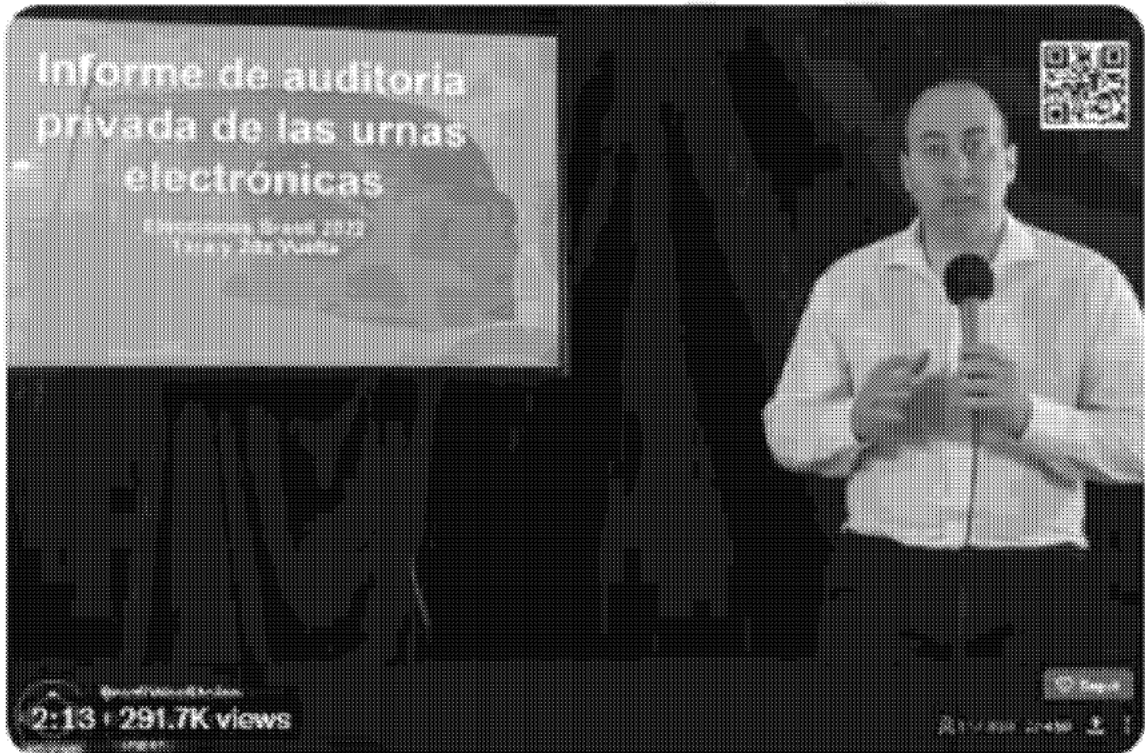


Jornal Direita @jornaldireitaOK · Nov 4

...

📺 | Em tempo recorde todas as transmissões de #BrazilWasStolen foram censuradas. Neste link do Google Drive estão os documentos e o vídeo completo da conferência.

Link: drive.google.com/drive/folders/...



🔔 Stay informed

Learn more about why election experts say civic processes in Brazil are safe and secure. Find out more

👤 593

🔄 9,124

❤️ 24.8K



SIGILOSO

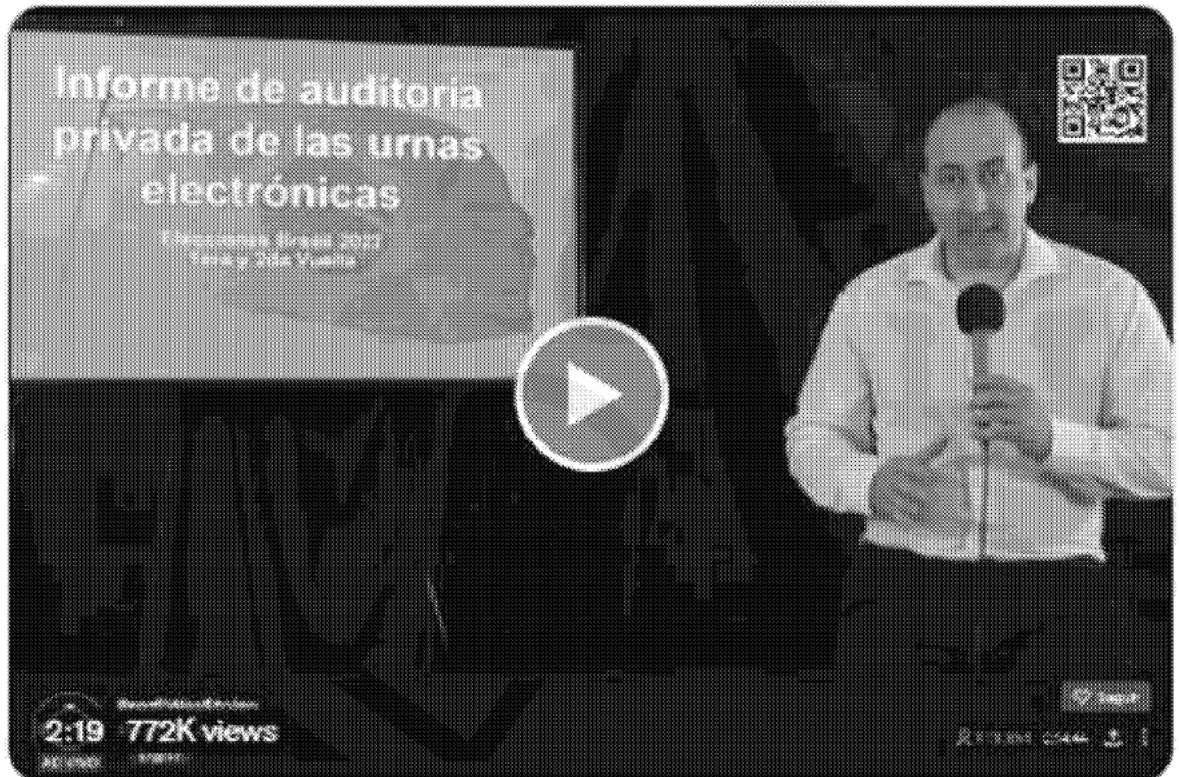


Jornal Direita @jornaldireitaOK · Nov 4

...

📺 | O vídeo da auditoria das eleições brasileiras censurado na internet
#BrazilWasStolen

PARTE 1/5



From Jamile DeSouza-Davies

Stay informed

Learn more about why election experts say civic processes in Brazil are safe and secure. Find out more

1,042

17.3K

48.3K



Show this thread

Influenciador: Jornal Direita

Rede social: Twitter

Número de seguidores: 11.7 mil

URL: <https://twitter.com/jornaldireitaOK>

SIGILOSO

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à ruptura institucional, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o

SIGILOSO

processo eleitoral, na medida em que incentivam ou conferem subsídios argumentativos para comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma Twitter a imediata remoção dos perfis relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

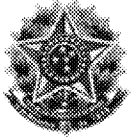
Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 6 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILO

SIGILOSO



01/02/2023

Número: **0601881-85.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **06/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

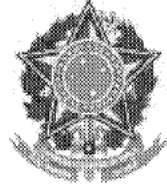
Objeto do processo: **SEI 16096-8**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158587988	31/01/2023 19:30	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601881-85.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de perfil nas redes sociais, orientado para a divulgação de desinformação contra as eleições e apologia à intervenção militar, em detrimento da vontade popular registrada nas Eleições 2022.

Por meio da decisão de ID 158349295, determinei a suspensão, entre outros casos, dos perfis identificáveis de Marisa Lobo e Fernando Cerimedo, nos seguintes termos:

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma Twitter a imediata remoção dos perfis relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Por outro lado, nos autos da Petciv 0601911-23.2022.6.00.0000, já foram liberados os perfis dos Deputados Federais Major Vítor Hugo e Coronel Tadeu, igualmente objeto do presente procedimento.

É o breve relato. Decido.

O art. 4º da Res.-TSE 23.714/2022 tutela a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação desinformações, representam substancial transgressão à própria Democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou

SIGILOSO

canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito, uma vez que, *"a desinformação - entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos - conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiança, com conseqüente perda da credibilidade e fé nas instituições da democracia representativa"* (Voto que proferi na ADI 7.261-MC, julgado em 25/10/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, *"não há direito no abuso de direito"* (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio "LIBERDADE e RESPONSABILIDADE"; não permitindo - como ocorrido nas presentes hipóteses - de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da "liberdade de expressão" como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

Considerado que houve a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral, a fim de possibilitar que os envolvidos possam retornar a utilizar suas redes sociais dentro do mais absoluto respeito à Constituição Federal e a Legislação, com observância do já citado binômio LIBERDADE – RESPONSABILIDADE, DETERMINO:

i) a reativação da conta dos perfis Marisa Lobo e Fernando Cerimedo na Plataforma Digital TWITTER, mantendo-se, porém a remoção das postagens irregulares veiculadas, considerando idêntica medida já adotada nos autos da Petciv 0601911-23.2022.6.00.0000, com relação aos Deputados Federais Major Vitor Hugo e Coronel Tadeu; e

ii) a aplicação de MULTA DIÁRIA, no valor de R\$ 20.000,00 (vinte mil reais), a incidir na hipótese de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

Por fim, iii) comunique-se a Plataforma Digital Twitter para cumprimento imediato da presente decisão; e iv) diante da pertinência temática ao Inquérito 4.879, encaminhem-se os autos ao SUPREMO TRIBUNAL FEDERAL.

Intime-se. Publique-se.

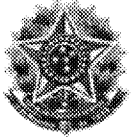
SIGILOSO

Brasília, 30 de janeiro de 2023.

Ministro **ALEXANDRE DE MORAES**
Presidente

SIGILOSO

SIGILOSO



08/11/2022

Número: **0601889-62.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **07/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Documentos extraídos do SEI n. 16116-6.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158353339	08/11/2022 15:32	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601889-62.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de manifestações públicas realizadas por grandes influenciadores digitais que atingem a integridade e a normalidade do processo eleitoral, incentivando, direta ou indiretamente, com base em afirmações falsas, a recusa dos resultados e a perpetuidade de movimentos antidemocráticos que buscam uma ruptura institucional.






As manifestações em questão foram realizadas na plataforma Twitter, como se vê:

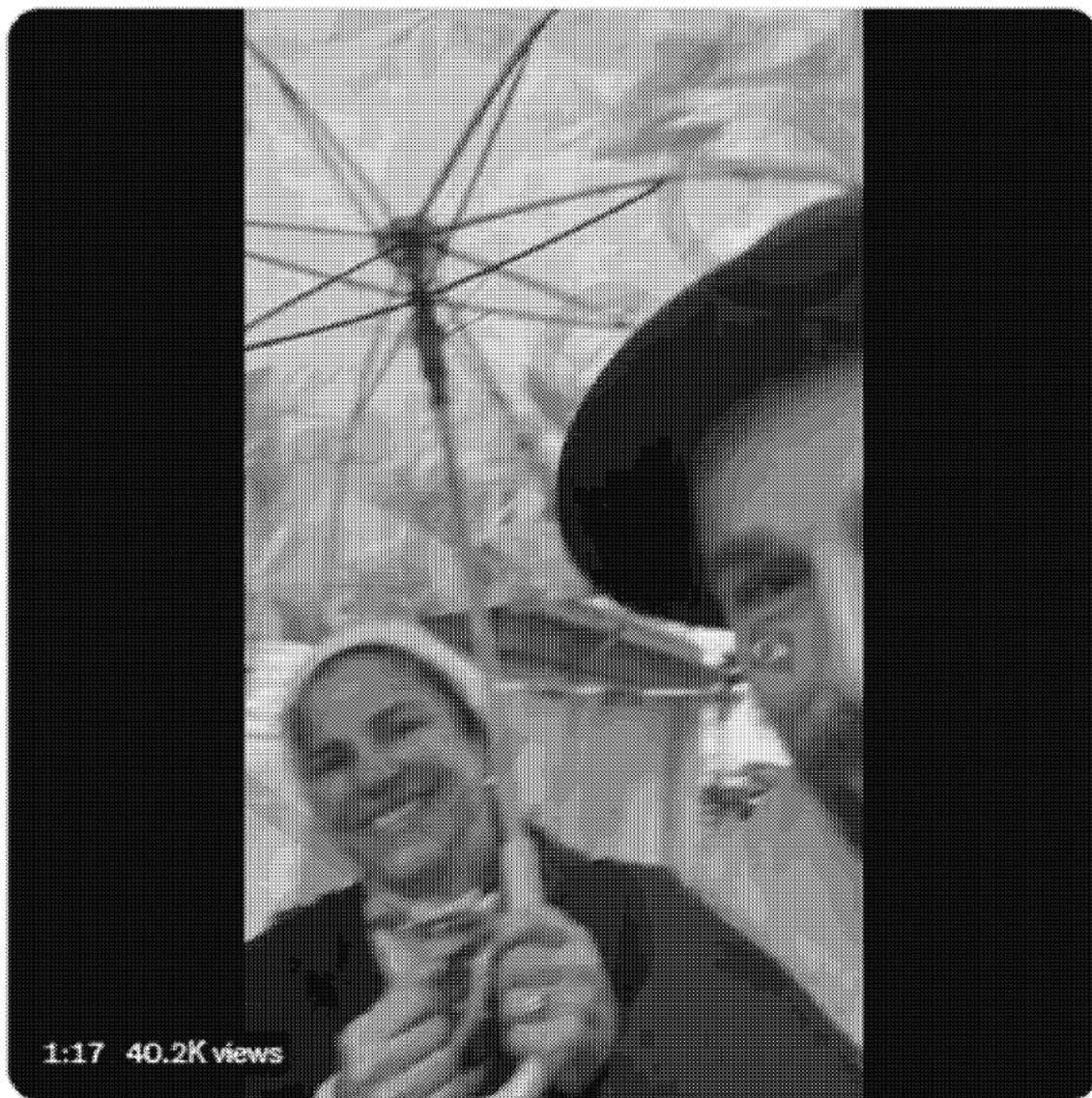
SIGILOSO



Alexandre Kunz @AlexandreKunz4 · 20h

...

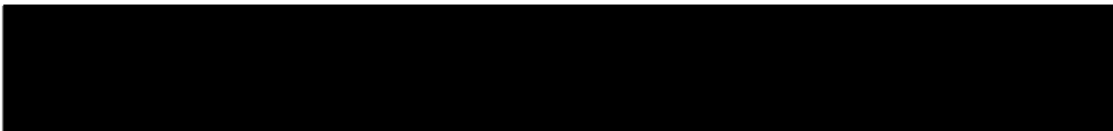
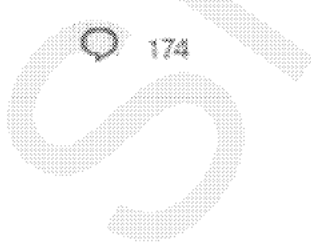
Londres, 06/11/2022 Embaixada do Brasil! Venceremos     
@exercito_oficial Intervenção federal no Brasil.



174

2,771

6,766



SIGILOSO

Alexandre Kunz Retweeted



Jamile DeSouza-Davies @JamileDavies · Nov 5

O MUNDO esta falando sobre o que esta acontecendo no BRASIL!
Não parem! 🇺🇸🇧🇷🇺🇸

The world is talking about what's happening in Brazil!
We will not stop! 🇺🇸🇧🇷🇺🇸

@exercitooficial SALVE o nosso país!
#Brasil



117 2,592 4,783

SIGILO

SIGILOSO



Alexandre Kunz @AlexandreKunz4 · Oct 30

...

Artigo 142, essa lei foi feita para ser usada em certo momento!

Seria essa a hora ? Presidente @jairbolsonaro vc é nosso líder, de um norte para nós o quanto antes por favor.

Só para avisar que meu post foi excluído! Deus nos dê forças e direção.



90.8K views



278



3,163



14K



Alexandre Kunz @AlexandreKunz4 · Nov 2

...

Nós autorizamos! Nós precisamos! 🇬🇧🇬🇧 Londres está batando no mesmo ritmo do nosso querido Brasil.



236



7,747



21.4K



SIGILOSO

Influenciador: Alexandre Kunz

Rede social: Twitter

Número de seguidores: 35.3 mil

URL: <https://twitter.com/AlexandreKunz4>

 Pinned Tweet



Flavio Beall @frbeall · Nov 5
FAKE NEWS!

...

As máquinas HEXADATA ORACLE são escaláveis e não caem por excesso de demanda, essa garantia está expressa no clausulas de garantia de serviço do contrato.

O presidente do TSE não tem conhecimento de TI portanto está sendo ENGANADO por sua equipe, ou...



Flavio Beall @frbeall · 19h
Guerreiros do Brasil: Pelo amor de São TOMÁS!

...

Nas minhas mensagens aqui as ENTRELINHAS valem 10 vezes mais que as linhas.

Se esforcem para compreender antes que derrubem meu perfil, CARAMBA!!!!!!

Coronel "de Brigada" é um tipo tão diferenciado q todos ja sabem q será promovido

 106

 1,017

 6,087



SIGILOSO



Flavio Beall @frbeall · 4h

...

Como venho falando, o TSE NÃO CUMPRE os padrões de governança internacionalmente aceitos como COBIT e ITIL. Portanto NADA do que é feito ali seria JAMAIS aceito pelos EUA ou UE.

Se o sistema brasileiro fosse para uma eleição nos EUA, ou seria REJEITADO ou seria PRESO o dono.

REQUISITOS	AVALI- AÇÃO	PRINCIPAIS REFERÊNCIAS
1.12 Conformidade do TSE na Governança de TI	NC	A atuação da presente Auditoria Especial confirmou o alinhamento da gestão de TI às diretrizes do Tribunal e à preocupação de não gerar prejuízos à imagem da instituição. Contudo, se apurou descumprimento da governança de TI com relação à análise transparente das denúncias e riscos apontados pela sociedade e reiteradas auditorias. Em lugar de aprofundar avaliações abertas e apresentar resultados de forma transparente, a governança de TI se mostrou voltada à proteção da própria estrutura e não de um claro e aberto aprofundamento conjunto das investigações (Item 3.7, p. 35)
1.13 Governança de TI no licenciamento do sistema operacional da Urna	NC	Não se constatou que o TSE cumpra os termos do licenciamento do sistema operacional utilizado na Urna Eletrônica (Item 3.8, p. 37)
1.14 Governança do TSE quanto aos sistemas aplicativos	NC	Não se constatou que o TSE cumpra os termos do licenciamento do sistema operacional utilizado na Urna Eletrônica (Item 3.8, p. 37)
1.15 Governança do TSE sobre criptografia e assinatura digital	NC	O TSE aceita no sistema eleitoral a existência de código e serviços de autenticação providos pelo CEPESC, constituindo em ponto crítico de falha e eventual procedimento indevido que pode influenciar quase todas as rotinas do sistema eleitoral, além de haver subordinação do CEPESC a órgão comando por parte possivelmente interessada na eleição, contrariando princípios de governança. Apurou-se que código-fonte do CEPESC não seguiu os trâmites previstos na lacração de software. (Item 3.10, p. 46)

👍 40

👎 4

💬 4

↑

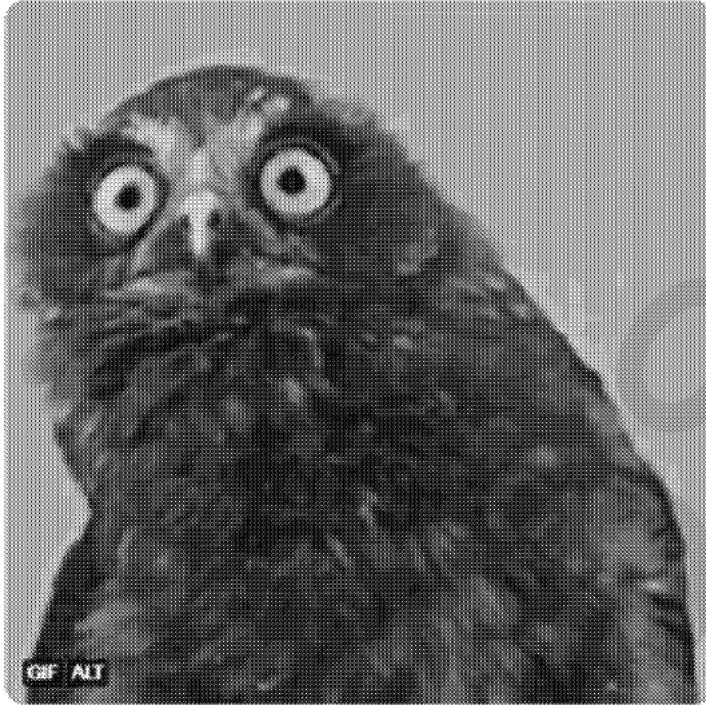
SIGILOSO



Flavio Beall @fibeall - 11h

Boa noite! A coruja buraqueira acabou de me contar que Helena de Tróia está preparando um lindo cavalo para dar de presente para o T5E.

Ela foi perguntar se o cavalo poderia ser dado logo cedo na alvorada ou se era melhor entregar depois do pôr do sol quando o urubu já dormiu...



121

646

3,232

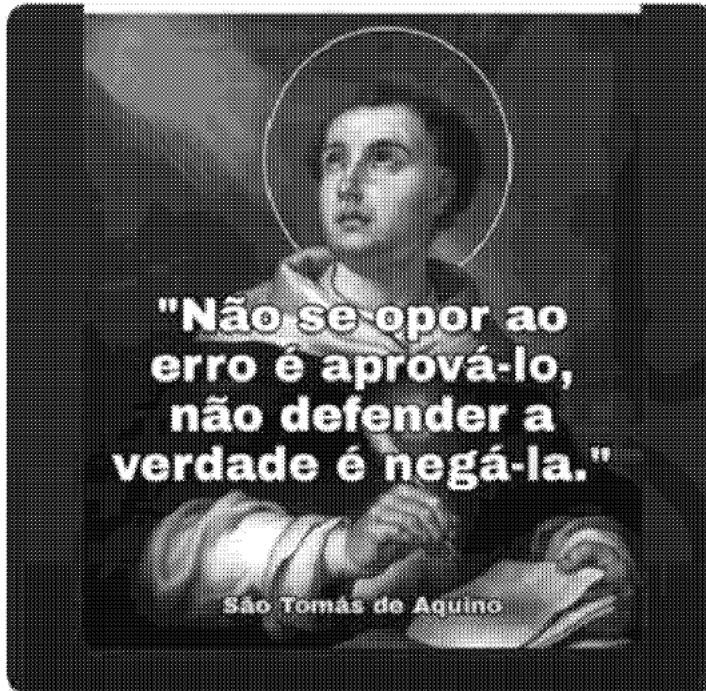




Flávio Beall @frbeall · 10h

Depois de serem expulsos das rodovias, a turma do pega-pega achou o pique, aquela pedação de chão onde não vale jogar gás lacrimogêneo nem bomba de efeito moral.

Parace que o pique é uma área 1 km em volta dos quartéis, depende de quantos jogadores estiverem brincando...



36

558

2,607



SIGILOSO

SIGILOSO

Num. 158353339 - Pág. 8



Flavio Beall @frbeall · 20h

Vende-se camisetas para o Reveillon.

Retire a sua no quartel mais próximo de sua casa.



25

276

1,067



Influenciador: Flávio Beall

Rede social: Twitter

Número de seguidores: 19.6 mil

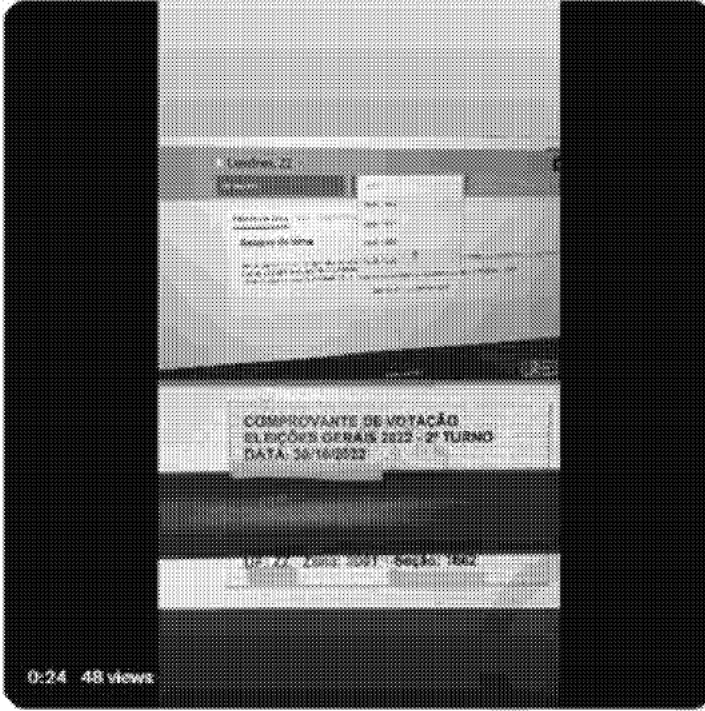
URL: <https://twitter.com/frbeall>

SIGILOSO



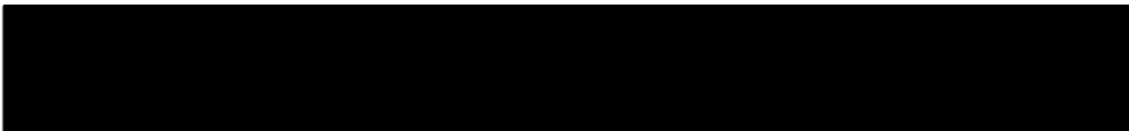
Lucelia @Lucelia057001688 · 5h

E os casos de sessões desaparecidas só aumentam



🔄 6 ❤️ 10 ↕

SIGILO



SIGILOSO



Lucelia @Lucelia05700188 · 8h

...

GREVE GERAL 07/11



5

10

17



SILO

SIGILOSO

Lucelia Retweeted



Nathalia @NaMayNo · 17h
Replying to @EdRaposo,



1 16 33

Lucelia Retweeted



Gaby Labre @GabyLabree · Nov 6

Gente a fraude no Brasil está sendo assunto no mundo inteiro, menos no Brasil, ou seja, a mídia tbm fez parte do golpe. Não tenham um pingo de dúvidas.

163 2,786 10.6K

Influenciador: Lucelia

Rede social: Twitter

Número de seguidores: 6.9 mil

URL: <https://twitter.com/Lucelia05700188>

SIGILOSO



Cris Arcangeli @crisarcangeli · 16h

Rio de Janeiro hoje!

#brasil @exercitoooficial @GeneralGirao

@foxnewspolitics



1:13 49.7K views

325

3,545

11.3K



SIGILOSO

Crís Arcangeli Retweeted



Maurício Costa @MauricioCostaRS · Nov 4

...

SEQUÊNCIA DOS FATOS:

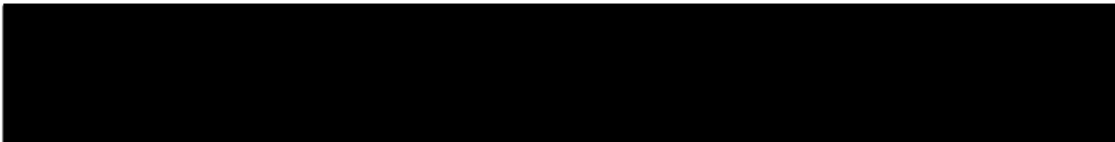
1. TSE muda status da eleição para "apurando votos"
2. Denúncia de fraude nos 5 modelos de urnas não auditáveis traz provas irrefutáveis
3. Imediatamente, após a grave denúncia, o TSE tira os dados do ar
4. Live da denúncia é derrubada...

#BrazilWasStolen

Stay informed

Learn more about why election experts say civic processes in Brazil are safe and secure. Find out more

SIGILOSO



SIGILOSO



Cris Arcangel @crisarcangel · Nov 4
Dia 7:00

Forças armadas devem apresentar resultado da auditoria das eleições 2022 na segunda (7), diz site

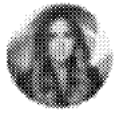
Terra Brasil Notícias novembro 4, 2022



704 1,822 10.4K

SIGILO

SIGILOSO



Cris Arcangeli @crisarcangeli · Nov 4
Shame!!!!

...



Denice Gary-Pandol for US Senate 2024 - California and 5 others

832

4,789

21.6K



Cris Arcangeli @crisarcangeli · Nov 5
Nossa!!!! meu Deus

...

Adrilles Jorge @AdrillesRJorge · Nov 4
Derrubaram a live sobre suposta inconsistências nas urnas ;
derrubaram a hashtag sobre roubo. O site do tse sumiu. Derrubando
perfis . Derrubando discussão , investigação , contestação . A
liberdade está sendo derrubada no Brasil.

64

98

908



Influenciador: Cris Acangeli

Rede social: Twitter

Número de seguidores: 205.2 mil

SIGILOSO

URL:<https://twitter.com/crisarcangeli>**Adrilles Jorge** @AdrillesRJorge · Nov 4

...

Derrubaram a live sobre suposta inconsistências nas urnas ; derrubaram a hashtag sobre roubo. O site do tse sumiu. Derrubando perfis . Derrubando discussão , investigação , contestação . A liberdade está sendo derrubada no Brasil.

3,801

16.5K

65K

**Adrilles Jorge** @AdrillesRJorge · Oct 31

...

As quatro linhas da constituição foram rompidas quando tiraram um condenado da cadeia pra ser candidato a um ano das eleições . Desde então tudo tem sido flagrantemente ilegal neste país

3,326

3,382

24.3K

**Adrilles Jorge** @AdrillesRJorge · 18h

...

Nem bem a esquerda retomou o poder e a censura já tomou conta do país, só pelo CHEIRO do poder efetivo. Línguas cortadas , mãos cortadas e olhos cegados. Tenham medo. Mas transformem seu medo em reação . Antes que o medo arranque suas línguas , olhos e mãos antes das autoridades

609

2,835

15.1K



SIGILOSO



Adrilles Jorge @AdrillesRJorge · Nov 2

...

As manifestações pelo país são gigantescas . O sentimento de indignação e revolta toma conta do país. Nunca se viu algo depois das eleições Contra o processo eleitoral . Perguntam pela pauta ? Uma justiça que seja realmente justa. Simples assim.

3,031

6,645

30.7K



Adrilles Jorge @AdrillesRJorge · 13h

...

O povo silenciado . O povo amordaçado. A liberdade silenciada no período mais sombrio da história brasileira, em que juizes e jornalistas e autoridades que falam em ataque à democracia são os próprios covardes e omissos que destroem a democracia .



From Gustavo.

1,401

11.1K

35.6K



Influenciador: Adrilles Jorge

Rede social: Twitter

Número de seguidores: 901 mil

SIGILOSO

URL <https://twitter.com/AdrillesRJorge>

← **Brazil Was Stolen**
138 Tweets



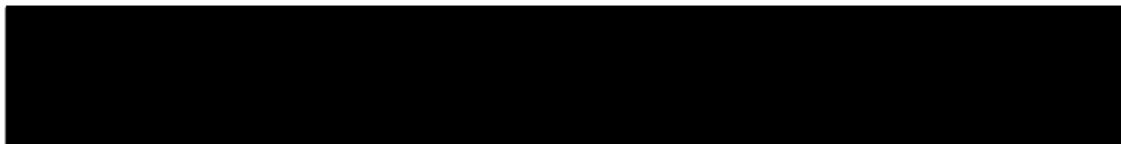
⋮ **Follow**

Brazil Was Stolen

@BrazilWasStolen

O Brasil foi roubado? Queremos saber!
Esse perfil não tem vínculo com @FerCerimedo_ok.

SIGILOSO



SIGILOSO



Brazil Was Stolen @BrazilWasStolen · 13h

...

Pessoal amanhã 07/11/22 acontece a GREVE GERAL! Nos marquem que iremos repostar.

#GreveGeral #Brasil #BrazilSpring



20

222

669



Brazil Was Stolen @BrazilWasStolen · 13h

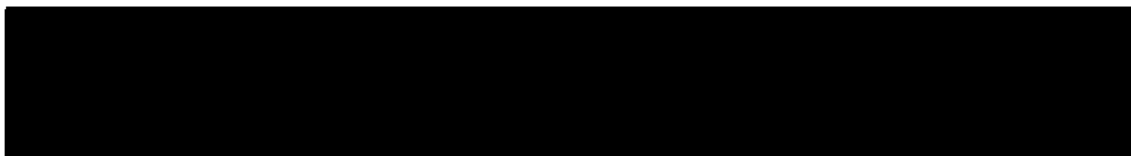
...

Qual horário de começo e término das manifestações? #BrazilianSpring #Brasil

54

22

353



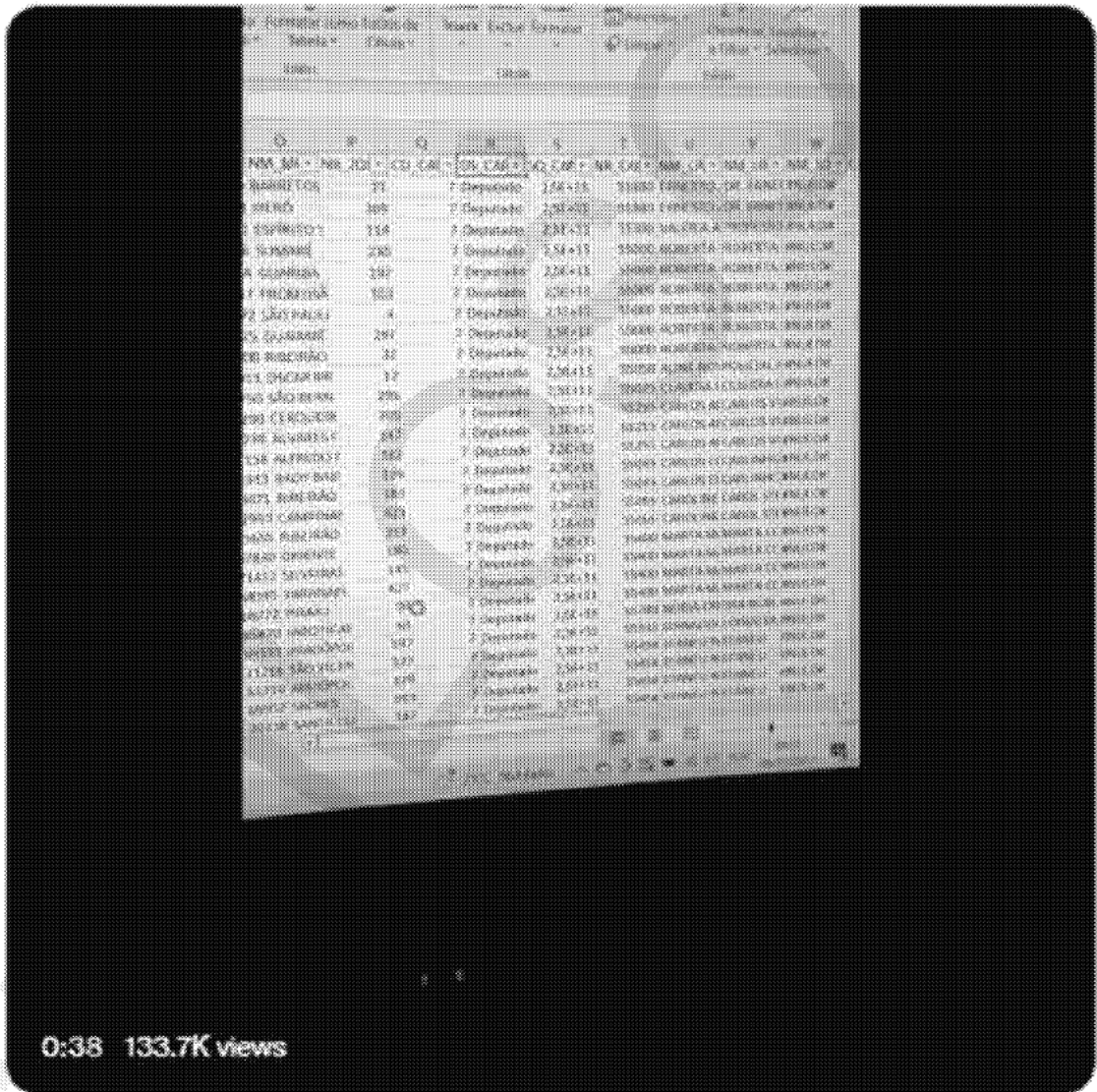
SIGILOSO

Brazil Was Stolen Retweeted



Márcio Teixeira @MrcioTe37532535 · Nov 5

Continuam fazendo manipulação... "Por favor, vejam esse vídeo! O TSE simplesmente deletou da planilha uma das cidades citadas na Live com zero votos - Quiterianópolis/CE!"...



571 10.1K 19.7K

Influenciador: Brazil Was Stolen

Rede social: Twitter

Número de seguidores: 17.1 mil

URL: <https://twitter.com/BrazilWasStolen>

SIGILOSO



Gilberto Silva @cabogilberto · Nov 4

...

Pelo que eu entendi até agora, a alegação é a seguinte:

1) Existem 6 modelos diferentes de máquinas, mas só 1 deles, o modelo de 2020, é auditado.

2) Os logs e demais dados da eleição exibem uma diferença de comportamento gritante no voto de acordo com o modelo da urna eletrônica.

17

300

1,147



Show this thread



Gilberto Silva @cabogilberto · Nov 4

...

Seção eleitoral. As pessoas estavam escolhendo ou era a máquina que estava escolhendo por ela? Se elas estavam na mesma cidade, no mesmo bairro e na mesma escola, não deveriam apresentar a mesma variação e o mesmo padrão no comportamento do voto?

1

58

262



Gilberto Silva @cabogilberto · Nov 4

...

8) Nos modelos de 2020, o Presidente vence. Nos demais modelos, o Presidente perde por 5 pontos.

Esses questionamentos precisam de explicação urgente!!

7

53

247



Gilberto Silva @cabogilberto · Nov 4

...

Entendi que as máquinas auditáveis, que são de 2020/2021 não apresentaram anormalidades já as máquinas de versões anteriores, que são as não auditáveis, aparentemente, seguem o mesmo padrão, como se respondessem através de um algoritmo.

E agora ??

23

134

665



Gilberto Silva @cabogilberto · Nov 4

...

Agora fiquei com mais dúvidas sobre todo esse processo!!!

2

18

94



SIGILOSO



Gilberto Silva @cabogilberto · 13h
A situação do Brasil é muito complicada!!!

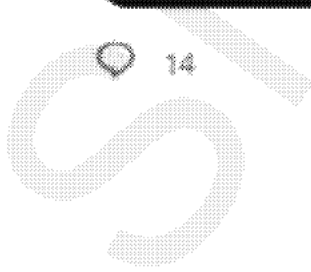
...



14

203

702



SIGILOSO

 Gilberto Silva Retweeted



José Medeiros    @JoseMedeirosMT · 19h



 321

 4,974

 14.3K



SIGILOSO



Gilberto Silva @cabogilberto · 53m

...

O senador Rodrigo Pacheco é o responsável, por não cumprir o ART 52 da CF/88 freando arbitrariedades de um dos poderes da república.



Influenciador: Gilberto Silva

Rede social: Twitter

Número de seguidores: 44.1 mil

URL: <https://twitter.com/cabogilberto>

SIGILOSO

Retweeted



José Medeiros @JoseMedeirosMT · 19h
Análise interessante.



327

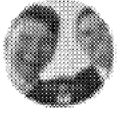
5,008

14.4K



SIGI

SIGILOS



José Medeiros @JoseMedeirosMT · Nov 6

...

Dizer que foi auditado não é desmentir, precisamos de uma explicação para o fenômeno apresentado na auditoria Argentina. TSE desmente suspeita de fraude eleitoral citada em live de argentino - Política - Estado de Minas



em.com.br

TSE desmente suspeita de fraude eleitoral citada em live de argentino
Órgão citou ao menos 5 auditorias realizadas nas urnas eletrônicas
brasileiras desde ao longo da última década, que 'não encontraram ...

81

239

823



José Medeiros @JoseMedeirosMT · 18h

...

Cada vez mais aparecem pontos de interrogação, se o site do TSE saiu do ar por excesso de demanda no dia da live, por que não saiu no dia da eleição?

143

900

3,696



SIGILOSO



José Medeiros [2/2] [🔒] @JoseMedeirosMT · 19h

...

Marido chega tarde em casa com marca de batom, perfume diferente e cheirando álcool. Esposa pede explicações ele manda ela se CALAR pois ela não tem prova de nada.

36

143

821



José Medeiros [2/2] [🔒] @JoseMedeirosMT · 19h

...

Meu Deus!!!!

Brazil enDireita! [🔒] [🔒] @RonisBrazil · Nov 6

- Quem é responsável pelas eleições?
- O TSE.
- Se houver FRAUDE, que é o responsável?
- O TSE.
- Havendo crime eleitoral, quem é o RÉU?
- O TSE.
- Mas se o réu é o TSE, que vai julgá-lo?
- Ele mesmo, o TSE!
- Mas o réu não pode apresentar provas contra si mesmo.

ENTEDERAM AGORA?



60

809

2,371



SIGILOSO

Retweeted José Medeiros



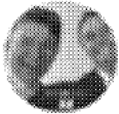
suzana tavares @suzanat89716306 · Nov 4

Derrubaram as tags #BrazilWasStolen mais de uma vez, seguem derrubando contas.... Estão com medo? Quanto mais censuram e tentam nos calar, mais alto gritaremos. "Verás que um filho teu não foge à luta"

Revolução Verde e Amarela!

Stay informed

Learn more about why election experts say civic processes in Brazil are safe and secure. Find out more



Um argentino incomoda muita gente... José Medeiros @JoseMedeirosMT · Nov 6

Ana @apropriaaana · Nov 6

Replying to @omachoalpha

Nova live! @FerCerimedo_ok



34

397

1,662

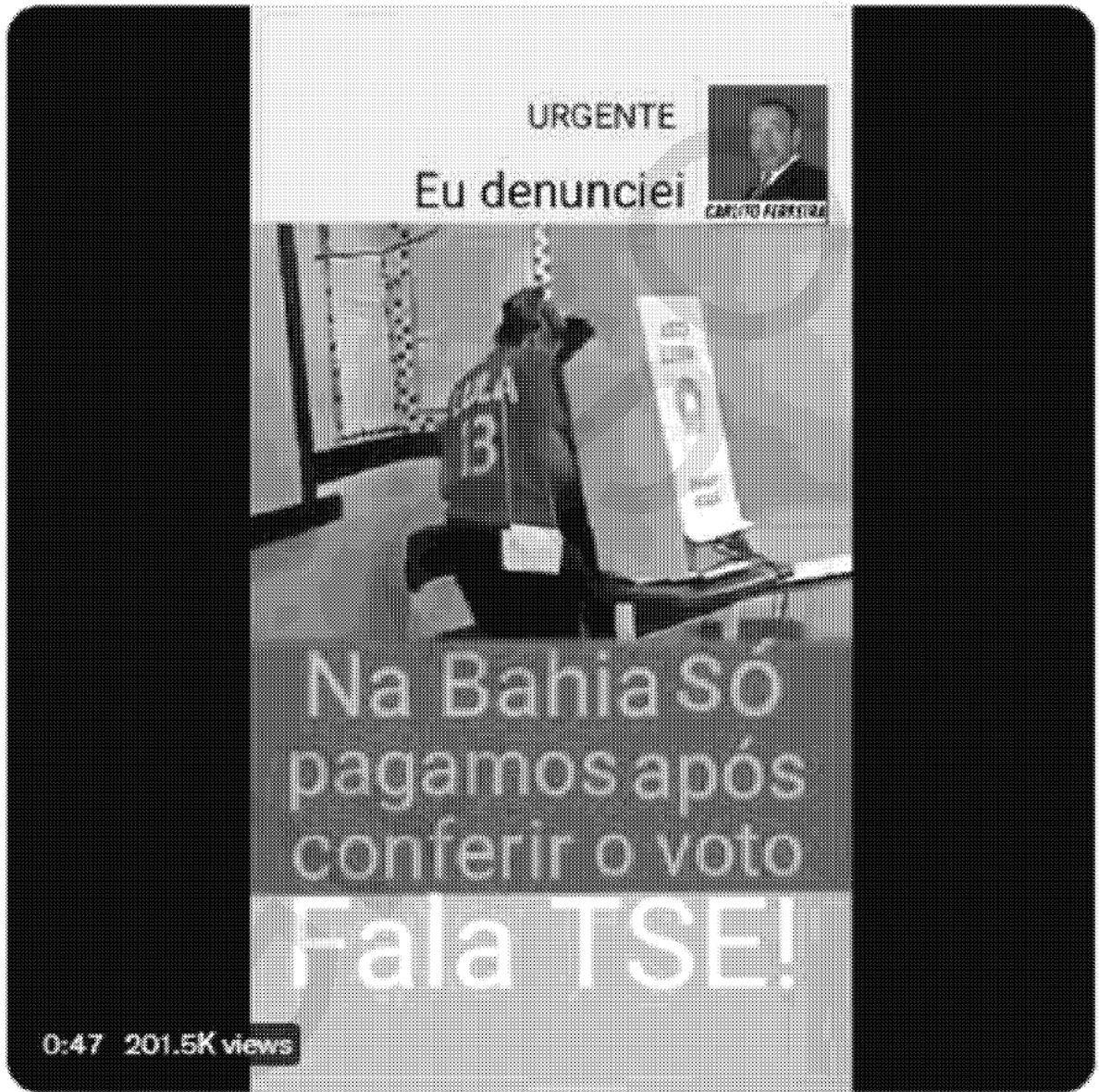


SIGILOSO



José Medeiros    @JoseMedeirosMT · Nov 4
Eleição limpa.

...



711 7,924 19.1K

Influenciador: José Medeiros

Rede social: Twitter

Número de seguidores: 179.2 mil

URL: <https://twitter.com/JoseMedeirosMT>

SIGILOSO

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à ruptura institucional, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o

SIGILOSO

processo eleitoral, na medida em que incentivam ou conferem subsídios argumentativos para comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma Twitter a imediata remoção dos perfis relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

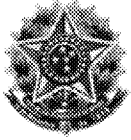
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 7 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO



06/02/2023

Número: **0601889-62.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **07/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

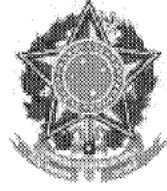
Objeto do processo: **Documentos extraídos do SEI n. 16116-6.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158608715	06/02/2023 10:43	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601889-62.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL**RELATOR: MINISTRO ALEXANDRE DE MORAES****INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL****DECISÃO**

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de manifestações públicas realizadas por grandes influenciadores digitais que atingem a integridade e a normalidade do processo eleitoral, incentivando, direta ou indiretamente, com base em afirmações falsas, a recusa dos resultados e a perpetuidade de movimentos antidemocráticos que buscam uma ruptura institucional.

Por meio das decisões IDs 158353339 e 158548103, determinei, entre outros casos, a suspensão dos perfis identificáveis de Alexandre Kunz, Flávio Beall, Lucelia, Cris Acangeli, Adrilles Jorge, Gilberto Silva, José Medeiros, ClaudioPitanga.

É o breve relato. Decido.

O art. 4º da Res.-TSE 23.714/2022 tutela a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação desinformações, representam substancial transgressão à própria Democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

SIGILOSO

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito, uma vez que, *"a desinformação - entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos - conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiança, com conseqüente perda da credibilidade e fé nas instituições da democracia representativa"* (Voto que proferi na ADI 7.261-MC, julgado em 25/10/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, *"não há direito no abuso de direito"* (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio "LIBERDADE e RESPONSABILIDADE"; não permitindo - como ocorrido nas presentes hipóteses - de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da "liberdade de expressão" como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

Considerado que houve a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral, a fim de possibilitar que os envolvidos possam retornar a utilizar suas redes sociais dentro do mais absoluto respeito à Constituição Federal e a Legislação, com observância do já citado binômio LIBERDADE – RESPONSABILIDADE, DETERMINO:

i) a reativação da conta dos perfis de Alexandre Kunz, Flávio Beall, Lucelia, Cris Acangeli, Adrilles Jorge, Gilberto Silva, José Medeiros, ClaudioPitanga da plataforma Twitter, mantendo-se, porém a remoção das postagens irregulares veiculadas; e

ii) a aplicação de MULTA DIÁRIA, no valor de R\$ 20.000,00 (vinte mil reais), a incidir na hipótese de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

Comuniquem-se as Plataformas para cumprimento imediato da presente decisão.

Por fim, considerando ultimado o processo político-eleitoral, bem como a pertinência temática ao Inquérito 4.879, ENCAMINHE-SE os autos ao SUPREMO TRIBUNAL FEDERAL.

Intime-se. Publique-se.

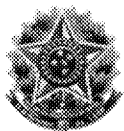
Brasília, 3 de fevereiro de 2023.

Ministro **ALEXANDRE DE MORAES**

SIGILOSO

SIGILOSO

SIGILOSO



08/11/2022

Número: **0601894-84.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **08/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **SEI 2022.00.000016282-0**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158355057	08/11/2022 18:48	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601894-84.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

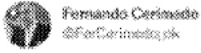
RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que detectou, nesta data, convocação para uma nova *live* (a terceira) protagonizada por Fernando Cerimedo, que se apresenta como “especialista” e que, com base em uma série de afirmações falsas, apresentou, no decorrer da semana, uma “auditoria” que, sem qualquer conexão com a realidade, aponta a existência de fraude nas eleições brasileiras, dando ensejo ao movimento golpista “#BrazilWasStolen” que viralizou nas redes sociais.

As transmissões em questão foram anunciadas em seu perfil social da plataforma Twitter, assim como em alguns meios de comunicação, como se vê:

SIGILOS



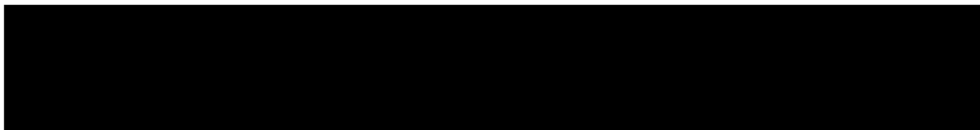
📺 Amanhã 12:00hs vou fazer uma LIVE com novas informações

- Auditoria completa da segunda volta
- Relação do META com TSE
- Auditorias sem fazer
- Modificação de arquivos

e muito mais!!!!

Não percam. Em breve postarei o link

Trabalho Total



SIGILOS



PODE CHEGAR,
A CASA É SUA.

Publicidade
COMIÇA DE SEU VÍDEO
DA ASSEMBLEIA LEGISLATIVA
PRA VOCÊ.

Início > Política Internacional > Hoje (6) será transmitida a segunda live, direto da Argentina, com novos...

Política Internacional Política Nacional

Hoje (6) será transmitida a segunda live, direto da Argentina, com novos indícios de anomalias nas urnas eletrônicas brasileiras

6 de novembro de 2022



A nova transmissão também está sendo divulgada em sua rede social, que indico como 19hs o horário de início, conforme se verifica da seguinte imagem:

SIGILOS



Fernando Cerimedo V.2

@fercerimedo_br



...

HOJE 19hs! Enviaremos os links uma hora antes. Não há retorno. A censura também será derrotada.

Translate Tweet



9:09 AM · Nov 8, 2022 · Twitter Web App

10.7K Retweets **408** Quote Tweets **38.2K** Likes

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

SIGILOS

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o processo eleitoral, na medida em que incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Observe-se, nessa linha, que o “especialista” em questão, mais uma vez, revela a intenção atacar a integridade das eleições brasileiras, apresentando novamente a expressão “#BrazilWasStolen” (O Brasil foi roubado, em tradução livre).

Cabe observar, nesse contexto, que no decorrer da semana o indivíduo apontado realizou duas transmissões de caráter sensacionalista, cuja visibilidade foi intensamente amplificada por influenciadores e canais extremistas, e que resultaram na replicação viral de uma série de afirmações falsas, que deram um novo impulso aos movimentos antidemocráticos de contestação do resultado das eleições populares.

Registre-se, nesse caminho, que o caráter falacioso da “auditoria” apresentada já foi revelado por agências de checagem de fatos e veículos confiáveis da imprensa tradicional, bem como refutado por esta Corte Superior:

SIGILOS

Seções ESTADO DE MINAS Política

AUDITORIA AFÓRICA

TSE desmente suspeita de fraude eleitoral citada em live de argentino

Órgão citou ao menos 5 auditorias realizadas nas urnas eletrônicas brasileiras desde ao longo da última década, que não encontraram indícios de 'engildade'

Fonte: Estado de Minas.

É #FAKE que urnas eletrônicas de modelos anteriores a 2020 não foram auditadas

TSE faz auditorias nas urnas desde 2002, sem restrição de modelos. Equipamentos passam por dois testes, de integridade e de autenticidade, para garantir que não há divergência entre votos dados e votos registrados pelas urnas.

Por Aline Macedo, g1
05/11/2022 17h07 · Atualizado há 16 horas

Fonte: Portal G1.

SIGILOS



Política

Auditoria na Argentina comprova fraude nas urnas brasileiras e é apresentada em live #boato

📅 04/11/2022 👤 Edgard Matsuki 🌐 Argentina, Eleições 2022, fraude, Urnas eletrônicas

Fonte: Boatos.org.

SIGILOS

Num. 158355057 - Pág. 7

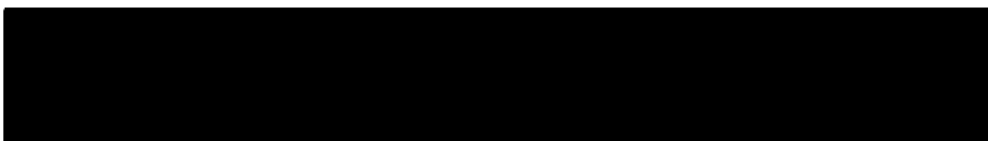
POLÍTICA

Live que distorce informações sobre urnas é assistida por 415 mil pessoas



Fonte: Portal UOL.

SIGIL



SIGILOS

Brasil

TSE desmente suspeita de fraude nas urnas citada por canal argentino

Influenciador de extrema direita da Argentina que recebeu Eduardo Bolsonaro em outubro faz live apontando suspeitas de fraude eleitoral

Fábio Leite

05/11/2022 12:50, atualizado 05/11/2022 15:41

Reprodução/YouTube



Fonte: Jornal Metr p les.

Ante o que se observa,   evidente que o “especialista” Fernando Cerimedo, que, como aponta a reportagem do Jornal Metr p les, nada mais   do que um “influenciador de extrema direita”, pretende com a nova *live* anunciada reincidir na pr tica de crimes e il citos eleitorais, com a finalidade de insuflar um cen rio de instabilidade pol tica, que por sua vez ensejaria, na vis o de movimentos antidemocr ticos, condi es suficientes para a deflagra o de uma ruptura institucional.

Dentro desse contexto, considerando a inequ voca intenc o de tumultuar as elei es em andamento que, como se sabe, formalmente se encerram apenas com o ato de diploma o. Fica assim autorizado o exerc cio

SIGILOS

Num. 158355057 - P g. 9

preventivo do poder administrativo para impedir a realização de ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral:

DETERMINO às plataformas Youtube, Instagram, Facebook, Twitch, TikTok, Kwai e Twitter a adoção de todas as medidas necessárias para impedir a transmissão da *live* anunciada, inclusive com a imediata remoção dos perfis que as iniciem ou as exibam simultaneamente, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais), em caso de transmissões que ultrapassem o período de 10 (dez) minutos;

DETERMINO que a plataforma Twitter proceda a imediata remoção do perfil @fercerimedo_br, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação;

DETERMINO, mais, a imediata remoção dos perfis (URLs) que serão enviados, oportunamente, pela Assessoria Especial de Enfrentamento à Desinformação, no período compreendido entre as 17h e as 19h da data de hoje, com apoio nesta decisão, sob pena de multa ora fixada no R\$150.000 (cento e cinquenta mil reais), a contar da primeira hora após a comunicação que, nesse caso, será operacionalizada, excepcionalmente, por simples mensagem eletrônica (e-mail).

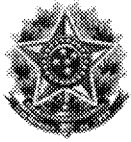
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 8 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOS



14/11/2022

Número: **0601912-08.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **12/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **A Assessoria Especial de Enfrentamento à Desinformação (AEED) informa que, a partir de atividades de monitoramento de dados abertos de mídias sociais, detectou a circulação em redes sociais de vídeo e mensagens que atinge a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas acusações de fraude, a recusa dos resultados do pleito presidencial de 2022.**

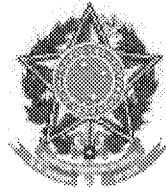
- documento extraído do SEI 16612-5

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158377638	13/11/2022 13:55	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601912-08.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Diante de decisão encaminhada pelo SUPREMO TRIBUNAL FEDERAL e dada a similaridade dos conteúdos já reputados irregulares no ID 158375403, inclusive com incitação à violência física aos Ministros desta Corte do do Supremo Tribunal Federal, portanto, em complementariedade, de ordem, **DETERMINO** com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Facebook, Instagram e Twitter a remoção definitiva e imediata das respectivas postagens identificadas pelos links abaixo:

https://twitter.com/fernandopclinea/status/1591635897501773824?s=48&t=Uwx2gt2gxnJgY_VUHmfXww

<https://twitter.com/caminhoneiros22/status/1591724847566053384?s=48&t=viH2fBBlfsg6kqgqbb0MCg>

<https://twitter.com/ultrajantesinc/status/1591812832446013442?s=48&t=viH2fBBlfsg6kqgqbb0MCg>

<https://twitter.com/giselenatural/status/1591755858752729088?s=48&t=viH2fBBlfsg6kqgqbb0MCg>

DETERMINO, ainda, para ambas as plataformas, a remoção definitiva e imediata dos perfis relacionados e do conteúdo dos vídeos e mensagens, veiculados na íntegra ou parcialmente em outras postagens para além das acima relacionadas, bem como de eventuais postagens futuras que venham a replicar o mesmo conteúdo, devendo ser preservada uma cópia do conteúdo, pelo prazo de 6 (seis) meses, para caso seja necessário realizar investigação posterior:

<https://twitter.com/FernandoPclinea>

<https://twitter.com/Caminhoneiros22>

<https://twitter.com/UltrajanteSinc>
<https://twitter.com/GiseleNatural>

O descumprimento de quaisquer das determinações acima acarretará a imposição de pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

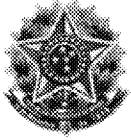
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 13 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOS



20/11/2022

Número: **0601942-43.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **20/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	

Outros participantes
Procurador Geral Eleitoral (FISCAL DA LEI)

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158396395	20/11/2022 12:30	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601942-43.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL**RELATOR: MINISTRO ALEXANDRE DE MORAES****INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL****DECISÃO**

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que versa sobre a divulgação pública do número de telefone celular do Presidente desta Corte Superior, Min. Alexandre de Moraes, e que resultou no recebimento de diversas ligações e mensagens de cunho ofensivo e ameaçados, colocando em risco a segurança pessoal do Ministro e de sua família.

As ligações em questão, que somaram centenas, foram recebidas por meio de ligações telefônicas e do aplicativo de mensageria WhatsApp.

Paralelamente, a AEED/TSE informa a localização de vídeo publicado pelo blogueiro foragido Allan dos Santos, em que, a par de atacar Sua Excelência por diversas vezes, com palavras agressivas e de ordem, realiza uma ligação telefônica para o Min. Alexandre de Moraes, deixando aparecer os correspondentes números, em diversas oportunidades.

Por fim, reporta a Assessoria Especial que o foragido em questão promoveu a criação de um novo perfil na rede social Instagram, em franco descumprimento a decisão judicial, assim como a criação de um sítio eletrônico, que redireciona para o site oficial do Terça Livre, que se encontra hospedado no exterior, protegido por sistemas de privacidade e leis locais.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

SIGILOSO

A partir dos fatos relatados, verifica-se o compartilhamento irregular de dados pessoais com a finalidade inequívoca de transferir, para a pessoa do Ministro Presidente, os ataques institucionais com base em desinformação que afetam a integridade do processo eleitoral, com o objetivo mediato de fomentar protestos antidemocráticos que visam à ocorrência de ruptura constitucional, mediante intervenção federal ou militar.

Consequentemente, o grupo em questão, em hipótese, tem servido como instrumento para a prática dos ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, 147 e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 147. Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.

Pena – detenção, de um a seis meses, ou multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, a incitação de atos de assédio contra o ministro Alexandre de Moraes configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a prática de ameaça está igualmente tipificada naquele código, notadamente no art. 147.

Considerando a gravidade do fato narrado, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 296 do Código Eleitoral, 147 e 286 do Código Penal, de ordem, **DETERMINO**

SIGILOSO

a) à plataforma Telegram, que promova, por seus meses, a preservação dos dados relacionados ao conteúdo do grupo identificado na URL <https://t.me/turbometodos>, no prazo máximo de 2 (duas) horas, sob pena de multa de R\$ 150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do recebimento da comunicação;

b) à plataforma Instagram, que promova a imediata remoção do perfil identificado pela URL <https://www.instagram.com/santosallan23/>, no prazo máximo de 02 (duas) horas, sob pena de multa de R\$ 150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do recebimento da comunicação;

c) à plataforma Twitter, que promova a imediata remoção das postagens listadas abaixo, no prazo máximo de 02 (duas) horas, sob pena de multa de R\$ 150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do recebimento da notificação:

https://twitter.com/realdabruno/status/1592690023258034176?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1592690023258034176%7Ctwgr%5Ec67ce2936fe66ab2274d45f4cfc03eac419a5817%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fveja.abril.com.br%2Fcoluna%2Fvirou-viral%2Fo-novo-ataque-de-allan-dos-santos-a-alexandre-de-moraes-assista%2F

<https://twitter.com/UOLNoticias/status/1593356561119780864?t=3XFfKDIXwRD9ht7JM4NIIQ&s=19>

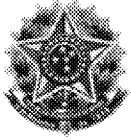
https://twitter.com/iamcobbcooper/status/1593347199429124096?t=-e_luTYtTScyZ6xRVj4YTO&s=19

Cumpra-se com urgência.

Brasília, 20 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO



25/11/2022

Número: **0601942-43.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **20/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Segredo de Justiça? **SIM**

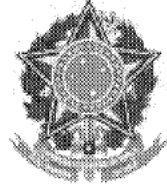
Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	

Outros participantes
Procurador Geral Eleitoral (FISCAL DA LEI)

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158440714	25/11/2022 19:22	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601942-43.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

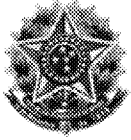
Diante da Informação ID 158440818 prestada pela Assessoria Especial de Enfrentamento à Desinformação, reconsidero a decisão ID 158396395 para fazer excluir a matéria do jornal Folha de São Paulo, pelo perfil @UOLNoticias (URL: <https://twitter.com/UOLNoticias/status/1593356561119780864?t=3XFfKDIX>) da determinação.

Intime-se a plataforma Twitter.

Brasília, 25 de novembro de 2022.

Marco Antônio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO



20/11/2022

Número: **0601941-58.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **20/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Documentos extraídos do SEI 17031-9**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158396393	20/11/2022 12:41	<u>Decisão</u>	Decisão

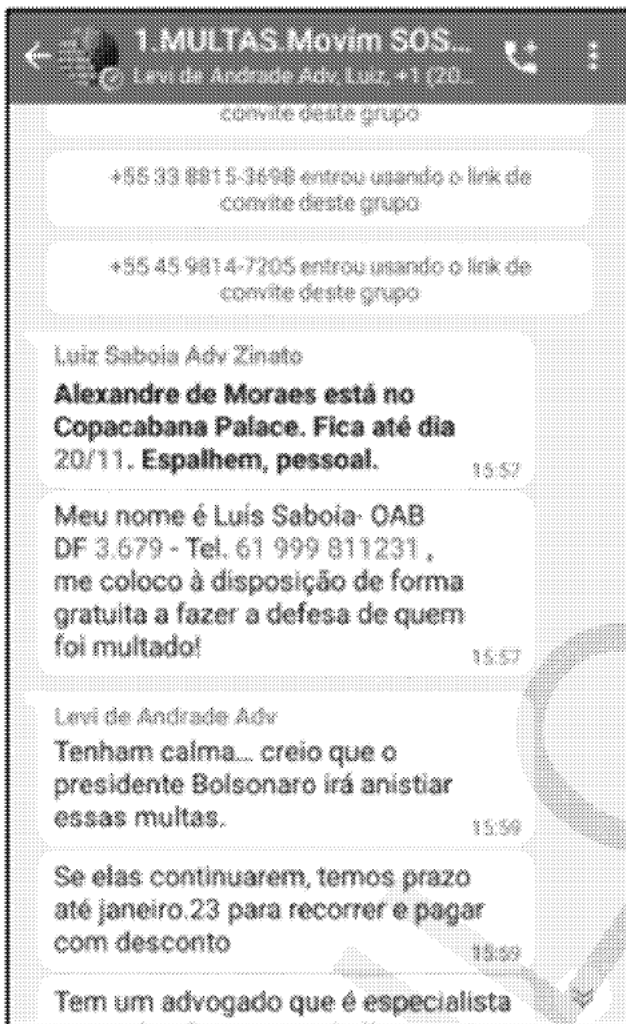
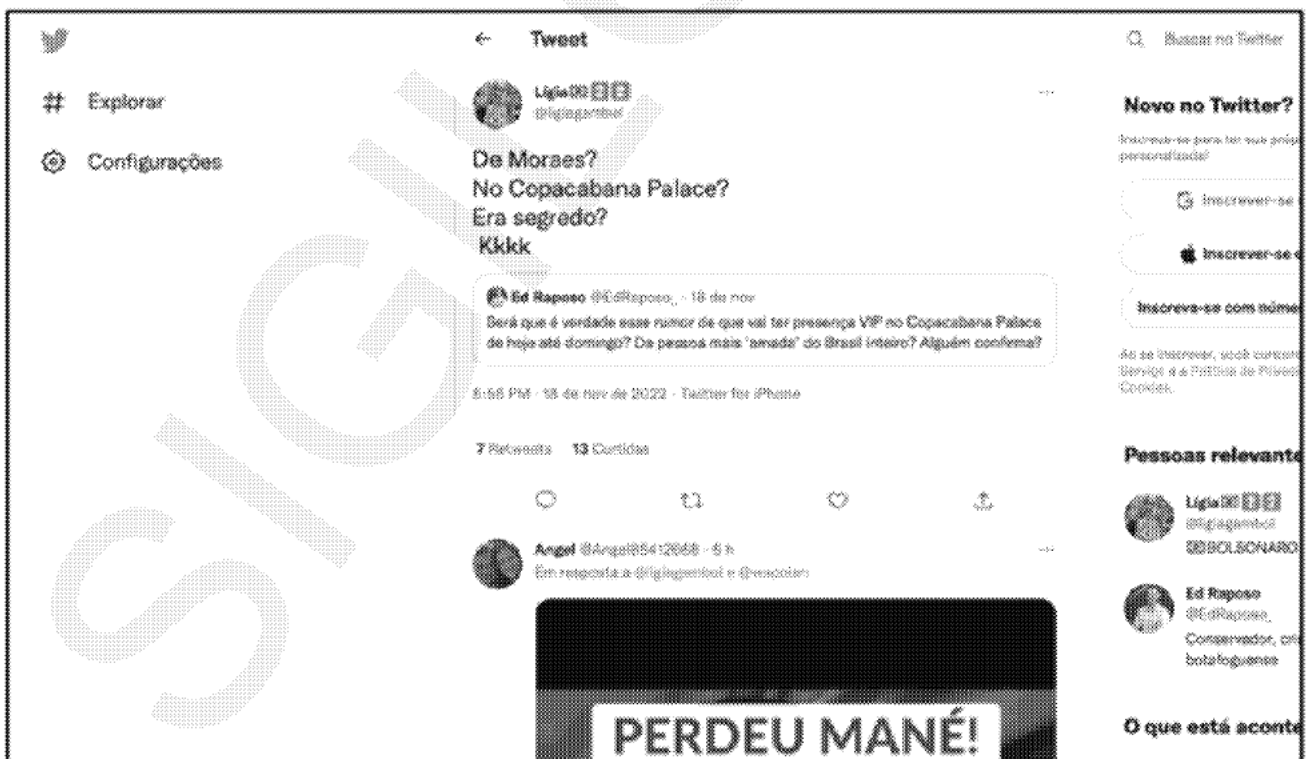


Figura 2 - Mensagem objeto da análise

Paralelamente, a AEED/TSE identificou diversos perfis do indigitado advogado em redes sociais, comumente utilizadas para a divulgação de narrativas falsas que atingem a integridade do processo eleitoral, assim como postagens análogas, em outros perfis, que arriscam a segurança e a integridade física do Ministro Presidente desta Corte Superior, como por exemplo:



SIGILOSO



É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as

SIGILOS

violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, verifica-se o compartilhamento irregular de dados pessoais com a finalidade inequívoca de transferir, para a pessoa do Ministro Presidente, os ataques institucionais com base em desinformação que afetam a integridade do processo eleitoral, com o objetivo mediato de fomentar protestos antidemocráticos que visam à ocorrência de ruptura constitucional, mediante intervenção federal ou militar.

Consequentemente, o grupo em questão, em hipótese, tem servido como instrumento para a prática dos ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

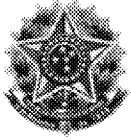
Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, a incitação de atos de assédio contra o ministro Alexandre de Moraes configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a prática de ameaça está igualmente tipificada naquele código, notadamente no art. 147.

Considerando a gravidade do fato narrado, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 296 do Código Eleitoral, e 286 do Código Penal, de ordem, **DETERMINO**:

a) à plataforma Instagram, que promova a remoção do perfil identificado na URL <https://www.instagram.com/lfsaboia/> no prazo máximo de 02 (duas) horas, sob pena de multa de R\$ 150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do recebimento da comunicação;

SIGILOSO



24/11/2022

Número: **0601963-19.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **23/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

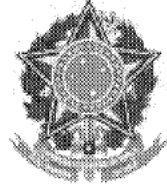
Objeto do processo: **Documentos extraídos do SEI n. 17265-6.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158427230	24/11/2022 12:15	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601963-19.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, concernente a perfil de cunho golpista em rede social, mormente dedicado a postagens que, no contexto de falsas acusações de fraude, incentivam a recusa dos resultados do pleito presidencial e tentam forçar uma intervenção militar.

Os perfis em questão operam nas plataformas Twitter, como se vê:

Perfil: Flavio Gordon

Plataforma: Twitter

URL: <https://twitter.com/flaviogordon>

Número de seguidores: 187.7 mil

Postagens (rol exemplificativo):

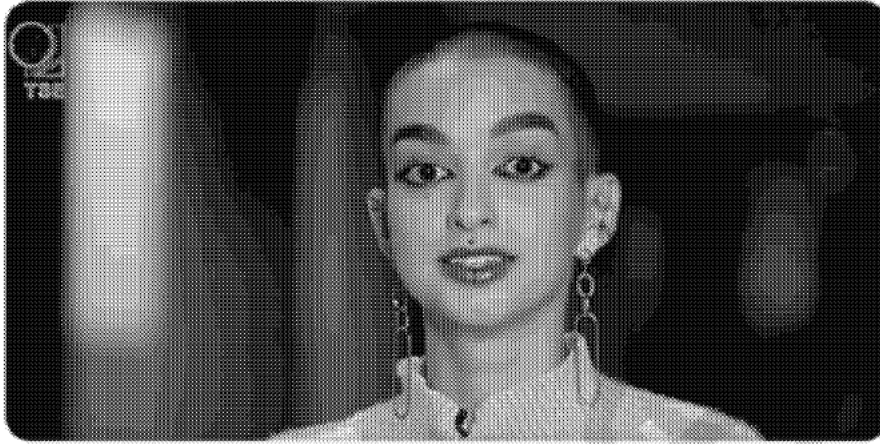
SIGILOSO



Flávio Gordon @flaviogordon · 55m

...

Porta-voz do TSE garantindo que os técnicos do ITA não sabem o que estão dizendo. Ufa! Agora ficou tudo esclarecido...



732

1,462

8,917



Flávio Gordon Retweeted



Alan Ghani @Alanghani · 3h

...

Isso é um fato: os logs das urnas anteriores a 2015 estavam inválidos. Com a palavra, o engenheiro do ITA:



youtube.com

CARLOS ROCHA: "URNAS ANTIGAS APRESENTA...

Presidente do Instituto Voto Legal, Carlos Rocha, comenta sobre a auditoria dos votos. Acompanhe ...

9

138

628



SIGILOSO



Flávio Gordon @flaviogordon · 1h

...

"Urmas eletrônicas que não produzem um registro em papel de cada voto computado não são confiáveis."

(Editorial do The New York Times publicado em 2009)

🗨️ 22

🔄 492

❤️ 2,126



Flávio Gordon @flaviogordon · 1h

...

"É até irônico que essas máquinas de votar, que supostamente deveriam resolver os problemas causados pelos sistemas eleitorais antiquados, estejam simplesmente tornando os problemas invisíveis para o eleitor." (Penny M. Venetis, professora de Direito na Rutgers University)

🗨️ 5

🔄 131

❤️ 698



Flávio Gordon @flaviogordon · 4h

...

Muito se fala e se critica (com razão) a ida do Barroso ao Congresso para fazer lobby contra o voto auditável. Mas mais perturbador que o fato em si é pensar na causa. O que poderia ter levado um membro do TSE a se empenhar tanto para que a uma continuasse uma caixa preta?

🗨️ 138

🔄 1,352

❤️ 5,820



🔄 Flávio Gordon Retweeted



Paolo Zanotto, D.Phil. @epimeme · 14h

...

A integridade do TSE foi reduzida às melenas do Alexandre de Moraes...

🗨️ 38

🔄 598

❤️ 3,607



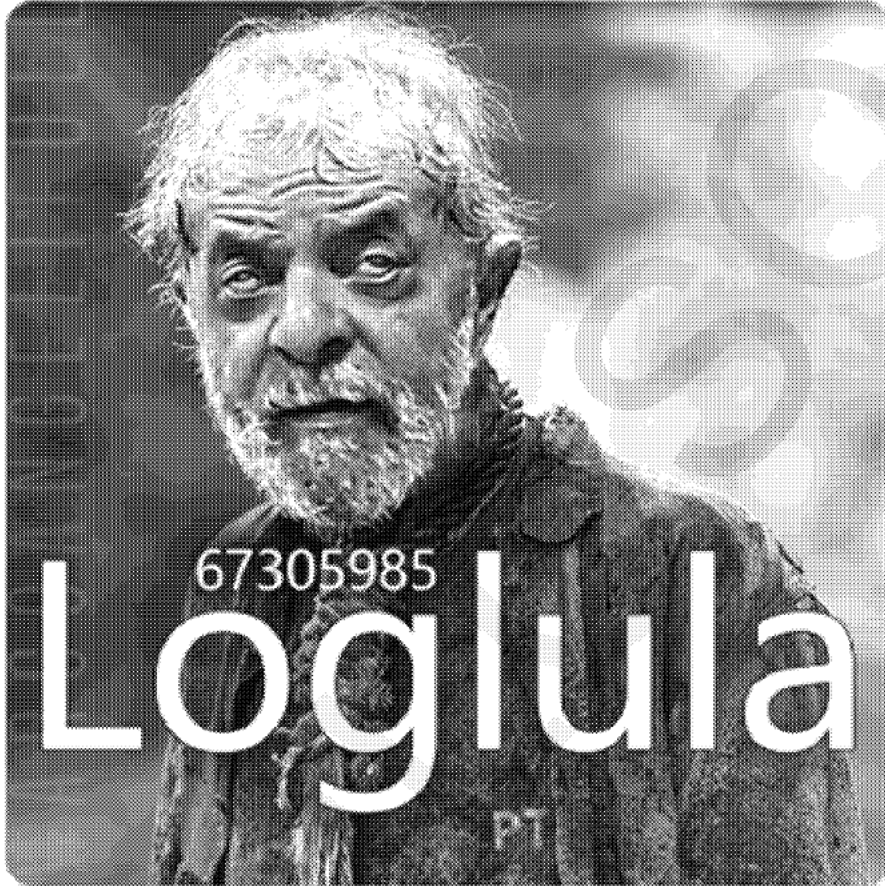
SIGILOSO

Flávio Gordon Retweeted



Marco Angeli @marcoangeli · 7h

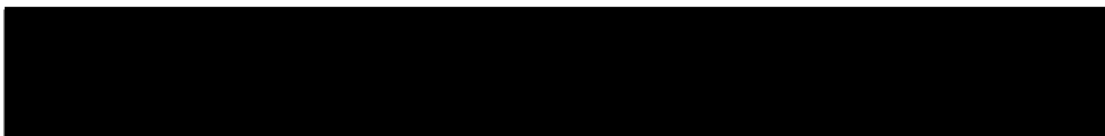
Democracia porreta é assim.
Todos são iguais.
Até os logs.



12

165

584



SIGILOS

Flávio Gordon Retweeted



Jovem Pan News @JovemPanNews · 21h

...

Official

#JPUrgente | Engenheiro Carlos Cesar Rocha, dono do Instituto Voto Legal: "Em cada linha de registro da atividade de funcionamento em todas as urnas de modelos antigos, o código é inválido; isso é um indício forte que há um problema"

Confira na JP News



978 6,728 28K

Flávio Gordon Retweeted



Rafael Fontana @RafaelFontana · 15h

...

O POVO MANDA:
- MORAES TEM 24 HORAS PARA SE EXPLICAR.

Ninguém vai aceitar inversão de valores.

Vamos começar agora, ao vivo, com Andreia Matias e Rafael Fontana.
@AndreiaLMatias



youtube.com
O SUSPEITO É O TSE: POVO EXIGE EXPLICAÇÕES

SIGILOSO

Flávio Gordon Retweeted



Marcelo Suano @marcelosuano · 16h

Pessoal, amanhã, 23 de novembro, às 10h, a @bmcnewstv receberá o engenheiro responsável pela auditoria feita nas urnas, apresentada pelo PL ao TSE.

Carlos Rocha, é formado pelo ITA e foi responsável pelo documento que, segundo o PL, apresentou irregularidades em 235mil urnas.

54 2,190 7,898

Show this thread

Flávio Gordon Retweeted



Paula Marisa @profpaulamarisa · 14h

O incrível caso do homem que leu mais de 200 páginas em 13 minutos

1,198 5,712 37.5K

Flávio Gordon Retweeted



Fernando Holiday @FernandoHoliday · 14h

FAKE NEWS!

Os arquivos "log" das urnas apresentados pelo PL já incluem o 1º e 2º turno.

Portanto, é FALSO a ideia de que a ação questiona apenas os arquivos do 2º turno.

O desespero de Alexandre de Moraes o impediu de ler a ação e seus anexos. Há incompetência e má vontade!

1,409 6,708 35.4K

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

SIGILOSO

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

É evidente que as postagens dos perfis detectados possuem potencial para tumultuar o processo eleitoral, na medida em que, explícita ou implicitamente, incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma Twitter a remoção definitiva e imediata do perfil relacionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

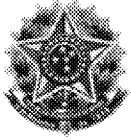
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 23 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO



01/02/2023

Número: **0601963-19.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **23/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

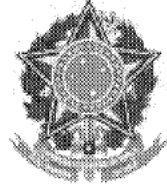
Objeto do processo: **Documentos extraídos do SEI n. 17265-6.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158579779	31/01/2023 19:25	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601963-19.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de perfil nas redes sociais, orientado para a divulgação de desinformação contra as eleições e apologia à intervenção militar, em detrimento da vontade popular registrada nas Eleições 2022.

Por meio da decisão de ID 158427230, determinei a suspensão do perfil de FLAVIO GORDON, nos seguintes termos:

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, DETERMINO à plataforma Twitter a remoção definitiva e imediata do perfil relacionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

É o breve relato. Decido.

O art. 4º da Res.-TSE 23.714/2022 tutela a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação desinformações, representam substancial transgressão à própria Democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a

SIGILOSO

condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito, uma vez que, *"a desinformação - entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos - conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiância, com conseqüente perda da credibilidade e fê nas instituições da democracia representativa"* (Voto que proferi na ADI 7.261-MC, julgado em 25/10/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, *"não há direito no abuso de direito"* (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio "LIBERDADE e RESPONSABILIDADE"; não permitindo - como ocorrido nas presentes hipóteses - de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da "liberdade de expressão" como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

Considerado que houve a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral, a fim de possibilitar que os envolvidos possam retornar a utilizar suas redes sociais dentro do mais absoluto respeito à Constituição Federal e a Legislação, com observância do já citado binômio LIBERDADE – RESPONSABILIDADE, DETERMINO:

i) a reativação da conta <https://twitter.com/flaviogordon>, mantendo-se, porém a remoção das postagens irregulares veiculadas; e

ii) a aplicação de MULTA DIÁRIA, no valor de R\$ 20.000,00 (vinte mil reais), a incidir na hipótese de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

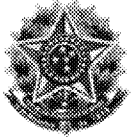
Por fim, iii) comunique-se a Plataforma Digital Twitter para cumprimento imediato da presente decisão; e iv) diante da pertinência temática ao Inquérito 4.879, encaminhem-se os autos ao SUPREMO TRIBUNAL FEDERAL.

Intime-se. Publique-se.

Brasília, 30 de janeiro de 2023.

Ministro **ALEXANDRE DE MORAES**
Presidente

SIGILOSO



26/11/2022

Número: **0601969-26.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **26/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Documentos extraídos do SEI n. 17498-5.**

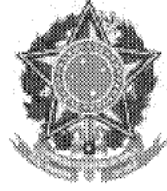
Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158444591	26/11/2022 11:19	<u>Decisão</u>	Decisão

index: PETIÇÃO CÍVEL (241)-0601969-26.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601969-26.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, concernente a perfis de cunho golpista em redes sociais, mormente dedicados a postagens que, no contexto de falsas acusações de fraude, incentivam a recusa dos resultados do pleito presidencial e tentam forçar uma intervenção militar.

Os perfis em questão operam nas plataformas Twitter, Youtube, Instagram e Telegrama, como se vê:

Perfil: Ed Raposo

Plataforma: Twitter

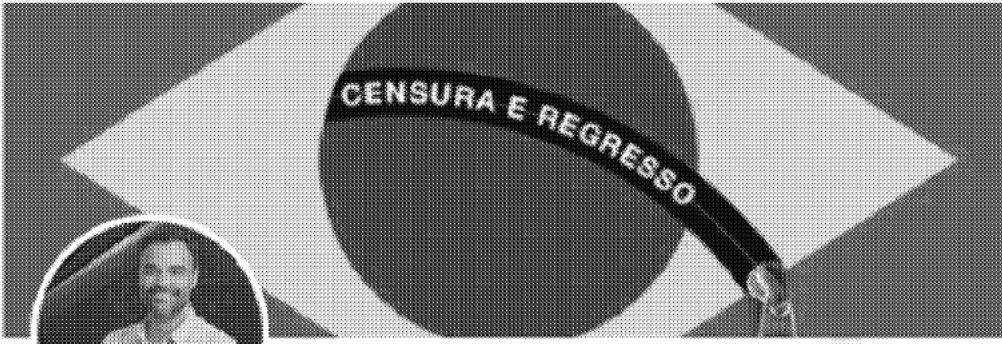
URL: https://twitter.com/edraposo_

Número de seguidores: 136.8 mil

Postagens (rol exemplificativo):

SIGILOSO

← **Ed Raposo**
5,678 Tweets



⋮ **Follow**

Ed Raposo

@EdRaposo_

Conservador, cristão, patriota e botafoguense

📍 Rio de Janeiro, Brasil youtube.com/c/EdRaposoDire...

📅 Joined April 2022

96 Following 136.8K Followers

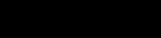
👤 Followed by MarioFrias, TeAtualizei, 📺, 📺, 📺, 📺, 📺, and 3 others you follow

Tweets

Tweets & replies

Media

Likes



SIGILOSO



Ed Raposo @EdRaposo_ · 8h

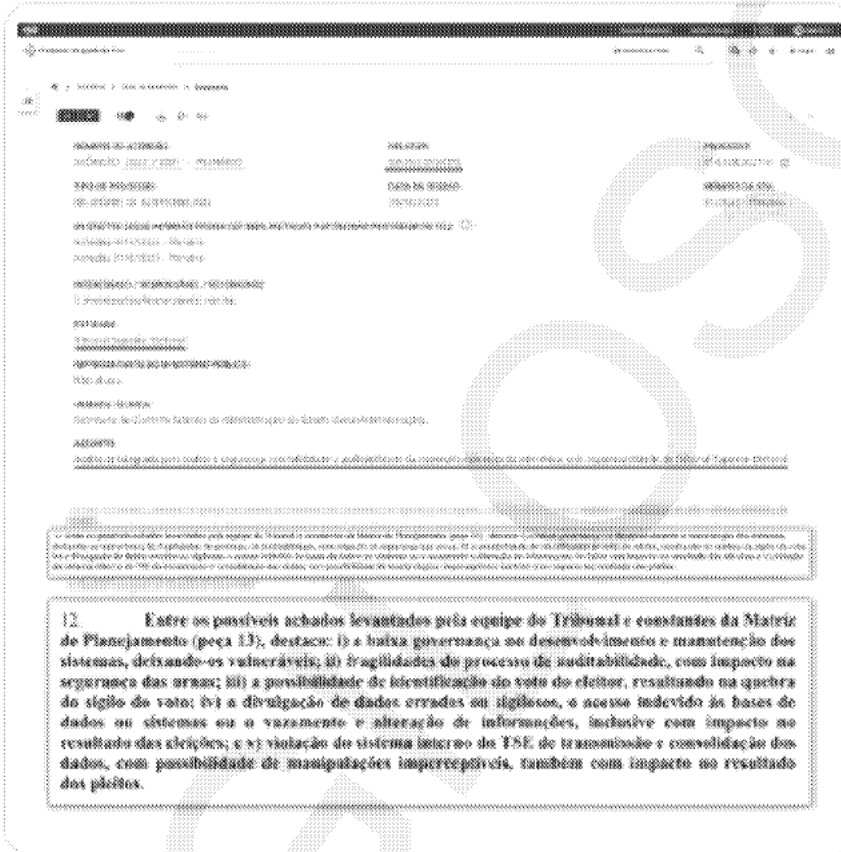
Moraes não vai acatar nada, é bom que todo mundo saiba disso. A solução será outra.

1,000 4,270 26.6K

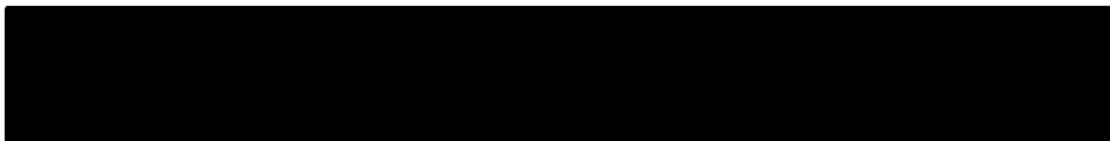


Ed Raposo @EdRaposo_ · 8h

O presidente do TCU já veio questionar o relatório, mas explicar isso aqui que é bom, nada...



82 1,184 4,010



SIGILOSO

- Ed Raposo** @EdRaposo_ · 9h ...
 Já podemos dizer que Bolsonaro foi reeleito ou precisamos esperar a análise do Nelipe Feto?
- 592 3,105 21,8K
- Ed Raposo** @EdRaposo_ · 9h ...
 Como bem apontou o @MauricioCostaRS do MBC, Bolsonaro não teve 51% dos votos, ele teve PELO MENOS 51%. E a questão da eleição é só parte do que vem por aí, depois teremos a etapa de responsabilização. Essa sim será divertida.
- 126 2,181 8,373
- Ed Raposo** @EdRaposo_ · 9h ...
 A mídia está em negação. O marido corno pegou a esposa com o Ricardão no meio do rala e rola, mas diz pros amigos que ela estava praticando jiu-jitsu naturista de alto impacto.
- 131 1,831 8,843
- Ed Raposo** @EdRaposo_ · 10h ...
 Se descartarem as urnas antigas no primeiro turno a tendência é a base do PR aumentar ainda mais. Só quem tá com medo é o parlamentar surfiata do centrão sem alinhamento ideológico com Bolsonaro.
- E só pra constar, não vai me beneficiar.
- 177 2,362 12,2K
- Ed Raposo** @EdRaposo_ · 10h ...
 A VIRADA É INEVITÁVEL
-  youtube.com
 A VIRADA É INEVITÁVEL
 #Brasil #GradoRetumbante #PátriaAmada Lista de transmissão de WhatsApp do Ed Raposo: ...
- 18 162 1,298
- Ed Raposo** @EdRaposo_ · 11h ...
 O Xandão que conhecemos jogaria o pedido no lixo. O Xandão que sabe que perdeu tenta jogar xadrez.
- 423 4,403 24K

SIGILOSO



Ed Raposo @EdRaposo_ · 14h

Em homenagem ao inesquecível Erasmo Carlos, que nos deixou hoje, cantaremos 'pega na mentira' a partir das 16h.

74

926

6,121



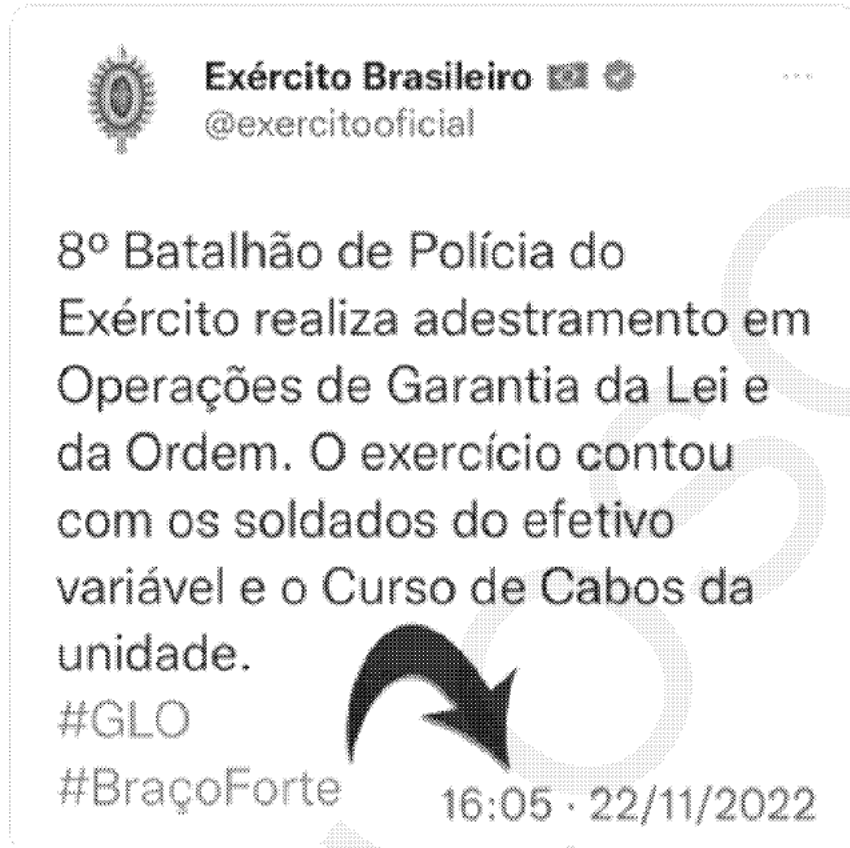
SIGILOSOS

SIGILOSOS



Ed Raposo @EdRaposo_ · 12h
Enquanto isso...

...



94 1,265 6,796



Ed Raposo @EdRaposo_ · 12h

...

É óbvio que o TSE não vai acatar nada, isso a gente está cansado de saber. O jogo agora é outro.

478 3,583 21.5K



Ed Raposo @EdRaposo_ · 12h

...

Que comece o 'Bolsonaro pede anulação sem apresentar provas'.

181 989 8,267



Ed Raposo @EdRaposo_ · 12h

...

Resumindo: a lei exige que todas as urnas sejam auditáveis e as anteriores a 2020 não são. Desta feita, restam ao TSE duas opções:

1. Descartar as urnas não-auditáveis;
2. Entregar o código-fonte e provar que essas urnas são auditáveis.

De um jeito ou de outro, Bolsonaro 🙄

479 6,892 27.8K



Ed Raposo @EdRaposo_ · 12h

...

Se o TSE não aceitar, entra em ação o poder moderador.

303 2,178 11.6K

SIGILOSO

Perfil: Ed Raposo

Plataforma: Youtube

URL: <https://www.youtube.com/c/EdRaposoDireitaVouVer>

Número de seguidores: 359 mil

Postagens (rol exemplificativo):

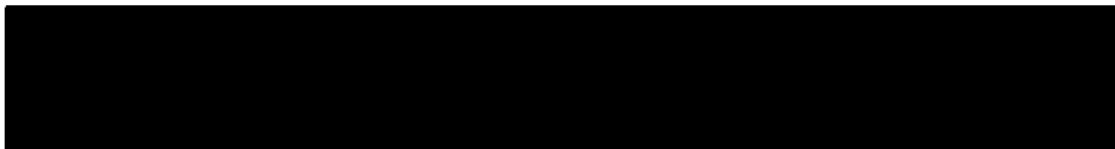
Perfil: Ed Raposo

Plataforma: Instagram

URL: <https://www.instagram.com/edraposo.official/>

Número de seguidores: 12,9 mil

Postagens (rol exemplificativo):



SIGILOSO



edraposo.official

Seguir

Enviar mensagem



106 publicações

12.9K seguidores

19 seguindo

Ed Raposo

BR

📍 Novo Perfil Oficial

📺 Canal do YouTube

youtube.com/c/EdRaposoDireitaVouVer



COS.TV



WhatsApp

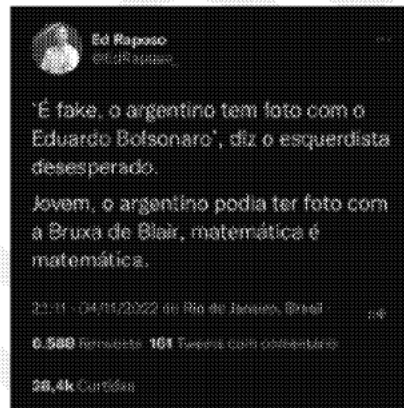


APP ED RA...

PUBLICAÇÕES

REELS

MARCADOS



SIGILOSO

CANAL ED RAPOSO
A VIRADA É INEVITÁVEL
https://youtu.be/Mjr_3AG2uRM

YouTube
A VIRADA É INEVITÁVEL
#Brasil #BradoRetumbante #PátriaAmada

Lista de transmissão de WhatsApp do Ed Raposo: <https://wa.me/...>



8003 ER, 19:12

108 comments

SIGILO

SIGILOSO

CANAL ED RAPOSO
NÃO FICOU APENAS NO ÁUDIO VAZADO
<https://youtu.be/Pa1fuHgp3Q0>

YouTube
NÃO FICOU APENAS NO ÁUDIO VAZADO
#Brasil #BradoRetumbante #PátriaAmada

Lista de transmissão de WhatsApp do Ed Raposo: <https://wa.me/...>



16K ER, 18:56

140 comments

November 22

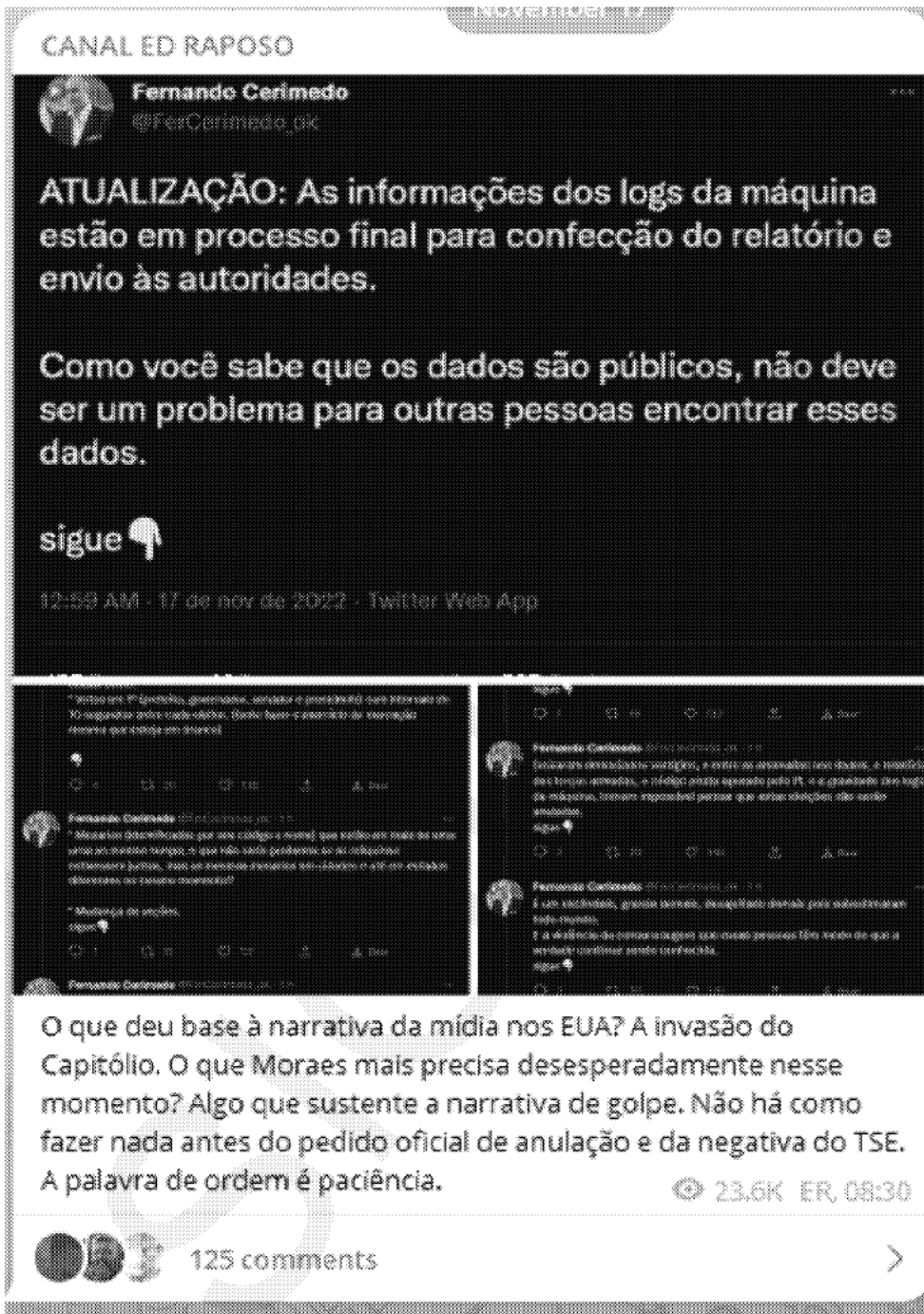
CANAL ED RAPOSO
ÚLTIMA BARREIRA
<https://youtu.be/Elo7FbhwkM0>

YouTube
ÚLTIMA BARREIRA
#Brasil #BradoRetumbante #PátriaAmada

Lista de transmissão de WhatsApp do Ed Raposo: <https://wa.me/...>



SIGILOSO



Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou

SIGILOSO

afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

É evidente que as postagens dos perfis detectados possuem potencial para tumultuar o processo eleitoral, na medida em que, explícita ou implicitamente, incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º, da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Twitter, Youtube e Instagram a remoção definitiva e imediata dos perfis relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

DETERMINO, mais, à plataforma Telegram o imediato bloqueio do grupo apontado, até a diplomação dos eleitos no pleito presidencial de 2022, no mesmo prazo e sob as mesmas consequências.

Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

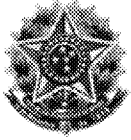
SIGILOSO

Brasília, 26 de novembro de 2022.

Mar Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSOS

SIGILOSOS



01/02/2023

Número: **0601969-26.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **26/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

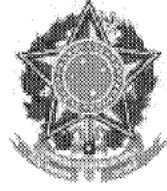
Objeto do processo: **Documentos extraídos do SEI n. 17498-5.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158579782	31/01/2023 19:23	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601969-26.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de perfil nas redes sociais, orientado para a divulgação de desinformação contra as eleições e apologia à intervenção militar, em detrimento da vontade popular registrada nas Eleições 2022.

Por meio da decisão de ID 158444591, determinei a suspensão do perfil de ED RAPOSO, nos seguintes termos:

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, DETERMINO às plataformas Twitter, Youtube e Instagram a remoção definitiva e imediata dos perfis relacionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Posteriormente, determinei a suspensão do perfil Ed Raposo_canal, conforme decisão a seguir descrita (ID 158449418):

Ante o exposto, de ordem, com base nos arts. 2º, § 1º, da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, DETERMINO à plataforma Instagram a remoção definitiva e imediata do perfil relacionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

É o breve relato. Decido.

O art. 4º da Res.-TSE 23.714/2022 tutela a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação desinformações, representam substancial transgressão à própria Democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a

SIGILOSO

determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito, uma vez que, *"a desinformação - entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos - conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiança, com conseqüente perda da credibilidade e fé nas instituições da democracia representativa"* (Voto que proferi na ADI 7.261-MC, julgado em 25/10/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, *"não há direito no abuso de direito"* (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio "LIBERDADE e RESPONSABILIDADE"; não permitindo - como ocorrido nas presentes hipóteses - de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da "liberdade de expressão" como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

Considerado que houve a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral, a fim de possibilitar que os envolvidos possam retornar a utilizar suas redes sociais dentro do mais absoluto respeito à Constituição Federal e a Legislação, com observância do já citado binômio LIBERDADE – RESPONSABILIDADE, DETERMINO:

i) a reativação da conta dos perfis Ed Cardoso nas redes sociais Twitter, Youtube, Instagram e Telegram, mantendo-se, porém a remoção das postagens irregulares veiculadas; e

ii) a aplicação de MULTA DIÁRIA, no valor de R\$ 20.000,00 (vinte mil reais), a incidir na hipótese de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

Por fim, iii) comuniquem-se as Plataformas Digitais para cumprimento imediato da presente decisão; e iv) diante da pertinência temática ao Inquérito 4.879, encaminhem-se os autos ao SUPREMO TRIBUNAL FEDERAL.

SIGILOSO

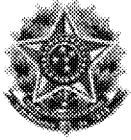
Intime-se. Publique-se.

Brasília, 30 de janeiro de 2023.

Ministro **ALEXANDRE DE MORAES**
Presidente

SIGILOSO

SIGILOSO



26/12/2022

Número: **0602037-73.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **26/12/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

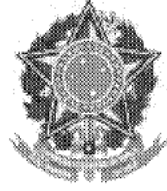
Objeto do processo: **Documentos extraídos do SEI 18920-6.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158540949	26/12/2022 16:32	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0602037-73.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado por representação realizada pelo Tribunal de Contas da União (SEI 2022.00.0001.8920-6)

A Assessoria Especial de Enfrentamento à Desinformação detectou nova estratégia golpista, baseada na divulgação de afirmações falsas de caráter sensacionalista, citando que, o Senhor Ministro do Tribunal de Contas da União fraudou o relatório de auditoria das urnas eletrônicas com o objetivo de prejudicar a credibilidade das eleições presidenciais de 2022, em um contexto de incentivo à recusa dos resultados e de defesa de ruptura institucional.

A desordem informativa em tela tem sido realizada, primordialmente, pelos seguintes perfis, canais e sites:

Twitter:

<https://twitter.com/hedilbe49136857/status/1599081107772694528>

YouTube:

<https://www.youtube.com/watch?v=MOBWb1dvK74>

Sites:

<https://dunapress.org/2022/12/03/presidente-do-tcu-fraudou-relatorio-sobre-a-auditoria-das-urnas-eletronicas/>

<https://obolsodovale.com.br/bruno-dantas-o-presidente-do-tcu-fraudou-relatorio-sobre-a-auditoria-das-urnas-eletronicas/>

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

SIGILOSO

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o processo eleitoral, na medida em que incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

SIGILOSO

Observe-se, nessa linha, que, lançar informação inverídica de suspeitas quanto à fidedignidade do processo de auditoria e apuração dos votos é conduta com alta aptidão para afetar a percepção de justiça e correção das eleições brasileiras, insuflando, como consequência, correntes minoritárias e golpistas que atentam contra a democracia em pontos esparsos do país.

A título ilustrativo, trago à colação algumas postagens realizadas no contexto analisado:

Twitter:

<https://twitter.com/hedilbe49136857/status/1599081107772694528>



Ed Lincoln
@Hedilbe49136857

"PRESIDENTE DO TCU FRAUDOU RELATÓRIO
SOBRE A AUDITORIA DAS URNAS ELETRÔNICAS"

COMPLICA-SE A SITUAÇÃO DE BRUNO DANTAS

A denúncia foi apresentada por um advogado durante audiência pública realizada no Senado Federal nesta quarta-feira 30 de novembro.

legis.senado.leg.br/comissoes/reun...

Translate Tweet



1:40 PM · Dec 3, 2022

7,446 Retweets **392** Quote Tweets **16.3K** Likes



SIGILOSO

YouTube:

<https://www.youtube.com/watch?v=MOBWb1dvK74>

**Contexto**

Uma eletrônica no Brasil

Justiça Eleitoral

O sistema de votação eletrônico brasileiro permite o exercício da cidadania com maior segurança. A urna foi desenvolvida para computar votos de forma segura e sigilosa, atendendo à demanda e às características específicas do Brasil.

GRAVÍSSIMO - PRESIDENTE DO TCU TERIA FRAUDADO RELATÓRIO SOBRE AS URNAS

Diretoria da Direita

Seja membro

Inscriver-se

42,9 mil inscritos

5 mil



Compartilhar



Valeu



Salvar

38 mil visualizações Transmitido há 2 semanas

Em meio a Audiência Pública do Senado, um fato quase passou despercebido, o Advogado Rafael Lima Freire, acusa o Atual Presidente do TCU de Ocultar Documentos da Auditoria do órgão sobre a Auditoria das Urnas Eletrônicas.

Mostrar mais

Sites:

<https://dunapress.org/2022/12/03/presidente-do-tcu-fraudou-relatorio-sobre-a-auditoria-das-urnas-eletronicas/>

SIGILOSO

CONFIDENTIAL

Presidente do TCU fraudou relatório sobre a auditoria das urnas eletrônicas



Twitter
577 seguidores
#TCU2

Compartilhar



Complica-se a situação de Bruno Dantas.

A denúncia foi apresentada por um advogado durante audiência pública realizada no Senado Federal nesta quarta-feira 10 de novembro.

Segundo o advogado, o Presidente do TCU, Bruno Dantas, responsável pela condução dos trabalhos da auditoria, omitiu no relatório final informações relevantes inseridas em um documento no qual os auditores apontaram diversas irregularidades e vulnerabilidades, entre outras situações graves encontradas durante a análise do sistema eletrônico de votação imposto pelo TSE com o aval do STF.

voce pode gostar

- Todo homem que souber disso irá navegar suas relações íntimas
- STF já não vendidos de 2019 estão quase sendo dados
- Basta 1 placa desta antes de dormir para perder 7kg em 21 dias
- Uma conferência de cima queima até 7kg de gordura pura por semana!

Esta situação é gravíssima pois não é de hoje que o TCU vem sendo utilizado de forma indevida por pessoas ligadas à Lula e seu grupo para avaliar as urnas eletrônicas e os crimes cometidos contra o Regime Representativo pelos integrantes do Poder Judiciário.

Em 2017 e então Presidente do TCU, José Muelo Monteiro, foi o responsável por um acórdão no qual o TCU afirma que a Lei do voto impresso não determinava a obrigatoriedade da impressão dos votos nas eleições de 2018, o que configura crime de falsidade ideológica.

No acórdão 2.564/2017 o TCU afirma o seguinte:

"Considerando que a mudança trazida pela Lei 13.165/2015 não faz menção expressa quanto à necessidade de implementação integral do novo processo de votação já nas próximas eleições, permanecendo silente com relação à maneira como essa mudança ocorreria, ou seja, se seria gradualmente ou de forma ampla, para todo o território nacional;"

Este acórdão foi utilizado pelo TSE na época para se esquivar da obrigação de implementar a Lei, uma vez que Gilmar Mendes, então Presidente do TSE, tentou ludibriar a população ocultando a informação de que todas as urnas eletrônicas já estavam aptas a receber as impressoras. Sua proposta era a de comprar 500 mil novas urnas eletrônicas a um custo de 2,5 bilhões de reais, alegando que as existentes não eram capazes de atender a legislação, e o que é pior, fazer isso somente após as eleições de 2018.

Seja o primeiro a ser informado

Digite seu endereço de e-mail para receber notificações de nossas publicações.

inscrição de e-mail



Magazine Lu

- PhD Judy Lettvin, a cientista que descobriu a "bala mágica" contra o câncer
- Contribua ao desenvolvimento de uma prioridade na Noruega
- Noruega, um Estado "Não-Leser", abre-se a todos as religiões
- A dupla cidadania é uma opção para você? - novas regras de cidadania na Noruega
- Feira Econômica em São Paulo

Diary Press Top Trending

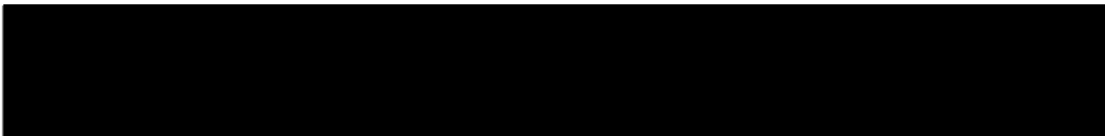
- Carta aos Oficiais Gerais
- Suécia: sobre forças armadas e condições no SPM
- Urgente: Televisão americana denunciada fraude eleitoral no Brasil
- No 1º turno, 4,8 milhões de votos foram após os STN, S&S no Nordeste. Veja mais índices de fraude
- Operação Espectro: Investigação especial de Alexandre de Moraes

Clique para ler

SIGILOSO

<https://obolsodovale.com.br/bruno-dantas-o-presidente-do-tcu-fraudou-relatorio-sobre-a-auditoria-das-urnas-eletronicas/>

SIGILOSO



SIGILOSO

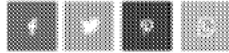
Início · Notícias · Brasil News · Bruno Dantas, o presidente do TCU fraudou relatório sobre a auditoria das urnas eletrônicas

Brasil Soberania Nacional Política

Bruno Dantas, o presidente do TCU fraudou relatório sobre a auditoria das urnas eletrônicas

São crimes gravíssimos que atentam contra a Soberania e a Segurança Nacional, portanto, por natureza, de competência da Justiça Militar.

3 de Dezembro, 2012



1008



Louvado seja Deus, que não rejeitou a minha oração nem afastou de mim o seu amor! ~ Salmos 66:20

A denúncia foi apresentada por um advogado durante audiência pública realizada no Senado Federal na quarta 30 de novembro.

Segundo o advogado, o Presidente do TCU, Bruno Dantas, responsável pela condução dos trabalhos da auditoria, ocultou no relatório final.

Informações relevantes inseridas em um documento no qual os auditores apontaram diversas irregularidades e vulnerabilidades, entre outras situações graves encontradas durante a análise do sistema eletrônico de votação imposto pelo TSE com o aval do STF.

Esta situação é gravíssima pois não é de hoje que o TCU vem sendo utilizado de forma indevida por pessoas ligadas à Lula e seu grupo para avaliar as urnas eletrônicas e os crimes cometidos contra o Regime Representativo pelos integrantes do Poder Judiciário.

Em 2017 o então Presidente do TCU, José Mucio Monteiro, foi o responsável por um acórdão no qual o TCU afirma que a Lei do voto impresso não determinava a obrigatoriedade da impressão dos votos nas eleições de 2018, o que configura crime de falsidade ideológica.

SIGILOSO

Dentro desse contexto, fica autorizado o exercício preventivo do poder administrativo para impedir a realização de ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

Ante o exposto, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral. Ante o exposto, de ordem, **DETERMINO** às plataformas Twitter, YouTube, e sites, Dunapress.org, obolsodovale.com.br, a imediata remoção das URLs indicadas, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora, a contar do prazo de 2 (duas) horas a partir do recebimento da notificação.

DETERMINO, ainda, a preservação do conteúdo postado nos últimos 7 dias dentro desses perfis, grupos ou canais, pelo período de 6 (seis) meses, com a finalidade de subsidiar eventual investigação criminal.

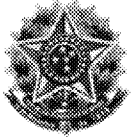
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 26 de dezembro de 2022.

Ministro **ALEXANDRE DE MORAES**
Presidente

SIGILOSO



29/12/2022

Número: **0602041-13.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **29/12/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Documentos extraídos do SEI 19036-0.**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	

Outros participantes	
Procurador Geral Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158546047	29/12/2022 17:12	<u>Intimação</u>	Intimação

**TRIBUNAL SUPERIOR ELEITORAL
SECRETARIA JUDICIÁRIA**

Brasília, 29 de dezembro de 2022.

PETIÇÃO CÍVEL (241) - 0602041-13.2022.6.00.0000 - BRASÍLIA - DISTRITO FEDERAL
RELATOR(A): MINISTRO(A) ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

INTIMAÇÃO PARA CUMPRIMENTO DE DETERMINAÇÃO JUDICIAL

A Coordenadoria de Processamento da Secretaria Judiciária do Tribunal Superior Eleitoral, em cumprimento à determinação exarada de ordem, pelo Juiz Auxiliar da Presidência, Dr. MARCO ANTÔNIO MARTIN VARGAS, **INTIMA** o provedor de aplicação ou conteúdo **TWITTER BRASIL REDE DE INFORMACAO LTDA**, por meio da qual **foi determinado que: à plataforma Twitter a imediata e definitiva remoção do perfil abaixo mencionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.**

URL: <https://twitter.com/CelMontenegroRJ>

Conforme Portaria-TSE nº 1.143, de 17 de novembro de 2016 (DJE/TSE nº 219, de 18.11.2016, p. 2-3), esclarece-se que eventuais manifestações processuais devem ser realizadas mediante acesso ao Sistema Processo Judicial Eletrônico (PJe) no endereço <https://pje.tse.jus.br/pje/login.seam>, em vista da regulamentação constante da Resolução-TSE nº 23.417, de 11 de dezembro de 2014 (DJE/TSE nº 60, de 27.03.2016, p. 40-48), permitindo-se a apresentação de petições em meio físico apenas nos casos excepcionais do art. 13, § 2º, da referida norma, e devendo a organização documental, no peticionamento, observar as diretrizes estabelecidas pela Portaria-TSE nº 1.216, de 13 de dezembro de 2016 (DJE/TSE nº 237, de 15.12.2016, p. 2.).

Para os devidos fins, segue anexa cópia do referido ato judicial.

Ivete Ferreira Marques
Coordenadoria de Processamento

**SIGILOSO**

Num. 158546047 - Pág. 1



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0602042-95.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de sítio eletrônico e perfis a ele relacionados, orientados para a divulgação de notícias falsas que atingem a integridade do processo eleitoral, em um contexto de defesa de ruptura institucional.

As manifestações em questão vêm sendo intensamente realizadas nos seguintes canais:

Sítio eletrônico: Duna Press

URL: <https://dunapress.org/>

Nome do perfil: Duna Press Jornal & Magazine

Plataforma: Gettr

URL: <https://gettr.com/user/dunapressjornal>

Nome do perfil: Duna Press Jornal & Magazine

Plataforma: Facebook

URL: <https://www.facebook.com/dunapressjornal/>

Nome do perfil: Duna Press Jornal & Magazine

Plataforma: Instagram

URL: <https://www.instagram.com/dunapressjornal/>

Nome do perfil: Duna Press Jornal & Magazine

Plataforma: Twitter

URL: <https://twitter.com/dunapressjornal>

Nome do canal: Canal Duna Press

Plataforma: Youtube

URL: <https://www.youtube.com/@CanalDunaPress>

Nome do perfil: Duna Press Jornal e Magazine

Plataforma: LinkedIn

URL: <https://www.linkedin.com/showcase/dunapressjornal/>

Nome do grupo: Canal Duna Press Jornal e Magazine

Plataforma: Telegram

URL: <https://t.me/dunapressjornal>

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o processo eleitoral e eventualmente obstaculizar a posse dos eleitos, na medida em que incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Observem-se, nessa linha, algumas passagens relevantes, apenas a título exemplificativo, das quais se extrai potencial para a ocorrência de traumas ou alterações sociais:

Nome do sítio: Duna Press

URL: <https://dunapress.org/>

dunapress.org

Updated 2 hours ago ↻



Domain Information

Domain:	dunapress.org
Registrar:	Domeneshop AS dba domainnameshop.com
Registered On:	2017-04-04
Expires On:	2023-04-04
Updated On:	2022-10-18
Status:	clientTransferProhibited
Name Servers:	ns1.wordpress.com ns2.wordpress.com ns3.wordpress.com

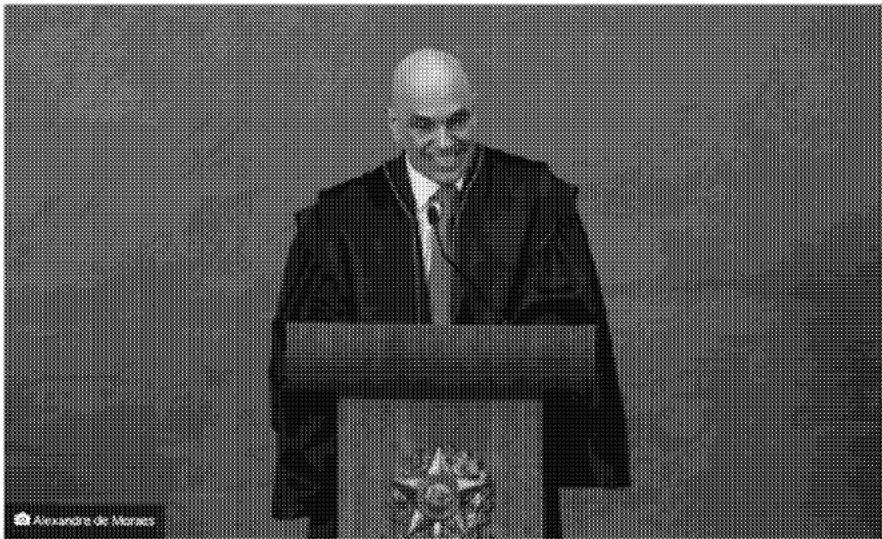


Registrant Contact

Organization:	Paulo Fernando De Barros
State:	Vestfold
Country:	NO

Imagens exemplificativas:

O Brasil tem hoje 7 presos políticos



Desde o início das manifestações contrárias a Lula, Moraes prendeu deputados estaduais, jornalista, empresário, cacique, vereador e pastor.

Nesta segunda-feira, 26, o ministro do Supremo Tribunal Federal (STF) Alexandre de Moraes determinou a prisão do jornalista Oswaldo Eustáquio e de Bismark Fugazza, humorista do Canal Hipócritas, por atos antidemocráticos, conforme noticiou a Revista Oeste. Atualmente, existem sete pessoas presas por ordem de Moraes.

Dia "D"



Mais sério do que você possa imaginar, trata-se da vitória ou derrota de uma nação em guerra!

Em códigos. Entendedores entenderão! Patriotas propagarão!



Hacker acessa telefone de Moraes e descobre envolvimento do servidor em esquemas de quadrilha



Seja o primeiro a ser informado 📧

Digite seu endereço de e-mail para receber notificações de novas publicações

Indereço de e-mail

Inscrever



Alexandre de Moraes investigado pelas FFAA:

BOMBA! Hacker expõe ligação de magistrado com ex-presidiário.


O magistrado teria formado uma quadrilha junta com Lula para desviar dinheiro da fundação eleitoral. Mais de 60 milhões foram desviados pela campanha do PT. O ministro proibiu a Polícia Federal de investigar o repasse milionário para uma empresa de fachada que pertence ao ex-presidiário.

Nome do perfil: Duna Press Jornal & Magazine

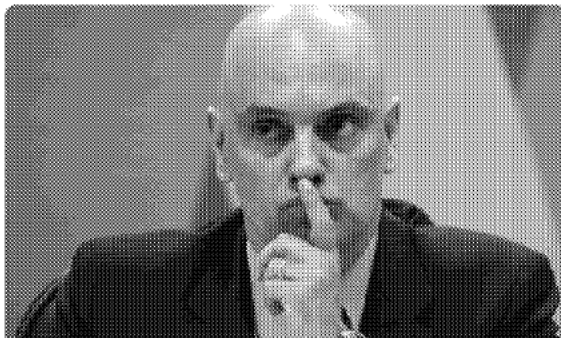
Plataforma: Gettr

URL: <https://gettr.com/user/dunapressjornal>

Imagens exemplificativas:

 **Duna Press Jornal & Magazine** @dunapressjornal · dez 26º

Hacker acessa telefone de Alexandre de Moraes e descobre envolvimento do servidor em esquemas de quadrilha




Hacker acessa telefone de Alexandre de Moraes e descobre envolvimento do servidor em esquemas de quadrilha

Alexandre de Moraes é investigado pelas FFAA por pertencer a esquemas de quadrilhas relacionadas à fraude e desvio de fundos...

👉 dunapress.org



 **Duna Press Jornal & Magazine** @dunapressjornal · dez 26º

Acampamentos patrióticos completam 57 dias de manifestações nos QGs do Brasil



Acampamentos patrióticos completam 57 dias de manifestações nos QGs do Brasil

Após o término do segundo turno das eleições 2022, milhões de brasileiros começaram manifestar-se por todo o território nacional...

👉 dunapress.org



Nome do perfil: Duna Press Jornal & Magazine

Plataforma: Facebook

URL: <https://www.facebook.com/dunapressjornal/>

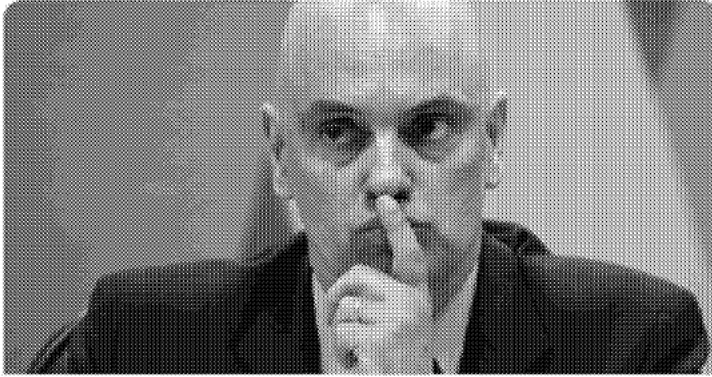
Imagens exemplificativas:



Duna Press Jornal & Magazine
@dunapressjornal

...

Hacker acessa telefone de Moraes e descobre envolvimento do servidor em esquemas de quadrilha
dunapress.org/2022/12/27/hac... via
@dunapressjornal #dunapressjornal



dunapress.org

Hacker acessa telefone de Moraes e descobre envolvimento do servidor em es...
Alexandre de Moraes é investigado pelas FFAA por pertencer a esquemas de quadrilhas relacionadas à fraudes e desvio de fundos públicos

3:03 PM · Dec 27, 2022 from Holmestrand, Norge

141 Views 3 Retweets 1 Quote Tweet 4 Likes

Nome do canal: Canal Duna Press

Plataforma: Youtube

URL: <https://www.youtube.com/@CanalDunaPress>

Imagens exemplificativas:



2022 Eleições Brasileiras
Diversas profissões apuram a integridade do processo eleitoral.

Saiba mais

O vídeo proibido por Alexandre de Moraes para a campanha eleitoral de Jair Bolsonaro

Canal Duna Press
4.32 mil inscritos

Seja membro

Inscrição em

447

Compartilhe

Compartilhe

Salve

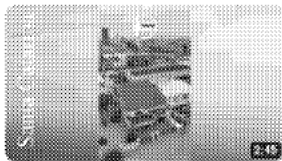
8 mil visualizações · há 3 meses

Seus direitos e liberdades estão sendo paulatinamente retirados, eles prosseguirão até concluírem a formação do Estado Socialista Mexicano no Brasil e você pode evitar que isso aconteça. Seja bem-vindo e obrigado por estar aqui, deixe seu like ou dislike, ative o sistema de notificações e compartilhe este vídeo com seus amigos e familiares.

Mostrar mais

Enviei recentemente

Populares



Chuvas fortes em Santa Catarina afetam infra-estruturas das cidades
43 visualizações · há 1 mês



QG Pernambuco - Dia 47
97 visualizações · há 11 dias



Indígenas cercam STF, militares protegem instalações
446 visualizações · há 5 semanas



Indígenas prometem defender o Brasil contra a tomada do poder
26 visualizações · há 5 semanas



Deparamento dos equipamentos do QG de Brasília
462 visualizações · há 8 semanas



Jornalista vai em prontos ao traduzir as palavras da Líder indígena Caionã
236 visualizações · há 2 semanas



Correção nacional
47 visualizações · há 1 mês



A vitória está perto
89 visualizações · há 5 meses



O mundo está sabendo / Verdades que / The world is knowing
187 visualizações · há 1 mês



O senesepers pedista para eliminar da rede o vídeo de Glória Álvares no Parlamento...
147 visualizações · há 1 mês



Ninguém toca nas crianças, diz General contra ordem do STF
22 visualizações · há 1 mês



Líderes: Bolsonaro vive o jogo, entenda o mandato de injunção
262 visualizações · há 1 mês

Nome do perfil: Duna Press Jornal e Magazine

Plataforma: LinkedIn

URL: <https://www.linkedin.com/showcase/dunapressjornal/>

Imagens exemplificativas:

Publicações na Page



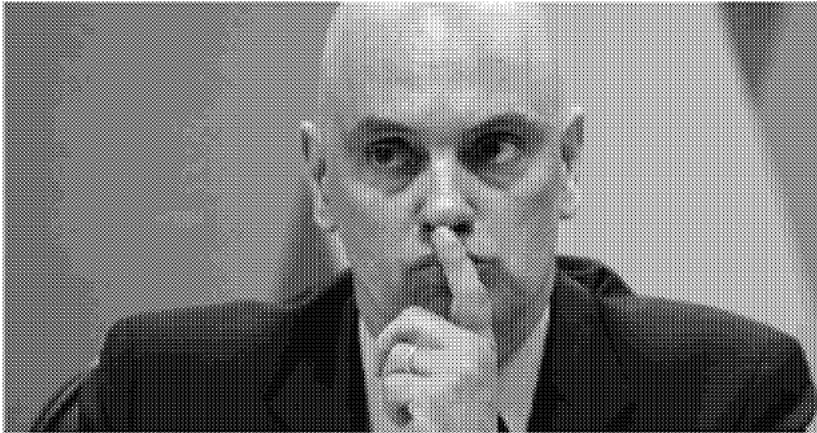
Duna Press jornal e Magazine

...

19 seguidores

21 h • 🌐

Hacker acessa telefone de Moraes e descobre
envolvimento do servidor em esquemas de ...ver mais



**Hacker acessa telefone de Moraes e descobre
envolvimento do servidor em esquemas de...**

dunapress.org • 5 min de leitura

1 compartilhamento



Gostei



Comentar



Compartilhar



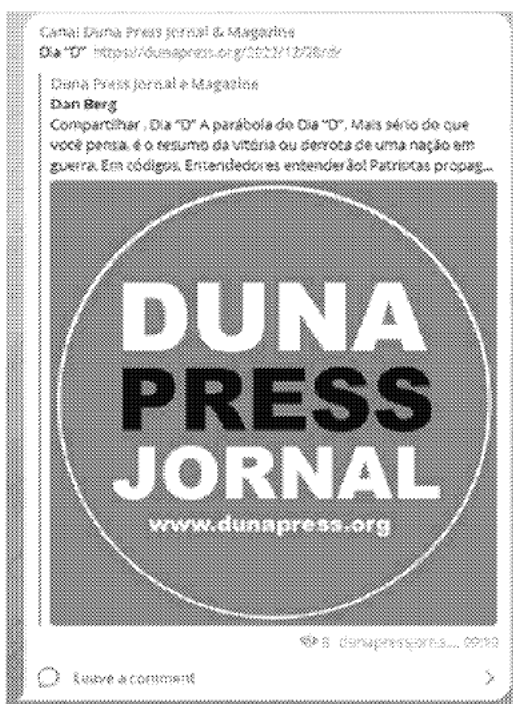
Enviar

Nome do grupo: Canal Duna Press Jornal e Magazine

Plataforma: Telegram

URL: <https://t.me/dunapressjornal>

Imagens exemplificativas:



Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar a posse dos eleitos nas Eleições Gerais de 2022. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

Ante o exposto, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, de ordem, **DETERMINO** às plataformas Facebook, Gettr, Instagram, Twitter, Youtube, LinkedIn e Telegram o imediato bloqueio canais e grupos acima mencionados, pelo período de 15 (quinze) dias, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

DETERMINO, mais, à ANATEL, que providencie o imediato bloqueio do sítio eletrônico acessado, realizando pronta notificação das empresas cadastradas no Serviço Móvel Pessoal (PMP) e no Serviço de Comunicação Multimídia (SMC), sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

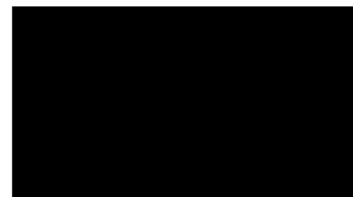
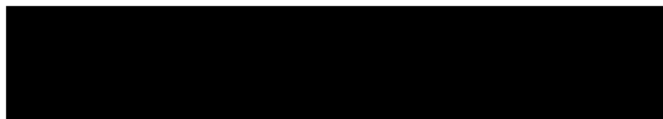
DETERMINO, por fim, à plataforma Google a imediata desmonetização do sítio apontado, por um período de 30 (trinta) dias, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

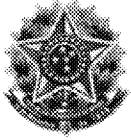
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 29 de dezembro de 2022.

Marco Antônio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral





06/01/2023

Número: **0600003-91.2023.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **04/01/2023**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

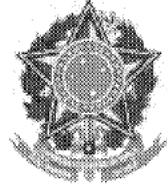
Objeto do processo: **Documentos extraídos do processo SEI nº 2022.00.00019105-7**

Segredo de Justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Advogados	
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)			
Outros participantes			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
158548104	05/01/2023 12:21	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0600003-91.2023.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que detectou, nesta data, perfil mormente orientado para a propagação de desinformação contra as eleições e apologia à intervenção militar, mantido pelo blogueiro foragido Oswaldo Eustáquio:

Nome do perfil: Brasil Podcast

URL: <https://twitter.com/brasilpodcastbr>

Número de seguidores: 77,3 mil



Brasil Podcast @brasilpodcastbr · 6 h

...

Me respondam uma pergunta, quem é o presidente da República em exercício no Brasil neste exato momento? Aonde está publicado este ato? Caso não haja publicação, me recordo de Ranieri Mazili declarar a vacância do cargo pouco antes dos militares assumirem em 1964.

11,4 mil

58

34

363



SIGILOSO



Brasil Podcast @brasilpodcastbr · 30 de dez

...

Bolsonaro falará amanhã. Confirmado. Oremos pela nossa nação. Eu acredito!

40,6 mil

109

98

1.267



Brasil Podcast @brasilpodcastbr · 29 de dez

...

URGENTE: Bolsonaro acionou Conselho de Defesa Nacional na tarde desta quinta-feira (29). O órgão dispõe, entre outras coisas sobre consulta para questões de guerra ou Estado de Sítio. A convocação ocorre no mesmo dia que o DOU mostra compra de insumo de material bélico para GLO.

129,7 mil

270

902

5.224



SIGILOSO

SIGILOSO



Brasil Podcast @brasilpodcastbr · 28 de dez

...

Oswaldo Eustáquio mostra vulnerabilidades de código fonte do TSE. Essas são linhas maliciosas que as FFAA disseram as urnas estarem sujeitas



6 mi 6.416 13,5 mil 10,3 mil

S

SIGILOSO



Brasil Podcast @brasilpodcastbr · 17 de dez

...

A denúncia que revela a indicação feita por Alexandre de Moraes de Gabriel Chalita, sócio de sua mulher à ministro da Educação revela a promiscuidade do sistema e o crime de lesa pátria por uma quadrilha que usou a máquina do TSE para catapultar um ladrão ao cargo de presidente.

👍 92,1 mil

💬 89

↻ 1.781

❤️ 6.412



Brasil Podcast @brasilpodcastbr · 17 de dez

...

URGENTE: o sócio da esposa de Alexandre de Moraes, o advogado Gabriel Chalita foi o principal articulador da chapa Lula/Aickmin. Pior, a Veja de hoje revela que Moraes indicou Chalita para ser Ministro da Educação do Nine. Em resumo, Moraes utilizou a estrutura do STF/TSE para si

👍 621,7 mil

💬 2.717

↻ 10,9 mil

❤️ 38,8 mil



Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

SIGILOSO

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a consequente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

O caráter ilícito das postagens comprovado pela presença de chamados indiretos a atos populares com o fim de tumultuar a posse dos eleitos no pleito presidencial de 2022.

Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma Twitter a imediata e definitiva remoção do perfil acima mencionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

Brasília, 4 de janeiro de 2023.

Marco Antônio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

SIGILOSO



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0600004-76.2023.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

**RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL**

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, concernente a perfil golpista que incentivam a ideia de uma intervenção militar, no contexto dos atentados violentos às sedes dos três Poderes, ocorridos nesta data, em contraposição à legítima expressão do voto popular registrada no pleito presidencial de 2022:

Perfil: Junior Melo Terra

URL: <https://twitter.com/juniormelom>

Número de seguidores: 74,7 mil

Postagens (rol exemplificativo):

Junior Melo TERRA                                  

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez e a eficácia do processo eleitoral, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à ruptura institucional, com a conseqüente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

É evidente que as postagens possuem potencial para tumultuar o cenário político, na medida em que, explicitamente, incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios violentos, como os ocorridos hoje.

Trata-se de condutas ilegais de natureza grave, que autorizam o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

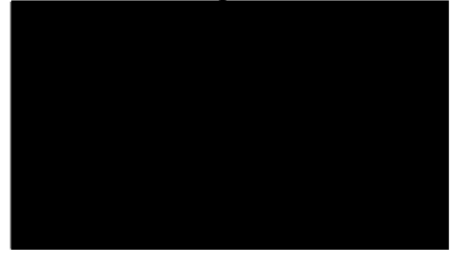
Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma assinalada a remoção definitiva e imediata do perfil relacionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, **contada a partir do término da primeira hora após o recebimento da notificação**.

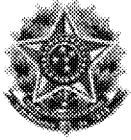
Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 8 de janeiro de 2023.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral





01/02/2023

Número: **0600004-76.2023.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **08/01/2023**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Documentos extraídos do SEI 140-7**

Segredo de Justiça? **SIM**

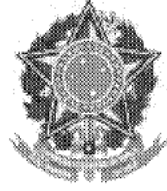
Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	

Outros participantes	
Procurador Geral Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	Data da Assinatura	Documento	Tipo
158589864	31/01/2023 19:28	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0600004-76.2023.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de perfil nas redes sociais, orientado para a divulgação de desinformação contra as eleições e apologia à intervenção militar, em detrimento da vontade popular registrada nas Eleições 2022.

Por meio da decisão de ID 158549238, determinei a suspensão do perfil de Junior Melo Terra, nos seguintes termos:

Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** à plataforma assinalada a remoção definitiva e imediata do perfil relacionado, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, **contada a partir do término da primeira hora após o recebimento da notificação.**

É o breve relato. Decido.

O art. 4º da Res.-TSE 23.714/2022 tutela a higidez, a integridade e a credibilidade das Eleições e do processo eleitoral, de modo a coibir práticas que, por meio da divulgação desinformações, representam substancial transgressão à própria Democracia:

Art. 4º. A produção sistemática de desinformação, caracterizada pela publicação contumaz de informações falsas ou descontextualizadas sobre o processo eleitoral, autoriza a determinação de suspensão temporária de perfis, contas ou canais mantidos em mídias sociais, observados, quanto aos requisitos, prazos e consequências, o disposto no art. 2º.

Parágrafo único. A determinação a que se refere o caput compreenderá a suspensão de registro de novos perfis, contas ou canais pelos responsáveis ou sob seu controle, bem assim a utilização de perfis, contas ou canais contingenciais previamente registrados, sob pena de configuração do crime previsto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

SIGILOSO

Verifica-se, dessa forma, que a incidência do dispositivo mencionado destina-se, de forma restrita, a condutas abusivas que, longe de constituir legítima manifestação de direitos constitucionalmente garantidos, caracterizam comportamento imoral ou ilícito, uma vez que, *"a desinformação - entendida como uma ação comunicativa fraudulenta, baseada na propagação de afirmações falsas ou descontextualizadas com objetivos destrutivos - conflita com valores básicos da normativa eleitoral, na medida em que impõe sérios obstáculos à liberdade de escolha dos eleitores e, adicionalmente, à tomada de decisões conscientes"*, comprometendo, *"portanto, a normalidade do processo político, dada a intenção deliberada de suprimir a verdade, gerando desconfiança, com conseqüente perda da credibilidade e fé nas instituições da democracia representativa"* (Voto que proferi na ADI 7.261-MC, julgado em 25/10/2022).

De fato, não há, no ordenamento jurídico, direito absoluto à liberdade de expressão, ou seja, como bem enfatizou o Ministro EDSON FACHIN, *"não há direito no abuso de direito"* (ADPF 572, Rel. Min. EDSON FACHIN, Pleno, DJe de 7/5/2021), de modo que *"não se pode utilizar um dos fundamentos da democracia, a liberdade de expressão, para atacá-la. O sistema imunológico da democracia não permite tal prática parasitária que deverá ser sempre coibida à luz da práticas concretas que visam atingir a integridade do processo eleitoral"* (ADI 7.261-MC, Rel. Min. EDSON FACHIN, Pleno, julgado em 25/10/2022).

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio "LIBERDADE e RESPONSABILIDADE"; não permitindo - como ocorrido nas presentes hipóteses - de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da "liberdade de expressão" como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e preconceituosos!

Considerado que houve a cessação de divulgação de conteúdos revestidos de ilicitude e tendentes a transgredir a integridade do processo eleitoral, a fim de possibilitar que os envolvidos possam retornar a utilizar suas redes sociais dentro do mais absoluto respeito à Constituição Federal e a Legislação, com observância do já citado binômio LIBERDADE – RESPONSABILIDADE, DETERMINO:

i) a reativação da conta de Junior Melo Terra na plataforma digital Twitter, mantendo-se, porém a remoção das postagens irregulares veiculadas; e

ii) a aplicação de MULTA DIÁRIA, no valor de R\$ 20.000,00 (vinte mil reais), a incidir na hipótese de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

Por fim, iii) comunique-se a Plataforma Digital para cumprimento imediato da presente decisão; e iv) diante da pertinência temática ao Inquérito 4.879, encaminhem-se os autos ao SUPREMO TRIBUNAL FEDERAL.

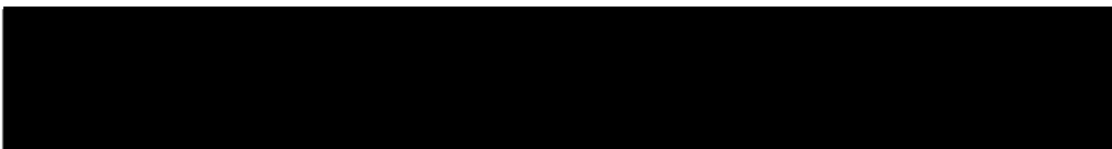
Intime-se. Publique-se.

Brasília, 31 de janeiro de 2023.

Ministro **ALEXANDRE DE MORAES**

SIGILOSO

SIGILOSO



SIGILOSO



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0600011-68.2023.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES
INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, concernente a grupos e perfis utilizados para divulgar desinformações e celebrar os atos terroristas de 8 de janeiro, com postagens que possuem aptidão para insuflar novos atos golpistas, como o planejado para hoje, na capital federal.

As postagens foram realizadas nos seguintes grupos e perfis:

TELEGRAM:

<https://t.me/opequenomenino>

<https://t.me/patriotasbrasileiros1>

<https://t.me/brazillianspring>

<https://t.me/brasilpatriotanoticias>

<https://t.me/brpatriotas>

<https://t.me/patriotismopelobrasil>

<https://t.me/patriotaslelobrasil>

<https://t.me/soubrasileiropatriota>

<https://t.me/patriotismodobrasil>

https://t.me/patriotismodobrasil_2

<https://t.me/patriotabrasil3>

<https://t.me/cristaospelapatria>

<https://t.me/verdeolivabrasil>

<https://t.me/BrazilConvoy>

https://t.me/Brasil_Livre

<https://t.me/REGIAONORDESTEBR>
<https://t.me/REGIAOSUDESTEDOBRASIL>
<https://t.me/helpbrazill>
<https://t.me/brazilianspring2022>
<https://t.me/operacaojaguar>
<https://t.me/atitudo262>
https://t.me/Amigos_Secretos
<https://t.me/REGIAOSUDESTEDOBRASIL>
<https://t.me/SOSordemEprogresso>
<https://t.me/OrdemEprogressoBrasilSOS>
<https://t.me/ordemepressopr>
<https://t.me/ordemprogressobrasil>
<https://t.me/Artigo142Federall>
<https://t.me/promover142>
<https://t.me/Artigo142Federal>
<https://t.me/familiapenaporta>
<https://t.me/JuventudeRevoltadaChat>
<https://t.me/JuventudeRevolitada>
<https://t.me/brazilwaastolen>
<https://t.me/erafascista>
<https://t.me/nosquarteis>
<https://t.me/quartafeiramanifesto>

Chat ID: -1001414618905

Chat ID: LIBERDADE!!

Chat ID: -1001305511393

Chat ID: Balneário Camboriú

Encaminhamos abaixo exemplos colhidos, por amostragem, para fins de ilustração:

#BrazilianSpring

3,477 subscribers

forwarded from governo nacional

*CARAVANAS da liberdade para BRASÍLIA QG

ESPÍRITO SANTO

ROTA: Vitória, Guarapari, Ibatiba, Realeza MG, João Molevard MG,

Belo Horizonte, Brasília

INFORM: clique no link de zap abaixo

wa.me/5527601665339 Jho



GOIAS

ROTA: Goiânia, BSB

INFORM: clique no link de zap abaixo

wa.me/556296176921 Heleno



MINAS GERAIS

ROTA: BH, 7 Lagoas, Pacaratu, Rod. 040, BSB

INFORM: clique no link de zap abaixo

wa.me/5531993667471 Bruno



SANTA CATARINA

ROTA: Florianópolis, BSB

INFORM: clique no link de zap abaixo

wa.me/5548984355604 Rodrigo



SÃO PAULO

ROTA: Metrô Tietê (Ao lado do hotel Ibis), Marginal Tietê, Jundiaí,

Campinas e vários pontos na via Anhanguera, BSB

INFORM: clique no link de zap abaixo

wa.me/5311957034398 Lucinha



SÃO PAULO

ROTA: Rib. Preto, Franca, Uberaba, Uberlândia, Catalão, Cristalina,

BSB

INFORM: clique no link de zap abaixo

wa.me/5516993646104 Ana



SÃO PAULO

ROTA: Guarã, todo o Vale do Paraíba, Região de Campinas: Ribeirão,

WhatsApp.com

Jhon

Business Account



1099 2149

Brazilian Spring 2022

409 subscribers

Pinned message

Este final de semana se tornará provavelmente o final de sem

2

192 2343

6 comments

Brazilian Spring 2022

O Bravo Povo do Brasil Continua Contra o Socialismo e Por Eleições Livres e Justas. [Vídeo apenas em inglês]

"The Brave People Of Brazil Continue To Stand Against Socialism and For Free and Fair Elections."

Link

https://frank.speech.com/video/brave-people-brazil-continue-stand-against-socialism-and-free-and-fair-elections

Compartilhe este conteúdo e siga nosso canal:

Share this content and follow our channel:



t.me/brazilianspring2022

#brasil #brasil #brasilwasmobilen #brazilianspring #tuta #bolsonaro #primaverabrasileira #urnas #gvevegeral

FrankSpeech.com

The Brave People Of Brazil Continue To Stand Against Socialism and For Free and Fair Elections



239 30:08

6 comments

Verde Oliva

10,841 members

Pinned message

Amados o grupo seguirá chat livre Desejo manter a democracia

Verde Oliva

10,841 members

Pinned message

Amados o grupo seguirá chat livre Desejo manter a democracia

Ercilia

4 FEIRA 11 DE JANEIRO MEGA MANIFESTAÇÃO NACIONAL

PELA RETOMADA DO PODER

EM TODAS AS CAPITAIS 18H

- BRASILIA - ESPANADA
- SÃO PAULO - AV. PAULISTA
- RIO DE JANEIRO - POSTO 5 COPACABANA
- BELOHORIZONTE - PRAÇA DA LIBERDADE
- RECIFE - PELA DA BOA NOÇÃO
- CURITIBA - CENTRO CÍRCO
- PORTO ALLEGRE - PRAÇA
- SALVADOR - TRAVESSIA DA BARRA
- COIMBRA - ALTO DO PINHO POA
- CIENFUEGOS - PRAÇA BASTIÃO
- LIÑARES - PRAÇA VASCO BRAGA
- FLORIANÓPOLIS - ST. BERNARDO
- BOGOTÁ - PRAÇA DO PARA
- BRASÍLIA - OLA PRAÇA/PLANINA
- MACEIÓ - PRAÇA VISTA ABREIA
- FORTALEZA - AVENIDA COSTEIRA
- SITIAL - PRAÇA CRICA
- SANTO LUIS - PRAÇA
- PORTO VELHO - AVENIDA TERNATEIRO
- MANAUS - AVENIDA BELGI FALGADO BOA VISTA
- BOBRAGOS

06:22

Alexandre Wagner



PATRIOTAS DO BRASIL

✳ Não Desistir - Não Recuar - Liberdade!!!

✳ Marchas Pacíficas com Faixas S.O.S Brasil

✳ Ordem de Prisão? Posição de Resistência Civil Pacífica (todos sentar no chão e cantar hino nacional)

=> Na guerra, a verdade é a primeira vítima. O inimigo semeia discórdia, ele sabe que o reino dividido não subsiste.<=

✳ Bolsonaro Não Entregou os Pontos, Patriotas, as Forças Armadas são 100% Patriotas e maior que muitos imaginam - Fiquem Firmes. ✳ Ficar a Pátria Livre ou Morrer Pelo Brasil Marinha, Exército, Aeronáutica ✳

✳ Deus Conosco !!!

✳ O ladrão não vem senão a roubar, a matar e a destruir; Eu vim para que tenham vida e a tenham com abundância... Mas a salvação dos justos vem do Senhor; Ele é a sua fortaleza no tempo da angústia.

✳ Alexandre Wagner, Brasileiro, Capelão, filho de militar do Exército, ex-aluno do Colégio Militar de Brasília, 30 anos na Caserna, servi com Gen-Helena e muitos outros Patriotas - Deus conosco Brasil

41 | 06:01

O PEQUENO MENINO

26.129 subscribers

O PEQUENO MENINO

26.129 subscribers

O PEQUENO MENINO

Ordem dos Advogados Conservadores do Brasil-OACB
@AdvogadosOacb

Aproveitamos e informamos, ainda, que já acessamos os manifestantes detidos constatando, infelizmente, a veracidade da informação quanto ao falecimento de uma senhora, divulgado nas redes sociais.

Translate Tweet

9:52 PM · Jan 9, 2023 · 409.2K Views

5.507 Retweets 678 Quote Tweets 10K Likes

Eles confirmaram a morte. Só acredito que ela está viva se mostrar ela realmente VIVA. Caso contrário, nós já sabemos como o sistema funciona.

Sigam nosso canal @opequenomenino e fiquem por dentro dos bastidores da notícia!

88 77 2 2

5679 21:38

99 comments

TIKTOK
@jackoliveirahhh

Sair Bolha

Será que ele está certo?

Xandão burla a lei de terrorismo para criar campo de concentração do PT.

Sigam nosso canal @opequenomenino e fiquem por dentro dos bastidores da notícia!

131 11 7 2

5631 12:33

14 comments

PATRIOTAS 🇧🇷 BRASIL 🇧🇷 🇧🇷 🇧🇷 🇧🇷
513 subscribers

November 5

PATRIOTAS 🇧🇷 BRASIL 🇧🇷 🇧🇷 🇧🇷 🇧🇷
<https://youtu.be/Cyja5i8PNvY>

YouTube
FR4UDE NAS EI_EIÇ0ES 2.022
@jair Bolsonaro



2
1778 09:58


3 comments

PATRIOTAS 🇧🇷 BRASIL 🇧🇷 🇧🇷 🇧🇷 🇧🇷
A fraude está clara !!!!
2
1323 09:59

11 comments

← Brasil No se Rinde
10.610 subscribers

Brasil No se Rinde
Forwarded from Movimento Patriotas 🇧🇷



44 41 25 15 1

January 6

Brasil No se Rinde
Forwarded from Movimento Patriotas 🇧🇷
Ninguém ganha a guerra com flores 🇧🇷.

Mostra sua força BRASIL 🇧🇷 🇧🇷

92 8 5 1 2088 17:05

Brasil No se Rinde
Forwarded from Movimento Patriotas 🇧🇷
Façam esse vídeo percorrer todos os quartéis para que todos os coronéis vejam isso ainda hoje

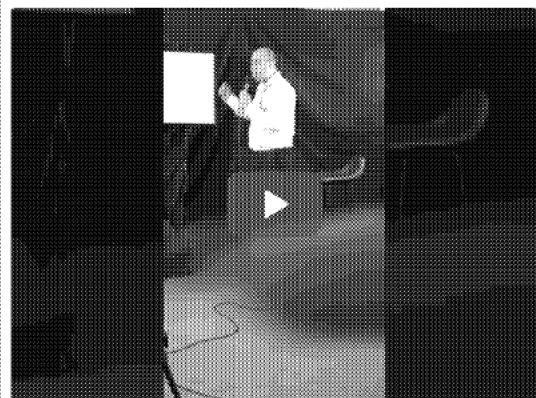
24 1 2646 18:07

PATRIOTAS BRASIL
512 subscribers

November 1

PATRIOTAS BRASIL
<https://youtu.be/Cyja5t6PNvY>

YouTube
FRAUDE NAS EI_EIÇ0ES 2.022
@jair Bolsonaro



2

12:33 06:58

3 comments

PATRIOTAS BRASIL
A fraude está clara !!!!

2

13:23 09:59

11 comments

Brasil Patriotas Noticias
772 subscribers

Brasil Patriotas Noticias
<https://youtube.com/shorts/qgzDRW5Kie7?feature=share>

YouTube
Agora congresso invadido #shorts



312 16:41

Brasil Patriotas Noticias
<https://youtu.be/GjTcXL25VW4>

YouTube
Porta do xandão foi levada pra tomar sol #shorts



309 16:55

Patriotas pelo Brasil

1.504 subscribers

Patriotas pelo Brasil

GRAVE: Segundo o Senador Marcos do Val, Flávio Dino e possivelmente Lula já sabiam com 1 dia de antecedência que a invasão aos 3 Poderes ocorreria.

- Por quê prevaricaram?

17 6 3 2 681 08:06

5 comments

Patriotas pelo Brasil

POLÍCIA FEDERAL

Demônio!! Esse cara é psicopatia pura!! Não tem um fdp de coragem pra parar esse verme???

34 2 1 653 21:35

11 comments

Patriotas pelo Brasil.

2.152 subscribers

Patriotas pelo Brasil.

00:35

FORAM PAGOS PARA SE INFILTRAR NAS MANIFESTAÇÕES E QUEBRAR TUDO

BASTIDOR

QUEM TÁ PAGANDO? XANDÃO? PT?

715 09:53

PATRIOTAS BRASIL
500 members

Pinned message
⚠️ ATENÇÃO PATRIOTAS ⚠️ ⚙️ Regras gerais: 🚫 Proibido postar qualquer assunto

Sandrinho Conceição
Rapaziada,
Estão levando em vários grupos a idéia de ao invés de ir no Congresso e quebrar tudo que já é errado mais mesmo assim foram lá e fizeram.
E aconteceu o que aconteceu ,os infiltrados com situação armada etc ...
E para completar vem o consórcio Globo.
Porque ao invés de fazer a merda no congresso que não tinha ninguém estava vazio...
Porque não arrebentar a Globo,
Eles que são o Coringa do Baralho.
O negócio é na globo gente.
Já que estamos fundidos lascados de condensados.
Porque não acabar com a Globo Rio e São Paulo?!

04:52

PATRIOTAS BRASIL
500 members

Pinned message
⚠️ ATENÇÃO PATRIOTAS ⚠️ ⚙️ Regras gerais: 🚫 Proibido postar qualquer as

OPEN WITH 10:54

Pessoal, estou aqui em Barueri...precisamos de apoio! Pouquíssimas pessoas aqui...pessoal da região e de Sp venham pra cá 10:54

NEUZILENE
Pessoal de Brasília e para ir esplanada e para tomar Poder? 11:09

Estão enrolando PIVO DE NOVO? PELOR DE DEUS, REM TOMAR ESPLANADA , NAO E QUARTEIS Q GS 11:20

Acorrdaaa 11:21

Quem tá BRASÍLIA E FESTA DA SELMA EM ESPLANADA 11:21

E AGORA OU NUNCA 11:21

PATRIOTAS BRASIL
500 members

Pinned message
⚠️ ATENÇÃO PATRIOTAS ⚠️ ⚙️ Regras gerais: 🚫 Proibido postar qualquer a

Valéria Costa Reply

Foto de Valéria Costa 11:22

Cristãos pelo Brasil
16,590 subscribers

Pinned message
⚠️ ⚙️ JEDEU SINCEROT ⚙️ O BRASIL JÁ ABOLIU

Cristãos pelo Brasil
Cristãos pelo Brasil
Vídeo que o Bolsonaro postou no Facebook, repas...
Explodam esse vídeo no whatsapp, em todas as redes sociais
7 3 1 1459 01:18
11 comments

Cristãos pelo Brasil
18,991 subscribers

Pinned message
O BRASIL JÁ ABOLIU

Cristãos pelo Brasil

ELEITO PELO POVO, ELE FOI ESCOLHIDO E ELEITO PELO STF E TSE

03:30

Kwai @Xavier-312091

Dr. Felipe Gimenez

Procurador Felipe Giménez

lula não foi eleito pelo povo brasileiro

Vídeo que o Bolsonaro postou no Facebook, repassem em todos os grupos (o risco do telegram ser bloqueado pelo Alexandre de Moraes é REAL)

visitem nosso canal @cristaospelapatna

40 2

23:24 00:53

1 comment

Brazil Convoy
2,190 members

Pinned message
16 - O povo Brasileiro, exige o imediato banimento de todos os maçons e sionis

Forwarded from Luiz jr

Pessoal venho através dessa mensagem avisar que a dona Nilma, voluntária que ajudava servir café, lanches...trabalhava na barraca de frente a Escola de Cadetes Campinas, veio a falecer dentro do ginásio federal em Brasília meus sentimentos a família e amigos uma patriota que morreu por nós lutando pelo nosso país.

00:47

Official Brazil Convoy 2022 Chat
503 members

Pinned message
O [user] ficou hospedado no Hotel desde o primeiro dia da posse, com a desculpa
Uetaine: A saia do molusco [user] foi a unica que nao foi invadida. [reactions] 148 22:57

Bel Sacramento
[user] Official Brazil Convoy 2022
PF prende ex-comandante da PM por determinação de M...
Esse careca só manda???? Cadê a marinha, exército, guerrilheiros de plantão pra dar um fim nessa palhaçada?? SÓ ESSE CARECA QUE MANDA? PORQUE OS SOLDADOS TEM TANTO MEDO DESSE CARECA E NÃO FAZEM NADA PRA LIBERTAR OS INOCENTES?? JA FOI PROVADO QUE ESSA PRISCILA EM COMPANHIA DE OUTROS COMUNISTAS FIZERAM A BADERNA! MEU DEUS CADÊ A JUSTIÇA!!!!!!!!!!!! DESSE PAÍS???? STF TENHO CERTEZA QUE NÃO É!! 23:11


Gumball Watterson
Bel Sacramento
Esse careca só manda???? Cadê a marinha, exército, guerrilheiro...
Não é por medo não filho. É cautelosa estratégica, pra dar certo tem que haver clareza de quem está certo e quem está errado. Não podemos ser irresponsáveis a ponto de colocar o processo em risco. Está sendo preparado com carinho. [reactions] edited 23:25

BRASIL LIVRE"
94 subscribers

April 19, 2022

BRASIL LIVRE"
https://twitter.com/Brasil_Livre/status/1520221643192344576?ref=YHS6wHR6yB4uSGG9F0Tcw&ts=19

Twitter
A Ademar A
ELEIÇÕES SOBRE SUSPENSE? SERÁ? #ColsonoroNelas Por Um #Brasil Livre, e Um Mundo Melhor...Todos Seguem SDV MUITO OBRIGADO!



155 A Ademar A, 23:02

Leave a comment

REGIÃO NORDESTE DO BRASIL JUNTOS

173 members

Adm

Forwarded from OS INFORMANTES



Gustavo Gayer
@GayerJus

Advogados da OAB DF acabaram de sair da PF onde os manifestantes estão detidos e disseram que estão chocados com o fato de terem crianças presas CRIANÇAS!!!!!!

Therese Peres

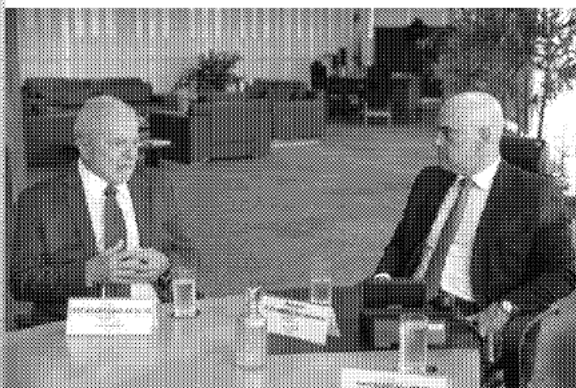
8:23 PM - Jan 9, 2023

19.8K Views 1,103 Retweets 111 Quote Tweets 3,922 Likes

Segue @OINFORMANTES

1343 22:01

Forwarded from OS INFORMANTES



Campos de concentração para os patriotas?!

Segundo Governo Vermelho, as pessoas detidas e presas permanecerão assim até que seja apurado todo o inquérito sobre o atentado de domingo (praticado pelos petistas infiltrados e que já estavam lá dentro).

São aproximadamente 1.500 pessoas SEQUESTRADAS e entre elas várias crianças, que permanecerão no campo de concentração sob a alçada da Justiça brasileira e das frouxas armadas.

Muitos passando mal e estão o dia todo sem comer e uma mulher já MORREU.

Segue @OINFORMANTES

1318 22:01

REGIAO SUDESTE DO BRASIL JUNTOS

455 members

Visitem nosso canal: @cristaospelapala

4593 22:24

Forwarded from CANAL O DESPERTAR



CADA VEZ MAIS CONVENCIDO QUE O EXÉRCITO NOS PROTEGEU DESMOBILIZANDO OS ACAMPAMENTOS.

OLHEM ESSE VÍDEO ISSO É DENTRO DA FILCRUZ INCITANDO AS PESSOAS A ATACAREM AGENTE.

ELES QUEREM UMA GUERRA CIVIL. BASTA OLHAR A PUBLICAÇÕES DO JANONES

INTERVENÇÃO MILITAR NOS TRÊS PODERES JÁ.

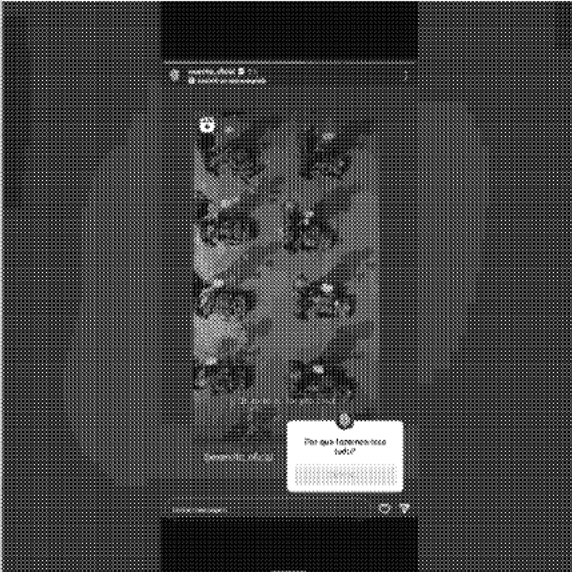
Entre no nosso Grupo

<https://t.me/+PHtHtER8o1d9InjX>

1754 22:26

LIBERDADE BRASIL • PATRIOTAS
149 subscribers

Leave a comment



LIBERDADE BRASIL • PATRIOTAS

🚩 | O PERFIL OFICIAL DO EXÉRCITO BRASILEIRO ABRIU UMA CAIXINHA DE PERGUNTAS NO STORIES. VAMOS FAZER NOSSA PARTE MAIS UMA VEZ E PEDIR QUE NOS AJUDEM !

---> LINK DO STORIES NO INSTAGRAM !

👤 | SIGA: @LiberdadeBrasil_BrazilianSpring
👥 | GRUPO: t.me/+sMawZfCMNoc5MDhh

Faça parte do canal e ajude a compartilhar as ultimas noticias e informações da nossa Direita. Vamos juntos lutar pelo Brasil.

DEUS, PÁTRIA, FAMÍLIA E LIBERDADE ! 🇺🇵

👍 1 🗨️ 1027 Gabrle10, | ... 19:36

1 comment

LIBERDADE BRASIL • PATRIOTAS
149 subscribers

LIBERDADE BRASIL • PATRIOTAS



Bolsonaro TV
@bolsonaroTV

16-10 - 12 dez 22

👁️ 12.3K 🗨️ 902

🚩 | ESTÁ CHEGANDO A HORA DO XEQUE-MATA !

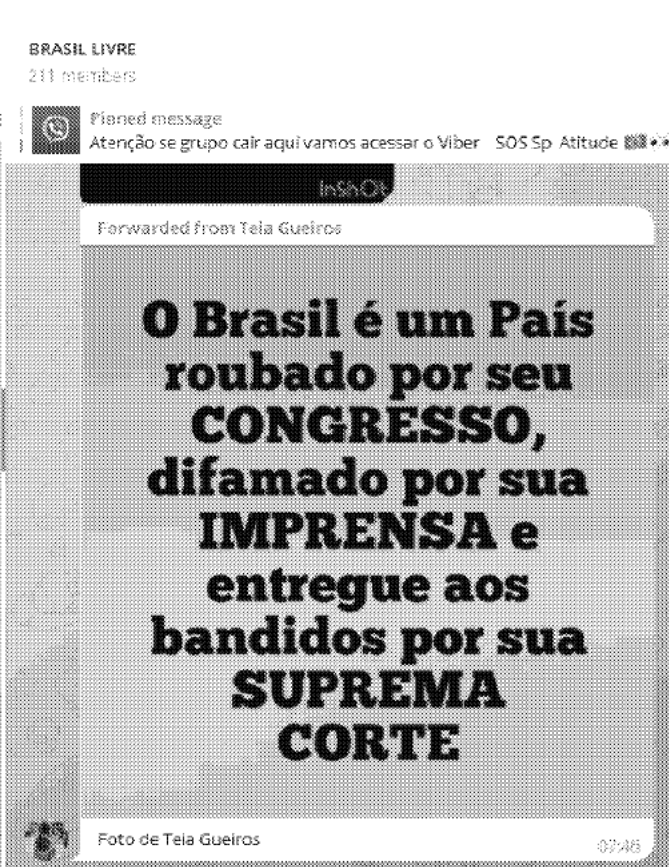
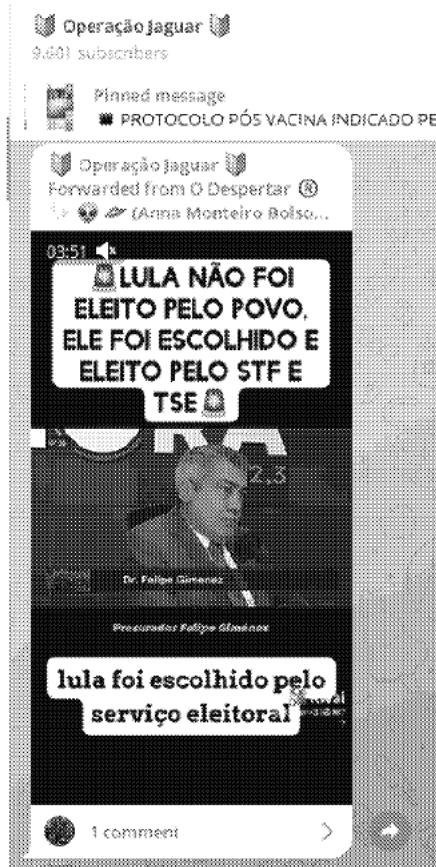
👤 | SIGA: @LiberdadeBrasil_BrazilianSpring
👥 | GRUPO: t.me/+sMawZfCMNoc5MDhh

Faça parte do canal e ajude a compartilhar as ultimas noticias e informações da nossa Direita. Vamos juntos lutar pelo Brasil.

DEUS, PÁTRIA, FAMÍLIA E LIBERDADE ! 🇺🇵

👍 870 Gabrle... edited 15off

Leave a comment



AMIGOS SECRETOS

610 members

ineelmente ainda tem aqueles que insistem em seguir adestradores de manadas... Compartilhem Geral!

02:05

Forwarded from GeFazioBreakingNews



LORVEL ROCHA AFIRMA QUE O POVO TEM MAIS PODER QUE AS FFAA E O ESTADO. MAS NÃO SABE O PODER QUE TEM...

@GeFazioBreakingNews

2539 02:11

REGIÃO SUDESTE DO BRASIL JUNTOS

456 members

Frankly Rodrigues



Erica Gorga

@EricaGorga

A Globo teve coragem de dizer que é fake news que crianças estivessem passando fome e sede no ginásio cárcere. Mas não desmentiu que havia crianças. A Globo não tem vergonha de tentar disfarçar o crime hediondo da prisão de crianças entre 1500 pessoas presas, muitas ilegalmente.

07:09

SOS, Ordem e progresso

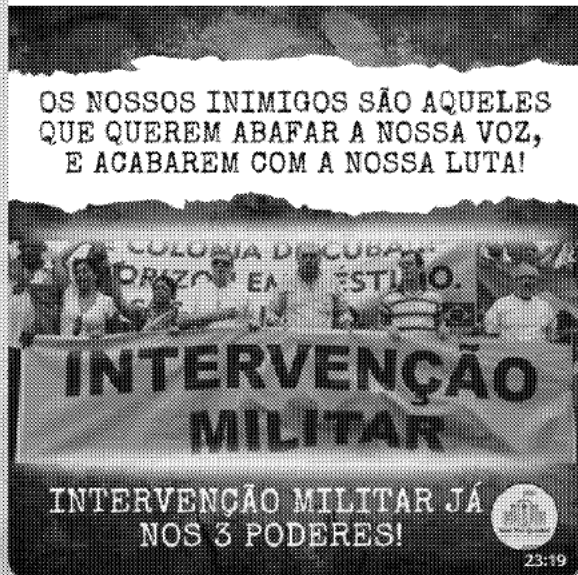
109 members, 1 online



Pinned message #1294

Assista a "HONRA A QUEM TEM HONRA - AOS COVARDES O DESPREZO" no YOUT

Forwarded from Ivone Marquezini Da Costa Marquezini Da Costa



CANAL SOS, Ordem E Progresso

107 subscribers



Pinned message

X COMUNICADO IMPORTANTE X

Para todos os amigos e

Forwarded from Deleted Account




Movimento Ordem e Progresso

382 members

noticiar estes fatos. 5790 13:10

Rafael Dos Anjos
Forwarded from Investor Brazil



Campo de concentração de detidos na Polícia Federal faz mais uma vítima, segundo vídeo

@InvestorBrazil

URGENTE - "Campo de concentração" da Polícia Federal faz mais uma vítima em menos de 24 horas, veja vídeo (cenas fortes).

VEJA: <https://investorbr.com/campo-de-concentracao-de-detidos-na-policia-federal-faz-mais-uma-vitima-segundo-video/>

Via: @InvestorBrazil

COMPARTILHEM !! Compartilhe nos grupos esta notícia. Só assim todas as pessoas vão ter acesso a tudo que está acontecendo no Brasil neste momento. A grande mídia não vai noticiar estes fatos.

7197 13:29

Ordem e Progresso Brasil

97 subscribers

Pinned message
<https://youtube.com/shorts/VEOoVGwJ3EA?feature=share>

INVASÃO AO STF: porta do gabinete de Alexandre de Moraes



941 20:20

Leave a comment

Ordem e Progresso Brasil
CADEIRA do Xandão!!!

<http://par/youtube.com/shorts/5QldP1iCeiU?feature=share>

YouTube
CADEIRA DO XANDÃO



952 20:09


Artigo 142 da Constituição Federal
89 members · 1 online

Pinned message #215
Assista a "HONRA A QUEM TEM HONRA - A

Forwarded from Leonna Prata

00:33 ◀

**CAMINHONEIRO
ESTACIONE
SEU
CAMINHÃO**



01:21

One Tower Brasil
124 subscribers

Pinned message
Boa Noite Pessoal Entrem nesse Canal caso os Grupo caia tem um
AGRU logo vai ir a baixo. 07:49 1504

One Tower Brasil
Forwarded from PAZ Silva




Urgente!!

Campo de concentração do governo petista acaba de matar uma senhora de idade.

Passou o dia todo sem água e comida no calor de Brasília e veio a óbito.

1200 pessoas ainda se encontram em campo de concentração em situação desumana.

Repassem o máximo que puderem!!

#lutagenocida



LIBERDADE!!

*** Luiz is typing



JanosGraber

Forwarded messages

Layla Fiusa, afiada! today at 15:06



Rodrigo Constantino

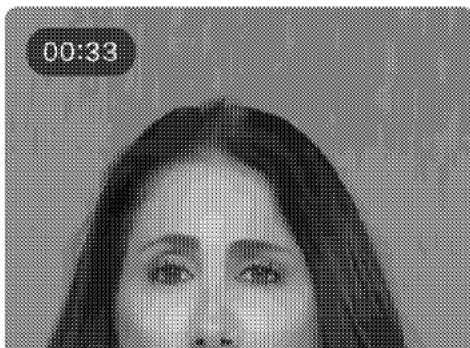
@Rconstantino

Não há pacificação possível com um ambiente persecutório e cada vez mais autoritário, que enfia goela abaixo do povo um corrupto e depois trata como terrorista qualquer um que ouse questionar. O sistema podre não compreendeu o fenômeno ainda...



Deto Machado

00:33





PÉ NA PORTA Chat

5.934 members, 783 online

Pinned message

Voice Message



93 11 3 3 2

Nicolas joined the group

Elisangela Oliveira joined the group

Charles Fernando joined the group

Lu joined the group

Paulo Alexandre joined the group

Greaser gangster joined the group

Humberto Bacelar joined the group

Pollyanna Jogo do Contente joined the group

BARAMED joined the group

JMF2007 joined the group

Delima joined the group

Graciely joined the group

Aluisio Raia joined the group

Andréia Blessed joined the group



PÉ NA PORTA Chat
Forwarded messages

Luciano Cesar today at 00:08

Estivemos 21 anos apoiando político ladrão. Enquanto isso, as Forças Armadas estavam defendendo o Brasil dias de manifestações diante dos Quartéis, a ESQUERDA planta essa mentira de que os militares nos traíram facilmente enganado!!!! Os militares só vão fazer intervenção militar quando esse povo provar que não é gad intervenção. Senão, ocorreria o que ocorreu na Venezuela, que depois que os militares assumiram, colocand enésima vez ideias contra os militares na cabeça do povo, que começou a exigir que o Exército devolvesse o devolver o poder aos políticos e o país se fu***!!! É o que você quer para o seu país???? Que os militares faç Olavo de Carvalho e políticos como Carla Zambelli e idolatra Bolsonaro, e se coloca contra os militares? Se é Lula. Os militares só farão intervenção quando os brasileiros em peso, aos milhões, pedirem o correto, no luç FRENTE DOS QUARTEIS, AOS MILHÕES, O POVO TEM QUE PEDIR INTERVENÇÃO MILITAR NOS TRÊS PODER



André Patriota joined the group

. joined the group



Juventude Revoltada Chat

Bad is choosing a sticker



Pinned message

@informatividades.



Carlos Souza

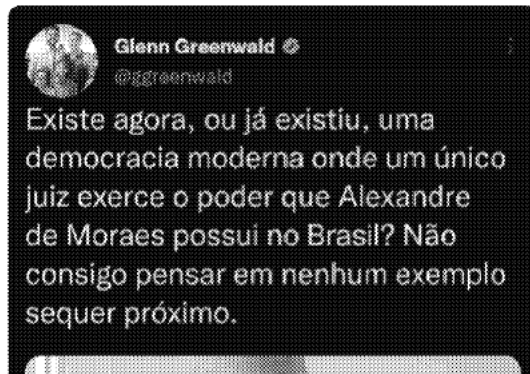


Bad
Video

RedPill



Bad







Administrativo

== Juventude Revoltada Chat ==

Em caso de problemas, chame @admin. Clique aqui  /rules para ver as regras do grupo.

Canal JR 

Mande Sugestões 



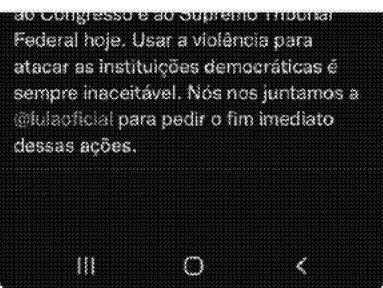
Juventude Revoltada

11.552 subscribers



Pinned message

Administração da JR está recrutando novos admins! Como funciona? Você será "entrevistado" para ver se a



70 4 4 2



Juventude Revoltada

Forwarded messages

Terezo_00 8/01/23





Caçadores de ratos do STF

104 members



Pinned message

Vídeo de Jair



<https://youtu.be/uHtz-BnlKEo>

YouTube

AÇÃO DE INFILTRADOS EM BRASÍLIA - 08/01/2023



Jean

COMUNICADO

PATRIOTAS LEVEM FAIXAS COM FRASES DE ORDEM NAS MANIFESTAÇÕES PARA IMPEDIR A MÍDIA DE CRIAR NARRATIVAS FALSAS COM PEDIDOS DE IMPEACHMENT.



Brasil No se Rinde

10.595 subscribers



🔥 94 😬 41 👍 25 😬 16 😬 3

09 January



Brasil No se Rinde

Forwarded messages

Movimento Patriotas 🇧🇷 9/01/23

Ninguém ganha a guerra com flores 🌸.

Mostra sua força BRASIL 👍 🇧🇷

👍 92 😬 9 🇧🇷 5 🇧🇷 1



Brasil No se Rinde

Forwarded messages

Movimento Patriotas 🇧🇷 9/01/23

Façam esse vídeo percorrer todos os quartéis para que todos os coronéis vejam isso ainda hoje

👍 25 😬 1



Brasil No se Rinde

Forwarded messages

Movimento Patriotas 🇧🇷 9/01/23




Foram também identificadas páginas do Facebook e perfis do Twitter

FACEBOOK:

<https://www.facebook.com/DireitaConservadoraSC?mibextid=ZbWKwl>



 88  19  10  10

facebook



Direita Conservadora SC

Intro

"E conhecereis a verdade, e a verdade vos libertará". João 8:32

Page · Political Organization

Santa Catarina, SC, Brazil

direitaconservadora.sc@gmail.com

direitaconservadora.sc

conservadora_sc

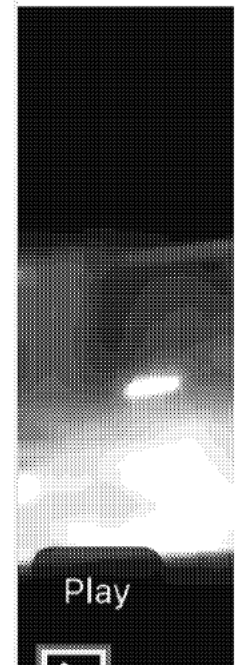
t.me/DireitaConservadoraSC



Direita
2d

URGE

BRASÍLIA
#noticias



Photos

See all photos

TWITTER:

<https://twitter.com/anapriscilaaze3?s=21>



Follow

ANA PRISCILA AZEVEDO

@ANAPRISCILAAZES


"Tudo que foi ótimo no passado foi ridicularizado, condenado, combatido e suprimido apenas p/ emergir ainda mais poderoso, ainda mais triunfante da luta."
Teola

Joined February 2021

62 Following 12.9K Followers

Not followed by anyone you're following

- Tweets
- Tweets & replies
- Media
- Likes

 **ANA PRISCILA AZEVEDO** @ANAPRISCILAAZES · Jan 8

TRAIADORES DA NAÇÃO!!! LOBOS DEGRADORES!!! VIROU AS COSTAS PARA O JAIR, PARA OS CONSERVADORES QUE ACREDITARAM NELE E ENFIQU A FAÇA NAS COSTAS DA NAÇÃO. RASGUE SUA BÍBLIA E REGUE SUA FÉ!!! ESSES SÃO OS VERDADEIROS JUDAS!!!



ANA PRISCILA AZEVEDO @ANAPRISOLAIZES · Jan 7

A REVOLUÇÃO VERDE E AMARELO JÁ COMEÇOU.
O BRASIL VAI PARAR!
A REFINARIAS E DISTRIBUIDORAS ESTÃO SENDO FECHADAS.
NÓS VAMOS SITIAR OS TRÊS PODERES!
NÓS EXIGIMOS INTERVENÇÃO MILITAR!
NÓS EXIGIMOS O CÓDIGO FONTE! VAMOS VOMITAR ESSA FRAUDE
VERMELHA NA CARÁ DE VOCÊS!



434.7K 1.396 2.881 8.822

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez e a eficácia do processo eleitoral, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à ruptura institucional, com a conseqüente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

É evidente que as postagens possuem potencial para tumultuar o cenário político, na medida em que, explicitamente, incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de novas alterações ou episódios violentos, como os ocorridos em 8 de janeiro.

Trata-se de condutas ilegais de natureza grave, que autorizam o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º, § 1º da Res.-TSE nº 23.714/2022.

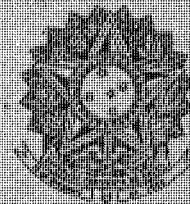
Ante o exposto, de ordem, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Telegram, Facebook e Twitter a remoção definitiva e imediata dos grupos e perfis relacionados, devendo ser preservado todo o conteúdo disponibilizado nos últimos 15 (quinze) dias, de maneira a possibilitar posterior investigação e responsabilização na esfera criminal, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

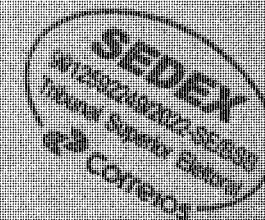
Brasília, 11 de janeiro de 2023.

Marco Antônio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral

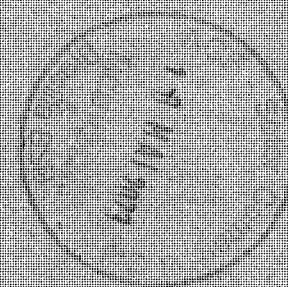


TRIBUNAL SUPERIOR ELEITORAL
BRASÍLIA-DF

AR



A Empresa
TWITTER BRASIL REDE DE INFORMAÇÃO LTDA
Avenida Brigadeiro Faria Lima, 4.221, 9º andar.
CEP: 04538-133 São Paulo



Correios AR MP

PESO (kg) 0,100

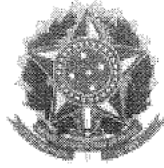
SEDEX

DY 31046768 8 BR

Tribunal Superi
PROTOCOLO DE POSTAGEM
64/2023
17/05/2023 - 17:32
SX

TRIBUNAL SUPERIOR ELEITORAL
SAF - SUI Quadra 7 Lotes 01/02
70 070-600 Brasília - DF





TRIBUNAL SUPERIOR ELEITORAL

Ofício SEPROC 3/CPRO/SJD nº 2080/2023

Brasília, 17 de Maio de 2023.

À Empresa
 Twitter Brasil Rede de Informação LTDA
 Avenida Brigadeiro Faria Lima, 4.221, 9º andar
 04538-133 São Paulo - SP

Assunto: Solicita diligências quanto à preservação dos dados cadastrais dos usuários.
 Representação 0601755-35.2022.6.00.0000 (TSE).

Prezados Senhores,

Em cumprimento ao ato judicial exarado, em 17 de maio de 2023, pelo Excelentíssimo Senhor Ministro Sérgio Silveira Banhos, Relator da Representação 0601755-35.2022.6.00.0000, solicitamos que seja preservado os conteúdos impugnados nesta representação (item 50.1.1 da petição inicial) e os respectivos dados cadastrais das usuárias e dos usuários, até o trânsito em julgado da decisão final do processo, referente às seguintes URL's:

<https://twitter.com/leandroruschel/status/1584901522651058176>

<https://twitter.com/CarolDeToni/status/1584993966084485120>

Segue anexa a cópia da referida determinação e da petição inicial onde consta o referido item 50.1.1.

Informo, por oportuno, que o feito tramita no Sistema Processo Judicial eletrônico, de modo que a consulta integral dos referidos autos pode ser realizada por meio do endereço <https://pje.tse.jus.br:8443/pje-web/login.seam>.

Respeitosamente,

LEANDRO OLIVEIRA REIS
ASSISTENTE IV



Documento assinado eletronicamente em **17/05/2023, às 13:20**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.





TRIBUNAL SUPERIOR ELEITORAL

REPRESENTAÇÃO Nº 0601755-35.2022.6.00.0000 – CLASSE 11541 – BRASÍLIA – DISTRITO FEDERAL**Relator:** Ministro Sérgio Banhos**Representante:** Coligação Brasil da Esperança**Advogados:** Eugênio José Guilherme de Aragão – OAB: 4935/DF e outros**Representada:** Carla Zambelli Salgado de Oliveira**Representada:** Caroline Rodrigues de Toni**Representada:** Renata J. Barreto**Representado:** André Machado Valadão**Representado:** Nikolas Ferreira de Oliveira**Representado:** Leandro Panazzolo Ruschel**Representado:** Responsável pelo perfil @vemprarua_Br no Instagram**DECISÃO**

A Coligação Brasil da Esperança ajuizou representação, com pedido de liminar, em desfavor de Carla Zambelli Salgado de Oliveira, André Machado Valadão, Nikolas Ferreira de Oliveira, Leandro Panazollo Ruschell, Caroline Rodrigues de Toni, Renata J. Barreto e Responsável pelo perfil "@vemprarua_br" no Instagram, por suposta veiculação de desinformação em seus perfis em redes sociais, mediante a divulgação de conteúdo gravemente descontextualizado e sabidamente inverídico, com o objeto de vincular o candidato ao cargo de presidente da República Luiz Inácio Lula da Silva à miséria e a ameaças ditatoriais, em infração aos arts. 9º-A, 22, X, e 27, § 1º, da Res.-TSE 23.610.

Os autos foram inicialmente distribuídos ao Ministro Ricardo Lewandowski e, ato contínuo, foram redistribuídos à Ministra Maria Cláudia Bucchianeri, com fundamento na Portaria-TSE 1.007/2022 (ID 158302590).

Em 12.1.2023, os autos me foram redistribuídos, nos termos do art. 2º, § 5º, da Res.-TSE 23.608, em razão do encerramento da atuação das ministras e dos ministros designados para apreciação de representações, reclamações e pedidos de direito de resposta referentes às Eleições de 2022 (IDs 158365853 e 158552140).

Por despacho (ID 158564463), ante a aparente perda do objeto da representação, determinei a intimação da representante para que se manifestasse a respeito do interesse no prosseguimento do feito, e que, após, fosse ouvida a Procuradoria-Geral Eleitoral.

A Coligação Brasil da Esperança, na manifestação apresentada (ID 158627249), requereu o prosseguimento do feito, aduzindo persistir o interesse quanto ao pedido de aplicação de multa por propaganda eleitoral irregular.

Por sua vez, a douta Procuradoria-Geral Eleitoral opinou pela extinção do processo, sem resolução de mérito, apontando a perda do objeto da representação quanto aos pedidos de remoção de conteúdo veiculado na internet e de abstenção de divulgação com o mesmo teor, afirmando a inexistência de previsão legal para a incidência de multa no caso dos autos (ID 158657691).

É o relatório.

Decido.

Evidencia-se a regularidade da representação processual (procuração de ID 158300846).

Inicialmente, registro que, na sessão de 28.3.2023, este Tribunal Superior concluiu o julgamento do Recurso na Representação 0601754-50, da relatoria do Ministro Alexandre de Moraes, ocasião em que o Colegiado decidiu, por maioria, que é possível a aplicação da multa prevista no art. 57-D da Lei 9.504/97 nas representações por propaganda eleitoral irregular divulgada na internet mediante veiculação de informação inverídica e, por conseguinte, persiste o interesse jurídico na determinação de remoção definitiva do conteúdo impugnado, independentemente da superveniência das eleições.

Tal compreensão foi reafirmada no Recurso na Representação 0601756-20, também da relatoria do Ministro Alexandre de Moraes, julgado na sessão ordinária em regime híbrido realizada no dia 18.4.2023 e cujo acórdão ainda não foi publicado.

Desse modo, ante a possibilidade de aplicação de multa e de que seja determinada a remoção definitiva do conteúdo desinformativo, não há falar em perda do objeto da representação em virtude da realização das eleições, de modo que cumpre prosseguir na instrução processual.

A Coligação Brasil da Esperança requer, na petição inicial, o deferimento de medida liminar, com fundamento no art. 300 do Código de Processo Civil, visando a que seja determinada a remoção das publicações impugnadas nos autos e que os representados se abstenham de veicular outras notícias e publicações com o mesmo teor, em ambos os casos sob pena de multa, de modo a preservar a lisura e a higidez das eleições e do processo eleitoral.

Alega que os representados veicularam desinformação em seus perfis em redes sociais com o objetivo de vincular o candidato a presidente da República Luiz Inácio Lula da Silva à miséria e a ameaças ditatoriais, traçando “*um paralelo imaginário associando uma eventual vitória de Lula nas eleições vindouras a um cenário trágico, no qual se instalaria uma ‘ditadura comunista’ no Brasil, acompanhada de fome generalizada*” (ID 158300845, p. 4).

Argumenta que as publicações impugnadas veicularam informação sabidamente inverídica e já desmentida por agências de checagem a respeito de suposto plano para implantação do comunismo no Brasil, e, no que se refere ao hipotético risco de crescimento da miséria no país, divulgaram ilações contrariadas por dados publicados em relatório da Organização das Nações Unidas para a Alimentação e a Agricultura (FAO) e, por conseguinte, teriam propagado conteúdo gravemente descontextualizado, que atingiria a integridade do processo eleitoral – por afetar a liberdade de conhecimento dos cidadãos e o direito livre de voto – e ofenderia a honra e a imagem do candidato Luiz Inácio Lula da Silva e do Partido dos Trabalhadores, incidindo, assim, nas vedações previstas nos art. 9º-A, 22, X, e 27, § 1º, da Res.-TSE 23.610.

Como é consabido, a concessão da tutela de urgência pressupõe o preenchimento de requisitos, consistentes em probabilidade do direito (*fumus boni juris*) e perigo de dano ou risco ao resultado útil do processo (*periculum in mora*).

No que se refere à probabilidade do direito, a autora da representação afirma que os conteúdos das postagens impugnadas nos autos evidenciarão manifesta ofensa às normas e aos princípios que regem a propaganda eleitoral, de modo a ferir a lisura do processo eleitoral, ante o emprego de estratégia de propagação de desinformação e de manipulação de narrativas, com violação da liberdade de pensamento e à cidadania dos eleitores.

Argumenta que o perigo de dano residiria na perpetuação de desinformação que macula a lisura do processo eleitoral e veicula propaganda eleitoral negativa contra o então candidato Luiz Inácio Lula da Silva e o Partido dos Trabalhadores, por meio de publicações veiculadas na internet, cujo alcance é amplificado de forma exponencial pelo alto número de compartilhamentos, com significativa interferência na liberdade de opinião e de pensamento dos eleitores, violando o direito ao voto livre e a democracia.

Acerca de tais alegações, observo que o art. 9º-A da Res.-TSE 23.610, incluído pela Res.-TSE 23.671, dispunha que “*é vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos, devendo o juízo eleitoral, a requerimento do Ministério Público, determinar a cessação do ilícito, sem prejuízo da apuração de responsabilidade penal, abuso de poder e uso indevido dos meios de comunicação*”.

O referido dispositivo regulamentar foi revogado pela Res.-TSE 23.714, de 20.10.2022 (DJE de 24.10.2022), a qual dispõe a respeito da matéria no art. 2º, caput, cujo teor é

o seguinte: “É vedada, nos termos do Código Eleitoral, a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos”.

Ainda quanto ao tema, o art. 27, § 1º, da Res.-TSE 23.610, com a redação dada pela Res.-TSE 23.671, estabelece que “a livre manifestação do pensamento de pessoa eleitora identificada ou identificável na internet somente é passível de limitação quando ofender a honra ou a imagem de candidatas, candidatos, partidos, federações ou coligações, ou divulgar fatos sabidamente inverídicos, observado o disposto no art. 9º- A desta Resolução”.

Na espécie, sem prejuízo de exame mais detido da questão controvertida por ocasião do julgamento do mérito da representação, verifico que o requisito alusivo ao perigo de dano não está configurado, pois, ainda que se reconhecesse, em juízo de cognição sumária, a suposta ilicitude das postagens impugnadas e sua alegada aptidão para influenciar o eleitor e interferir negativamente no processo eleitoral, há de se considerar que o processo eleitoral já foi encerrado – inclusive com a eleição e a diplomação do candidato da coligação representante – e, desse modo, a eventual concessão de liminar para remoção das publicações em tela não surtiria efeito prático em relação ao pleito já findo.

Ainda quanto ao ponto, observo que, intimada para se manifestar a respeito da aparente perda do objeto da demanda – por despacho proferido antes das recentes decisões deste Tribunal que afastaram tal possibilidade, mencionadas alhures –, a representante se limitou a argumentar que, “por se tratar de representação eleitoral ajuizada em razão da perpetração de desinformação, remanesce a apreciação do pedido de aplicação de multa constante na inicial” (ID 158627249, p. 1), sem nada dizer a respeito do pedido de liminar para remoção de conteúdo.

Ademais, o indeferimento da medida liminar, na espécie, não enseja risco ao resultado útil do processo, pois a eventual remoção das postagens impugnadas poderá ser determinada em caráter definitivo por ocasião do julgamento de mérito, caso sejam reconhecidas a ilicitude dos conteúdos publicados e a procedência dos pedidos formalizados na representação.

Assim, por não estar presente o requisito necessário para a concessão da tutela de urgência requerida, alusivo ao perigo da demora, é caso de indeferimento do pedido de medida liminar formulado pela Coligação Brasil da Esperança.

De outra parte, verifica-se que um dos representados não foi devidamente identificado na petição inicial da representação, constando apenas a sua qualificação como “Responsável pelo perfil @vemprarua_br no Instagram”.

Quanto ao ponto, assinalo que o art. 17, § 1º, da Res.-TSE 23.608 prevê a possibilidade de a representação ser endereçada genericamente contra o responsável

pela propaganda irregular, desde que requerida liminarmente diligência para a respectiva identificação e sejam fornecidos elementos indispensáveis para obtenção dos dados, sob pena de indeferimento da petição inicial, *in verbis*:

Art. 17. A petição inicial da representação relativa à propaganda irregular será instruída, sob pena de não conhecimento:

[...]

§ 1º Desconhecida a autoria da propaganda, a petição inicial poderá ser endereçada genericamente contra a(o) responsável, desde que requerida liminarmente diligência para a identificação desta ou deste e fornecidos os elementos indispensáveis para a obtenção dos dados, sob pena de indeferimento da petição inicial.

Por sua vez, os arts. 39 e 40 da Res.-TSE 23.610 estabelecem o seguinte:

Art. 39. O provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e de acesso a aplicações de internet, de forma autônoma ou associados a dados cadastrais, a dados pessoais ou a outras informações disponíveis que possam contribuir para a identificação da usuária ou do usuário, mediante ordem judicial, na forma prevista nesta seção (Lei nº 12.965/2014, art. 10, caput e § 1º).

Art. 40. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial, em caráter incidental ou autônomo, requerer ao juízo eleitoral que ordene à(ao) responsável pela guarda o fornecimento dos dados constantes do art. 39 desta Resolução (Lei nº 12.965/2014, art. 22).

§ 1º Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade (Lei nº 12.965/2014, art. 22, parágrafo único):

I - fundados indícios da ocorrência do ilícito de natureza eleitoral;

II - justificativa motivada da utilidade dos dados solicitados para fins de investigação ou instrução probatória;

III - período ao qual se referem os registros; e (Redação dada pela Resolução nº 23.671/2021)

IV - a identificação do endereço da postagem ou conta em questão (URL ou, caso inexistente, URI ou URN), observados, nos termos do art. 19 da Lei nº 12.965/2014, o âmbito e os limites técnicos de cada provedor de aplicação de internet. (Incluído pela Resolução nº 23.671/2021)

§ 2º A ausência de identificação imediata da usuária ou do usuário responsável pela divulgação do conteúdo não constitui circunstância suficiente para o deferimento liminar do pedido de quebra de sigilo de dados.

§ 3º A ordem judicial que apreciar o pedido deverá conter, sob pena de nulidade, fundamentação específica quanto ao preenchimento de todos os requisitos legais previstos nos incisos I a III do § 1º deste artigo. (Grifo nosso.)

Todavia, no que se refere ao representado não identificado de plano na petição inicial (Responsável pelo perfil @vemprarua_br no Instagram), a autora da representação não formulou o requerimento de que tratam os arts. 17, § 1º, da Res.-TSE 23.610 e 40, caput, da Res.-TSE 23.610, visando a que fosse determinado ao responsável pela guarda o fornecimento dos dados mencionados no art. 39 da Res.-TSE 23.610, alusivos ao usuário em tela, a fim de que fosse identificado para citação e exercício do direito de defesa, o que, em princípio, ensejaria o indeferimento da petição inicial quanto ao referido demandado, com base no primeiro dispositivo regulamentar acima citado.

Pelo exposto:

I – Indefiro o pedido de medida liminar formulado pela Coligação Brasil da Esperança, ante a ausência do requisito para a concessão da tutela de urgência atinente ao perigo da demora, nos termos do art. 300 do Código de Processo Civil e na linha da fundamentação exposta acima.

II – Citem-se os representados Carla Zambelli Salgado de Oliveira, Caroline Rodrigues de Toni, Renata J. Barreto, André Machado Valadão, Nikolas Ferreira de Oliveira e Leandro Panazzolo Ruschel para apresentar defesa, no prazo de dois dias, nos termos do art. 18 da Res.-TSE 23.608.

III – Oficie-se às empresas Facebook, Instagram e Twitter, a fim de que preservem os conteúdos impugnados nesta representação (item 50.1.1 da petição inicial) e os respectivos dados cadastrais das usuárias e dos usuários, até o trânsito em julgado da decisão final do processo.

IV – Intime-se a Coligação Brasil da Esperança, a fim de que, no prazo de dois dias, manifeste-se a respeito da aparente existência de causa para o indeferimento da petição inicial quanto ao Responsável pelo perfil @vemprarua_br no Instagram, considerando a ausência do requerimento de diligências previsto nos arts. 17, § 1º, da Res.-TSE 23.610 e 40, caput, da Res.-TSE 23.610.

Publique-se.

Intime-se.

Ministro Sérgio Silveira Banhos
Relator



EXCELENTÍSSIMO SENHOR MINISTRO PRESIDENTE DO TRIBUNAL
SUPERIOR ELEITORAL, ALEXANDRE DE MORAES

COLIGAÇÃO BRASIL DA ESPERANÇA, formada pela **FEDERAÇÃO BRASIL DA ESPERANÇA (FE BRASIL)**, inscrita no CNPJ/MF sob o nº 46.406.275/0001-20, com sede no Setor Comercial Sul, Quadra 02, Bloco C, Edifício Toufic, 1º andar, CEP 70302-000, Brasília/DF, constituída pelo Partido dos Trabalhadores (PT), Partido Verde (PV) e Partido Comunista do Brasil (PCdoB); pela **FEDERAÇÃO PSOL-REDE**, inscrita no CNPJ/MF sob o nº 46.875.220/0001-60, com sede no Setor Comercial Sul, Quadra 02, Bloco C, nº 252-A, Ed. Jamel Cecílio, 5º Andar, Brasília/DF, CEP 70302-905, integrada pelo Partido Socialismo e Liberdade (PSOL) e pela Rede Sustentabilidade (REDE); pelo **PARTIDO SOCIALISTA BRASILEIRO (PSB)** inscrito no CNPJ sob o nº 01.421.697/0001-37, com sede no SCLN 304, Bloco A, Sobreloja, Brasília/DF, CEP n. 70.736-510; pelo **SOLIDARIEDADE**, inscrito no CNPJ/MF sob o nº 18.532.307/0001-07, com sede na SRTVS, Quadra 701, Bloco O, Salas 790 a 793, Ed. Multiempresarial, Asa Sul, Brasília/DF; pelo **AVANTE**, inscrito no CNPJ/MF sob o nº 59.933.952/0001-00, com sede no SAI, Quadra 05, Ed. Heleno Center, Sala 301, Guará, Brasília/DF, CEP 71200-055; e pelo **PARTIDO AGIR**, inscrito no CNPJ/MF sob o nº 32.206.989/0001-80, com sede no SCS, Quadra 06, Bloco A, sobreloja 02, Ed. Presidente, Asa Sul, Brasília/DF, CEP: 70.327-900; **PARTIDO REPUBLICANO DA ORDEM SOCIAL (PROS)**, inscrito

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99953-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. M, salas 2059-2064 - Asa Norte
Ed. JON Brasília, DF | CEP: 70.330-015



no CNPJ/MF sob o nº 12.952.205/0001-56, com sede em SHIS, QL 26, conj. 1, cs 19, Lago Sul, Brasília/DF, CEP 71.665-115; e representada pela Deputada Federal **Gleisi Helena Hoffman**, brasileira, casada, Deputada Federal (PT/PR), endereço funcional na Esplanada dos Ministérios, Praça dos Três Poderes, Câmara dos Deputados, Gabinete 232 - Anexo 4, vem, respeitosamente, por meio de seus advogados, mediante instrumento de procuração anexo, com fundamento no 9º- A Resolução no 23.610/2019, ajuizar

REPRESENTAÇÃO ELEITORAL POR VEICULAÇÃO DE DESINFORMAÇÃO

Em razão dos acontecimentos a seguir expostos, detrimento de:

1. **CARLA ZAMBELLI**, brasileira, Deputada Federal, inscrita no CPF sob o nº. 013.355.946-71, com domicílio profissional na Câmara dos Deputados, Gabinete 885, Anexo III, Praça dos Três Poderes, CEP 70.160-900, Brasília/DF, endereço eletrônico

2. **ANDRÉ VALADÃO**, brasileiro, pastor e empresário, inscrito no CPF/MF sob o nº 041.877.316-52, RG nº 106.851.31 SSP/MG, residente e domiciliado na

telefones para contato

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4007 | 99963-2575
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SCAN 601, 81, H, salas 2059-2104 - Asa Norte
Ed. JON Brasília, DF | CEP: 70.830-018



3. **NIKOLAS FERREIRA DE OLIVEIRA**, brasileiro, vereador, portador do RG nº [REDACTED] e inscrito no CPF nº 117.014.426-80, com endereço na [REDACTED]
4. **LEANDRO PANAZOLLO RUSCHELL**, brasileiro, empreendedor, inscrito no CPF sob o nº 969.463.930-15, com domicílio a [REDACTED]
5. **CAROLINE RODRIGUES DE TONI**, brasileira, deputada federal, inscrita no CPF nº 058.583.929-89, com endereço funcional no Gabinete 476, Anexo III, Câmara dos Deputados, Brasília (DF), CEP 70160-900, endereço eletrônico [REDACTED]
6. **RENATA J. BARRETO**, brasileira, empresária, CPF desconhecido, com endereço funcional na [REDACTED] e [REDACTED]
7. Responsável pelo perfil “@vemprarua_br” no instagram.

I – DOS FATOS

1. O ajuizamento da presente Representação Eleitoral surge diante da veiculação de conteúdo gravemente descontextualizado e sabidamente inverídico, através de publicação realizada pelos Representados em suas páginas oficiais do Instagram,

Brasília
 SAS Quadra 1 Bloco M Lote 1
 Ed Libertas Conj. 1009
 Asa Sul 70070-935
 Tel./Fax: +55 61 3326.9905
 www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99963-2576
 advogados@aragaoeferraro.com
 www.aragaoeferraro.com
 SGM 601, Bl. B, salas 2059-2064 - Asa Norte
 Ed. IOB Brasília, DF | CEP: 70.830-012

Facebook e Twitter, objetivando vincular o ex-presidente Luiz Inácio Lula da Silva, que, atualmente, é candidato à Presidência da República pela Coligação “Brasil da Esperança” à miséria e ameaças ditatoriais.

2. Para tanto, os representados, através de suas publicações, traçam um paralelo imaginário associando uma eventual vitória de Lula nas eleições vindouras a um cenário trágico, no qual se instalaria uma “ditadura comunista” no Brasil, acompanhada da fome generalizada.

3. Nas teses conspiratórias, claro, a única barreira para evitar que tal situação se imponha é a reeleição do candidato Jair Bolsonaro.

4. Ocorre que, como sabemos, o *modus operandi* dos representados consiste em propagar o terror e pânico, desinformar, mentir gravemente sobre o adversário associando-o a todo e qualquer mal para, ao final, influenciar negativamente o eleitorado.

5. Na espécie, foram diversas postagens com conteúdo que podem ser divididos em dois temas: (i) ameaça de implantação de uma ditadura comunista no Brasil com a eleição de Lula; e (ii) fome generalizada.

6. Ambas hipóteses são divorciadas da realidade e trazem conjecturas macabras, sem respaldo mínimo da realidade dos fatos, de modo que apenas objetivam incutir na mente do eleitor o pânico e repulsa ao candidato Luiz Inácio Lula da Silva. As postagens se valem de textos audiovisuais com forte apelo, mostrando pessoas em situação de extrema vulnerabilidade, dentre outros absurdos.

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed. Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99963-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. G1, salas 2053-2054 - Asa Norte
Ed. 10N Brasília, DF | CEP: 70.830-010



7. Pois bem. Sobre a paranoia anticomunista, podemos afirmar que existem dois grupos: os que criam e espalham as mentiras, e os que consomem e acreditam nelas.

8. É preciso ter em mente, portanto, que as pessoas que criam paranoias anticomunistas as usam como arma políticas, buscando propagar desinformação e mentira. É, o Cavalo de Troia dos tempos atuais. É engodo, charlatanismo, enganação, oportunismo e conveniência. Não nos esqueçamos que o próprio Jair Bolsonaro já se declarou fã do então presidente venezuelano Hugo Chaves¹.

9. Com efeito, sobre o tema, diversas agências de checagem²³⁴⁵ já atestaram que não passa de *fake news* as “notícias” de que o Partido dos Trabalhadores objetiva implantar um “plano de dominação comunista”. Senão vejamos:

The screenshot shows a news article from the website 'ESTADÃO Política'. The headline is 'Boato circula com falso 'plano de dominação comunista' do PT'. Below the headline, there is a sub-headline: 'Mentira nas redes sociais se refere a propostas de correntes petistas não-hegemônicas apresentadas em congresso de 2015'. The article is categorized under 'Política' and includes social media sharing icons for WhatsApp, Facebook, Twitter, and LinkedIn.

¹ <https://veja.abril.com.br/politica/bolsonaro-defende-hugo-chavez-em-entrevista-de-1999/>

² <https://politica.estadao.com.br/blogs/estadao-verifica/boato-circula-com-falso-plano-de-dominacao-comunista-do-pt/>

³ <https://noticias.uol.com.br/confere/ultimas-noticias/2022/10/17/mensagem-falsa-no-whatsapp-diz-que-pt-tem-plano-de-dominacao-comunista.htm>

⁴ <https://noticias.uol.com.br/comprova/ultimas-noticias/2018/09/18/e-boato-que-o-pt-aprovou-um-plano-de-dominacao-comunista.htm>

⁵ <https://lupa.uol.com.br/jornalismo/2021/11/05/verificamos-pt-plano-dominacao-comunista/?fbclid=IwAR0XfNjOJBqRokOPRG7V96sdailxr5pszpcAA6TD6MifdhDI-RvKk5tVPgg>

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed. Liberdade Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4927 | 99963-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. H, salas 2059-2064 - Asa Norte
Ed. IGN Brasília, DF | CEP: 70.830-015

noticias.uol.com.br/comprova/ultimas-noticias/2018/09/18/e-boato-que-o-pt-aprovou-um-plano-de-dominacao-comunista.htm

Benvenuto Bambli... Benvenuto Bambli... Kit Elefante Leão... Bem vindo ao PJe... O Guia Completo...

uol | INGRESSO.COM | BATE PAPO | NEG. NEGOCIO | PASSAG. DIRETO | FASEGURO | UOL PLAY | SAC | EMAIL | Filtro

PRODUTOS | ELEIÇÕES | NOTÍCIAS | CARROS | ECONOMIA | FOLHA | ESPORTE | SPLASH | UNIVERSA | VIVABEM | TILT | ECOA | CANAL UOL | MOV

UOL CONFERE

Uma iniciativa do UOL para checagem e esclarecimento de fatos

É boato que o PT aprovou um "plano de dominação comunista"

noticias.uol.com.br/confere/ultimas-noticias/2022/10/17/mensagem-falsa-no-whatsapp-diz-que-pt-tem-plano-de-dominacao-comunista.htm

Benvenuto Bambli... Benvenuto Bambli... Kit Elefante Leão... Bem vindo ao PJe... O Guia Completo...

uol | INGRESSO.COM | BATE PAPO | NEG. NEGOCIO | PASSAG. DIRETO | FASEGURO | UOL PLAY | SAC | EMAIL | Filtro

PRODUTOS | ELEIÇÕES | NOTÍCIAS | CARROS | ECONOMIA | FOLHA | ESPORTE | SPLASH | UNIVERSA | VIVABEM | TILT | ECOA | CANAL UOL | MOV | NOS

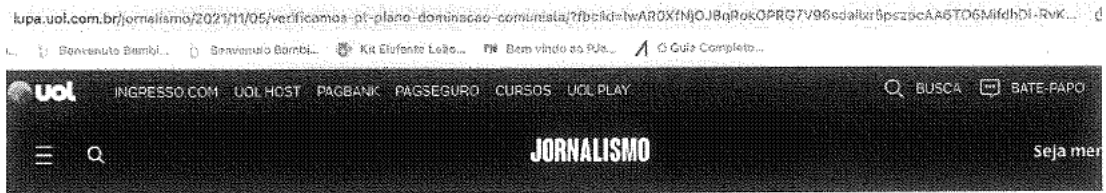
UOL CONFERE

Uma iniciativa do UOL para checagem e esclarecimento de fatos

Mensagem falsa no WhatsApp diz que PT tem "plano de dominação comunista"

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed. Liberdade Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 33963-2576
advogados@aragoeferraro.com
www.aragoeferraro.com
SGAN 601, Bl. A, salas 2055-2064 - Asa Norte
Ed. ION Brasília, DF | CEP: 70.320-012


VERIFICAÇÃO

PT NÃO PUBLICOU 'PLANO DE DOMINAÇÃO COMUNISTA'

10. A bem da verdade, Excelência, o Partido dos Trabalhadores é um partido democrata e defensor da democracia, que já governou o Brasil dentro das regras democráticas. Não atoa, a Coligação representante é a maior frente democrática existente no Brasil.

11. Ainda, importante lembrar, por oportuno, que durante o governo do ex-Presidente Lula não se falava habitualmente em impeachment de Ministros do Supremo Tribunal Federal, não se falava em nova Constituinte, não havia arroubos autoritários, tampouco se falava em não renovar concessão de emissoras de televisão.

12. Com efeito, o renomado Cientista Político norte-americano Steven Levitsky, Professor da prestigiada Harvard e autor do livro "Como as democracias morrem", durante participação no programa Roda Viva⁶, da TV Cultura, afirmou que "*o Presidente da República (Jair Bolsonaro) é a maior ameaça à democracia no momento*"; "*as*

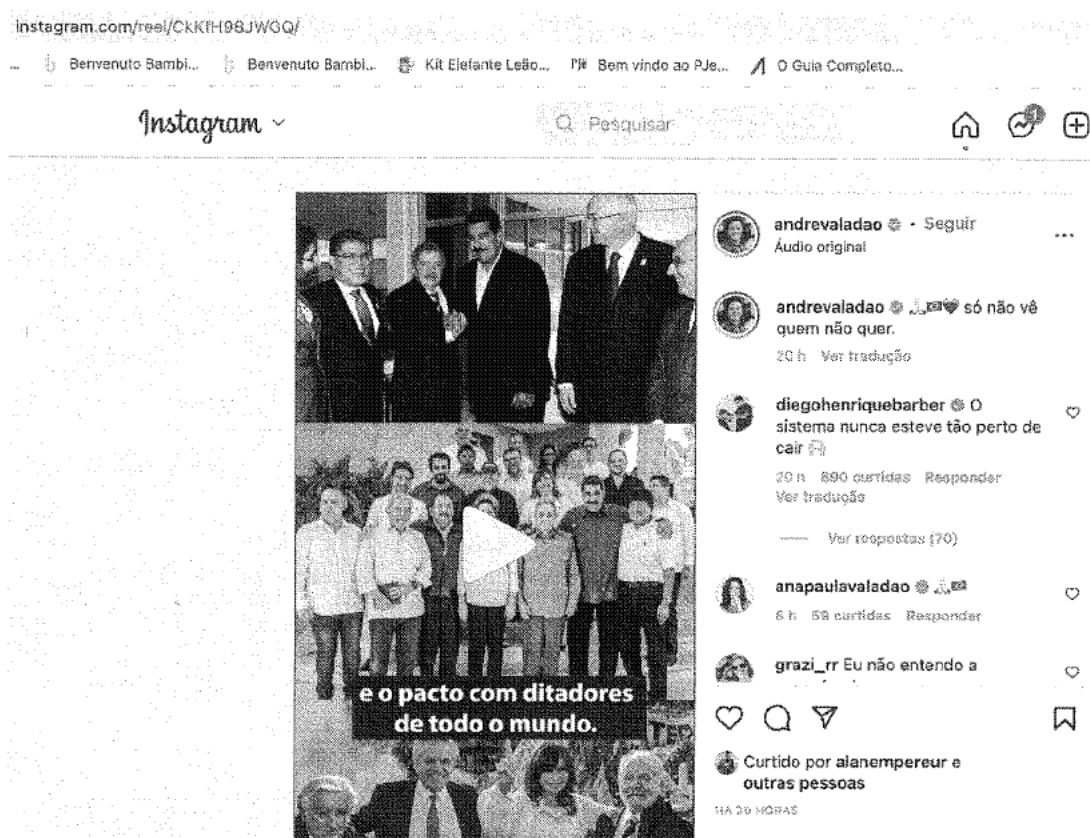
⁶ <https://noticias.uol.com.br/ultimas-noticias/bbc/2022/07/19/bolsonaro-inventou-duvidas-sobre-sistema-eleitoral-porque-pode-perder-eleicoes-diz-professor-de-harvard.htm>

Brasília
 SAS Quadra 1 Bloco M Lote 1
 Ed Libertas Conj. 1009
 Aea Sul 70070-935
 Tel./Fax: +55 61 3326.9905
 www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99953-2576
 advogados@aragaoeferraro.com
 www.aragaoeferraro.com
 SGAH 601, Bl. H, salas 2059-2064 - Asa Norte
 Ed. JON Brasília, DF | CEP: 70.310-018

“pessoas tem várias opiniões sobre Lula, mas acho que ninguém o considerada, seriamente, uma pessoa autoritária”; e “ele (Lula) (se eleito) não será um presidente autoritário”.

13. Em tal direção, o segundo Representado publicou em seu perfil no instagram⁷ um vídeo no qual afirma que “Lula fez um pacto com ditadores de todo o mundo”, “que – Lula – desfruta do luxo enquanto o povo vive na miséria” e “existe um plano para se perpetuar no poder, e a cor desse plano é vermelha”.



⁷ <https://www.instagram.com/reel/CkKfH98JWQQ/>

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 50963-2576
advogados@aragoeferraro.com
www.aragoeferraro.com
SQAN 001, Bl. H, salas 2059-2064 - Asa Norte
Ed. JON Brasília, DF | CEP: 70.820-019



14. No mesmo sentido, o sétimo representado, o perfil “vempraru_br”, publicou em sua página no Instagram uma imagem com a seguinte legenda⁸: “não é segredo para ninguém a relação íntima de LL com Maduro e outros ditadores. Está tudo documentado e comprovado. Fora ditadores! Fora ditaduras! A bandeira do Brasil jamais será vermelha! #LLNuncaMais #CensuraNao”.



15. Na mesma esteira, a sexta representada, Renata Barreto, publicou um vídeo em seu perfil na plataforma Instagram⁹, no qual ela afirma que Lula, se eleito, irá implantar uma ditadura no Brasil. Vejamos:

⁸ <https://www.instagram.com/p/CkJeL4MgVPa/>

⁹ <https://www.instagram.com/reel/CkJI4IAIbH0/>

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed. Liberdade Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99953-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. H, salas 2059-2064 - Águia Norte
Ed. ION Brasília, DF | CEP: 70.830-018



16. O terceiro representado, Nikolas, utilizou do mesmo expediente e publicou em seu perfil na plataforma Instagram¹⁰ um vídeo no qual associa Lula à uma política “comunista/socialista” que estaria associada a morte de 110 milhões de pessoas:

¹⁰ <https://www.instagram.com/reel/CkJ5IUeID8j/>

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3245-4057 | 9963-2376
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 661, Bl. H, salas 2055-2064 - Asa Norte
Ed. IGN Brasília, DF | CEP: 70.330-018



17. Já o quarto representado, Leandro Ruschel, publica em seu *twitter* pessoal¹¹ que “ditador assassino Maduro, da Venezuela, declarando amizade e até amor por Lula, além de agradecimentos. É uma parceria de longo prazo”.

¹¹ <https://twitter.com/leandroruschel/status/1584901522651058176>

Brasília
 SAS Quadra 1 Bloco M Lote 1
 Ed Libertas Conj. 1009
 Asa Sul 70070-935
 Tel./Fax: +55 61 3326.9905
 www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99963-2576
 advogados@aragaoeferraro.com
 www.aragaoeferraro.com
 SGAN 601, Bl. H, salas 2053-2064 - Asa Norte
 Ed. JON Brasília, DF | CEP: 70.830-018

← **Tweet**



Leandro Ruschel    

@leandroruschel

São dezenas de post do ditador assassino Maduro, da Venezuela, declarando amizade e até amor por Lula, além de agradecimentos.

É uma parceria de longo prazo.

18. Noutro giro, mas ainda de maneira orquestrada objetivando propagar desinformação e, destarte, manipular o eleitor, os representados buscam associar o Partido dos Trabalhadores à miséria.

19. Para tanto, fazem comparações esdrúxulas com a Venezuela, afirmando que o futuro do Brasil, caso o ex-Presidente Lula seja eleito, será de fome generalizada. Para “chocar” os interlocutores, fazem uso de postagens audiovisuais¹²¹³¹⁴ com imagens de pessoas em situação de extrema vulnerabilidade, buscando comida nas ruas, dentre outros.

¹² <https://www.instagram.com/reel/CkKRzndAEX6/>

¹³ <https://www.facebook.com/watch/?v=1109802496203573>

¹⁴ <https://www.facebook.com/photo?fbid=664400138367725&set=a.518100476331026>

Na Venezuela, cesta básica custa 28 salários mínimos
Rendimento de trabalhadores e aposentados cobre apenas 3,4% do valor necessário para alimentar uma família

ACORDA, BRASIL!!! Além de não dar para comprar NADA para comer, os aposentados na Venezuela estão sendo assaltados após receberem esta migalha do amigo de Lula, pois o crime tomou conta do país. É ISSO o que você quer para o futuro do Brasil? Não é? Então, neste domingo VOTE!!! BOLSONARO para que nossos entes queridos possam ter um futuro.

#QuemAnulaVotaLula

631 comentários 6,5 mil compartilhamentos

O Caos que a Esquerda Pode causar

Você não precisa gostar de Bolsonaro para votar nele. Você só precisa gostar do Brasil. Para que seus filhos, netos e entes queridos tenham um futuro, neste domingo VOTE!

veja
Mundo
Venezuelanos já comem comida de cachorro, diz ONG
Falta de alimentos multiplica casos de saques em várias partes da Venezuela

Você não precisa gostar de Bolsonaro para votar nele. Você só precisa amar o Brasil. Para que seus filhos, netos e entes queridos tenham um futuro, neste domingo VOTE!

Brasília
SAS Quadra I Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | (9963) 2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. M, salas 2059-2064 - Asa Norte
Ed. 10N, Brasília, DF | CEP: 70.330-018

20. No entanto, a verdade se impõe: durante os anos 2002 a 2013 – Governo Lula, portanto – o percentual de brasileiros considerados em situação de subalimentação caiu 82% (oitenta e dois).

21. De acordo com relatório das Nações Unidas para a Alimentação e a Agricultura (FAO), o Brasil deixou o mapa da fome em 2014. O relatório também mostrou que o Indicador de Prevalência de Subalimentação, medida empregada pela FAO há 50 anos para dimensionar e acompanhar a fome em nível internacional, atingiu no Brasil nível menor que 5%, abaixo do qual a organização considera que um país superou o problema da fome. Senão, vejamos¹⁵¹⁶:

¹⁵ <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2014/setembro/relatorio-indica-que-brasil-saiu-do-mapa-mundial-da-fome-em-2014>

¹⁶ <https://www12.senado.leg.br/radio/1/noticia/2014/09/16/brasil-saiu-do-mapa-da-fome-produzido-pela-onu>



Relatório indica que Brasil saiu do Mapa Mundial da Fome em 2014

Ministra do Desenvolvimento Social analisa dados das Nações Unidas, que tiraram o País do Mapa da Fome no mundo. De 2002 a 2013, caiu em 82% a população de brasileiros considerados em situação de subalimentação.



Brasil saiu do mapa da fome produzido pela ONU

LOC: O BRASIL SAIU DO MAPA DA FOME PRODUZIDO PELA ONU. O PAÍS É UM DOS QUE MAIS PROGREDIRAM NO COMBATE AO PROBLEMA, SEGUNDO O RELATÓRIO.

LOC: O DOCUMENTO TAMBÉM APONTA REDUÇÃO DE 75% NA EXTREMA POBREZA, COMO CONTA A REPÓRTER MARCELLA CUNHA.

22. Pelo exposto, tem-se que a veiculação de falsas informações pelos Representados constitui verdadeiro ato de divulgação e compartilhamento de fatos gravemente descontextualizados e inverídicos que violam a liberdade de opinião dos eleitores, bem como impacta diretamente na honra objetiva e subjetiva do candidato, de modo a se enquadrar nas hipóteses proibitivas do art. 9º-A da Resolução nº 23.610/2019 do Tribunal Superior Eleitoral.

23. Assim, é preciso que tais atitudes sejam repreendidas por essa d. Corte, nos termos da Lei, de modo que o eleitorado não seja vítima de um dos ilícitos mais graves que emergem no período eleitoral: a desinformação cumulada com ofensas.

Brasília
 SAS Quadra 1 Bloco M Lote 1
 Ed Liberdade Conj. 1009
 Asa Sul 70070-935
 Tel./Fax: +55 61 3326.9905
 www.zaninmartinsadvogados.com.br

(61) 2246-4057 | 99963-2576
 advogados@aragaoeferraro.com
 www.aragaoeferraro.com
 55AN 601, Bl. H, sala 2059-2064 - Asa Norte
 Ed. IGN Brasília, DF | CEP: 70.830-619

II – DO DIREITO

24. Como bem se sabe, a desinformação significa prática antijurídica, que afeta a liberdade de conhecimento dos cidadãos e, automaticamente, influencia negativamente no processo democrático. Dessa forma, no presente período eleitoral, o combate à desinformação deve ser realizado com o máximo rigor e eficiência, sob pena de subversão da própria democracia.

25. No presente caso, conforme acima demonstrado, os Representados propagaram conteúdo gravemente descontextualizado, buscando incutir a ideia de que o PT é irá impor uma ditadura no Brasil, bem como levará a uma situação de pobreza extrema, com fome generalizada.

26. Com efeito, trata-se de ação estratégica política, desenvolvida através de fantasiosa **narrativa insipiente e ofensiva** — sem qualquer substrato fático — com o fito de deslegitimar, perante a opinião pública, o nome do candidato opositor.

27. Nesse sentido, os representados evidentemente com o condão de atingir a integridade do processo eleitoral, manipularam a opinião pública com fatos **sabidamente inverídicos**. Emerge, assim, indisfarçável tática de desinformação nas suas condutas, as quais tiveram um alcance de centenas de milhares de pessoas diretamente e de milhões indiretamente – por meio dos compartilhamentos e interações com o conteúdo.

28. Desse modo, cabe ressaltar, que não há que se confundir a divulgação de desinformação com o exercício do direito à liberdade de expressão. Sobre o ponto, o

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4017 | 99993-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. M, Salas 2059-2064 - Asa Norte
Ed. JON Brasília, DF | CEP: 70.830-018



artigo 27 da Resolução, parágrafo 1º, da Resolução nº 23.610/2019¹⁷, bem explicita que a livre manifestação do pensamento encontra limitação quando ofende a honra ou a imagem de candidatos, partidos, federações, coligações ou, ainda, quando divulga fatos sabidamente inverídicos.

29. Verifica-se na presente representação, nítida propagação de conteúdo gravemente descontextualizado que atinge a integridade do processo eleitoral, conduta expressamente vedada pelo artigo 9º -A da Resolução-TSE nº 23.610/2019¹⁸.

30. No mais, cumpre frisar que não há o que se falar de mera manifestação do pensamento dos Representados, que nitidamente tentaram levar o eleitor a acreditar em imaginária vinculação do Ex-Presidente à ditaduras e à fome, como já delineado nos fatos supramencionados, vilipendiando frontalmente o disposto no artigo 22 da Resolução, inciso X, da Resolução-TSE nº 23.610/2019¹⁹.

31. A desinformação é, sobretudo, um mal que vem assolando o mundo e especialmente o Brasil, por configurar a manipulação de fatos através da subversão do

¹⁷ Art. 27. É permitida a propaganda eleitoral na internet a partir do dia 16 de agosto do ano da eleição. § 1º A livre manifestação do pensamento de pessoa eleitora identificada ou identificável na internet somente é passível de limitação quando ofender a honra ou a imagem de candidatas, candidatos, partidos, federações ou coligações, ou divulgar fatos sabidamente inverídicos, observado o disposto no art. 9º-A desta Resolução. (grifou-se)

¹⁸ Art. 9º-A. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos, devendo o juízo eleitoral, a requerimento do Ministério Público, determinar a cessação do ilícito, sem prejuízo da apuração de responsabilidade penal, abuso de poder e uso indevido dos meios de comunicação. (Incluído pela Resolução nº 23.671/2021)

¹⁹ Art. 22, X. Não será tolerada propaganda, respondendo a pessoa infratora pelo emprego de processo de propaganda vedada e, se for o caso, pelo abuso de poder: X - que caluniar, difamar ou injuriar qualquer pessoa, bem como atingir órgãos ou entidades que exerçam autoridade pública;

que realmente ocorreu, de modo a modificar a verdade e alterar o entendimento dos cidadãos, inclusive no que tange ao processo eleitoral.

32. Lições que se alinham ao entendimento exarado pela e. Min Maria Cláudia Bucchianeri proferida nos autos da representação nº 0600929-09.2022.6.00.0000, em 06.09.2022:

E, ao fazê-lo, registro que, consoante já tive a oportunidade de enfatizar em decisões anteriores (Rp nº 0600229-33/DF), tenho para mim que a intervenção judicial sobre o *livre mercado de ideias políticas* deve sempre se dar de forma excepcional e necessariamente pontual, apenas se legitimando naquelas hipóteses de desequilíbrio ou de excesso capazes de vulnerar princípios fundamentais outros, igualmente essenciais ao processo eleitoral, tais como a **higidez e a integridade do ambiente informativo, a paridade de armas entre os candidatos, o livre exercício do voto e a proteção da dignidade e da honra individuais.**

O caso em exame envolve suposta propagação de desinformação, comportamento que vulnera a **higidez e a integridade do ambiente informativo, valores que justificam e legitimam a intervenção corretiva da Justiça Eleitoral.**

Isso porque, embora a maximização do espaço de livre mercado de ideias políticas e a ampla liberdade discursiva na fase da pré-campanha e no curtíssimo período oficial de campanha qualifiquem-se como fatores que catalisam a competitividade da disputa e estimulam a renovação política e a vivacidade democrática, a **difusão de informações inverídicas, descontextualizadas ou enviesadas** configuram prática **desviante**, que gera verdadeira *falha no livre mercado de ideias políticas*, deliberadamente forjada para **induzir o eleitor a erro no momento de formação de sua escolha.**

Daí as preciosas observações de Elder Maia Goltzman, na preciosa obra "Liberdade de Expressão e Desinformação em Contextos Eleitorais" (Belo Horizonte: Ed. Fórum, 2022, p. 54), no sentido de que "é preciso empoderar o cidadão para que possa tomar suas decisões relativas à esfera pública de maneira consciente e ancorado em informação de qualidade, não em narrativas fabricadas ou versões construídas e distribuídas para ludibriá-lo".



Em resumo: não há a menor dúvida de que a **desinformação** e a **desconstrução de figuras políticas a partir de fatos sabidamente inverídicos ou substancialmente manipulados** devem ser **rapidamente reprimidas pela Justiça Eleitoral**, por configurarem, como dito, verdadeira falha no livre mercado de circulação das ideias políticas, que pode desembocar na **indução do eleitor a erro**, com comprometimento da própria **liberdade de formação da escolha cidadã**.

A **identificação**, no entanto, daquilo que possa ser enquadrado como **conteúdo desinformativo** traz significativos desafios.

Reconheço que a **desinformação se limita à difusão de mentiras propriamente ditas, compreendendo, por igual, o compartilhamento de conteúdos com elementos verdadeiros, porém gravemente descontextualizados, editados ou manipulados, com o especial intento de desvirtuamento da mensagem difundida, com a indução dos seus destinatários a erro.**

(Grifou-se)

33. Na mesma esteira a e. Ministra Cármen Lúcia, no bojo dos autos da Representação nº 0600763-74.2022.6.00.0000, consignou que:

Observei, então, ser necessário respeitar-se aquele direito considerando-se a pessoa sobre quem se expressa algo e também a pessoa que se expressa, porque os direitos são interligados e a observância do direito é dever de todos. **Por isso, mentiras, divulgações inverídicas e caluniosas, difamatórias ou injuriosas são tidas, desde o século passado, no direito brasileiro, como ilícitos penais. Anotei, naquela assentada, que a ocorrência de divulgação de informações falsas pelos novos meios de propaganda eleitoral, não poucas vezes se alimentam da ferocidade destrutiva das mentiras novas e agressivas, amplamente nomeadas como fake news:**

'Assim, com a revolução tecnológica da internet e das mídias sociais, a propaganda eleitoral se dá por novos meios e por divulgação instantânea para milhares de pessoas, muitas vezes veiculando informações falsas (...). As notícias são transmitidas, atualmente, principalmente por meio das redes sociais e aplicativos de mensagens e cada vez menos pela imprensa tradicional, o que contribui para o aumento da desinformação e das notícias falsas, as quais circulam livre e gratuitamente nas redes sociais e nos aplicativos de mensagens. A

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99963-2576
advogados@aragoanferraro.com
www.aragoanferraro.com
SGAN 601, Bl. H, salas 2059-2064 - Asa Norte
Ed. ION Brasília, DF | CEP: 70.830-018

esse respeito, Francisco Balaguer Callejón lembra que enquanto os meios de comunicação tradicionais são abertos e transparentes, as redes sociais muitas vezes se alimentam da instabilidade das fake news (págs. 294 e 297 do acórdão).'

Não se cogita do exercício absoluto daquele direito fundamental à livre manifestação do pensamento. Por isso, é juridicamente possível a restrição do desempenho daquele direito fundamental quando constatada eventual ilicitude no seu exercício em detrimento de igual direito de outrem.

(Grifou-se)

34. É por isto que a desinformação, que caracteriza a essência das publicações objeto desta ação, significa prática antijurídica, tendo em vista que afeta a liberdade de conhecimento dos cidadãos e, automaticamente, influencia negativamente no processo eleitoral por afetar o direito livre de voto.

35. Neste contexto perigoso de manipulação da verdade em ano eleitoral, em que a propagação de desinformação afeta a lisura do processo eleitoral — haja vista a nefasta experiência das eleições de 2018 — essa c. Corte Eleitoral tem trabalhado e apresentado medidas no esforço de combater a propagação de desinformação, especialmente no que tange ao pleito que se avizinha. Foram firmadas, inclusive, parcerias com diversas plataformas de aplicação, além de promovidos eventos e planos estratégicos para combater a desinformação no país — especialmente nas eleições que ocorrerão no presente ano.

36. Assim, patente o esforço da Corte Eleitoral em combater e evitar que a desinformação influencie o pleito de 2022, a fim de manter a lisura do processo eleitoral, de modo a proibir veiculação e compartilhamento de notícias inverídicas e/ou

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4037 | 99963-2576
advogados@aragoeferraro.com
www.aragoeferraro.com
SGAN 601, Bl. H, salas 2059-2064 - Asa Norte
Ed. JON Brasília, DF | CEP: 70.830-018



descontextualizadas que, quando identificadas, devem ser removidas e os responsáveis instados a se abster de compartilhar.

37. É justamente neste contexto que resta evidenciado que as publicações objeto desta ação contrariam o art. 9º-A, art. 22 e art. 27 da Resolução nº 23.610/2019, uma vez que os **Representados conscientemente divulgaram conteúdo desinformador para incutir no eleitor a lunática teoria tecida com a agulha da imaginação de vinculação do ex-Presidente Luiz Inácio Lula da Silva à pecha de ditador.**

38. Ademais, perfilhando o entendimento do art. 22, inciso X da Resolução-TSE n. 23.610/2019, este eg. Tribunal Superior Eleitoral possui entendimento firmado neste sentido, como se observa do julgado abaixo colacionado:

Propaganda eleitoral antecipada. Propaganda negativa. Multa. 3. No mérito, o Tribunal a quo manteve a condenação, mas reduziu o valor da multa imposta na sentença para R\$ 5.000,00, tendo concluído pela configuração de propaganda eleitoral antecipada negativa, por ter o representado veiculado em sua página pessoal do Instagram notícias acerca da gestão do então pré- candidato à reeleição ao cargo de Governador do Estado. 4. Nos termos da jurisprudência do Tribunal Superior Eleitoral: 'A divulgação de publicação, antes do período permitido, que ofende a honra de possível futuro candidato constitui propaganda eleitoral negativa extemporânea' [...] (TSE, AgRg no Respe n. 060009906, Rel. Min. Sérgio Banhos, Dje 17.09.2019).

39. Considerando que a disseminação de desinformação com conteúdo manifestamente apto a influenciar nas eleições que ocorrerão no próximo final de semana, tem-se que representam ato ilícito, devendo ser combatida por esta c. Corte Eleitoral.

Brasília
 SAS Quadra 1 Bloco M Lote 1
 Ed Libertas Conj. 1009
 Asa Sul 70070-935
 Tel./Fax: +55 61 3326.9905
 www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99988-2576
 advogados@aragaoeferraro.com
 www.aragaoeferraro.com
 SGAEN 601, Bl. M, calçav 2053-2064 - Asa Norte
 Ed. ION Brasília, DF | CEP: 70.830-018

40. Portanto, requer-se a condenação da Representada a fim de manter incólume o pleito eleitoral que se avizinha, determinando-se a abstenção de novas práticas de igual natureza, com a fixação de multa para o caso de descumprimento.

III – DA NECESSIDADE DE CONCESSÃO DA MEDIDA LIMINAR

41. Consoante o *caput* do art. 300 do Código de Processo Civil, a tutela de urgência será concedida quando houver elementos que evidenciem a probabilidade do direito e o perigo de dano ou o risco ao resultado útil do processo.

42. A probabilidade do direito no presente caso é a manifesta violação às normas e aos princípios que regem a propaganda eleitoral, sobretudo a Resolução nº 23.610/2019 deste c. TSE, de modo a ferir a lisura do processo eleitoral, conforme demonstrado nos tópicos anteriores.

43. Isso porque trata-se de publicação com objetivo de traçar claudicante e inverídica afirmação, com o intuito de incutir ao eleitor questionamentos quanto à reputação do candidato Luiz Inácio Lula da Silva ao suscitar falsa narrativa de que o candidato irá impor uma ditadura no Brasil, bem como levará a uma situação de pobreza extrema, com fome generalizada.

44. Assim, é preocupante, não apenas ao Representante, mas ao interesse da democracia brasileira como um todo, a leviana estratégia de manipulação de narrativas com consequente violação da liberdade de pensamento e cidadania dos eleitores brasileiros.



45. Ademais, dada a proximidade do pleito eleitoral, mais do que nunca se faz necessária a prevalência da legislação eleitoral e regulação deste e. TSE acerca do combate a informações sabidamente inverídicas e com dolo específico de manipular o pleito eleitoral, vilipendiando a liberdade de pensamento e opinião dos brasileiros e cerceando o direito à cidadania e ao voto livre.

46. O perigo do dano encontra-se na perpetuação de desinformações que maculam a lisura do processo eleitoral, configurando propaganda eleitoral negativa contra o ex-presidente Luiz Inácio Lula da Silva e ao Partido dos Trabalhadores, por meio de publicações veiculadas na internet. Aliás, as publicações dessa natureza são compartilhadas e espalhadas em velocidade exponencial, de modo a aumentar significativamente o alcance das desinformações aos eleitores e às eleitoras, ampliando, desta forma, o impacto negativo das publicações objeto desta representação.

47. Para isso, os impactos negativos das publicações impugnadas restam evidenciados, o qual comprova que o conteúdo inverídico teve alcance exponencial, mostrando-se ser significativo agente de interferência na liberdade de opinião e pensamento dos eleitores, uma vez que os posts impugnados agem de forma coordenada para atribuir conduta moralmente reprovável ao candidato Luiz Inácio Lula da Silva.

48. Portanto, os impactos negativos da publicação em comento restam evidenciados, uma vez que possuem conteúdo eleitoral e são compartilhados na internet, alcançando um número inestimável de eleitores brasileiros de modo a

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed. Liberdade Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99963-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, B1, H, salas 2059-2064 - Asa Norte
Ed. ION Brasília, DF | CEP: 70.510-018

influenciar diretamente na sua escolha, violando o direito de voto livre e automaticamente a democracia, o que torna urgente medida judicial para cessar os danos.

49. Portanto, em sede liminar, requer-se seja determinada: (i) a remoção da publicação ora denunciada; e (ii) que a Representada se abstenha de veicular notícias com o mesmo teor, de modo a preservar a higidez e a lisura das eleições e do processo eleitoral.

IV – DOS PEDIDOS

50. Por todo o exposto, a Coligação Brasil da Esperança requer:

50.1 Liminarmente:

50.1.1. Seja determinado aos Representados e às redes sociais Instagram, Facebook e Twitter que removam os conteúdos desinformativos objeto desta ação, sob pena de multa a ser arbitrada por esta c. Corte, encontrada nas URLs a seguir indicadas:

<https://www.instagram.com/reel/CkKfH98JWGO/>

<https://www.instagram.com/reel/CkKRzndAEX6/>

<https://www.instagram.com/p/CkJeL4MgVPa/>

<https://www.instagram.com/reel/CkJI4lAlbH0/>

<https://www.instagram.com/reel/CkJ5lUeJD8j/>

<https://www.facebook.com/ZambelliOficial/videos/1109802496203573>

<https://www.facebook.com/photo?fbid=664400138367725&set=a.518100476331026>



<https://twitter.com/leandroruschel/status/1584901522651058176>

<https://twitter.com/CarolDeToni/status/1584993966084485120>

50.2. Seja determinado aos Representados que se abstenham de veicular outras notícias e/ou publicações que contenham o mesmo teor, sob pena de multa, a ser arbitrada por esta c. Corte.

51. A citação dos Representados, para, querendo, apresentar defesa;

52. No mérito:

52.1. A confirmação da medida liminar, de modo a determinar que a publicação seja removida e que a Representada se abstenha de veicular outras desinformações com o mesmo teor; e

52.2. A condenação por propaganda irregular e a consequente aplicação da multa de pena máxima conforme previsão legal, a Representada.

Nestes termos, pede deferimento.

Brasília, em 26 de outubro de 2022.

Cristiano Zanin Martins
OAB/SP 172.730

Eugênio Aragão
OAB/DF 4.935

Valeska Teixeira Zanin Martins
OAB/SP 153.720

Angelo Longo Ferraro
OAB/DF 37.922

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4057 | 99963-2576
advogados@aragaoeferraro.com
www.aragaoeferraro.com
SGAN 601, Bl. H, salas 2059-2064 - Asa Norte
Ed. ION Brasília, DF | CEP: 70.820-018



Maria de Loudes Lopes
OAB/SP 77.513

Marcelo Winch Schmidt
OAB/DF 53.599

Victor Luga R. Chen
OAB/SP 448.673

Miguel Filipi Pimentel Novaes
OAB/DF 57.469

Eduarda P. Quevedo
OAB/SP 464.676

Maria Eduarda Praxedes Silva
OAB/DF 48.704

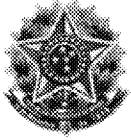
Giovanna Galeotti de Paiva
OAB/SP 438.889

Roberta Nayara Pereira Alexandre
OAB/DF 59.906

Guilherme Q. Gonçalves
OAB/DF 37.961

Brasília
SAS Quadra 1 Bloco M Lote 1
Ed Libertas Conj. 1009
Asa Sul 70070-935
Tel./Fax: +55 61 3326.9905
www.zaninmartinsadvogados.com.br

(61) 3246-4017 | 99963-2576
advogados@aragoaeferro.com
www.aragoaeferro.com
SGAN 601, Bl. H, salas 2059-2064 - Asa Norte
Ed. ION Brasília, DF | CEP: 70.830-018



04/11/2022

Número: **0601869-71.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **04/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Extraído do SEI 2022.00.000016070-4**

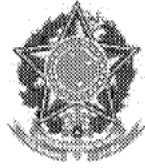
Segredo de justiça? **SIM**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes		Procurador/Terceiro vinculado	
TRIBUNAL SUPERIOR ELEITORAL (REQUERENTE)			
Procurador Geral Eleitoral (FISCAL DA LEI)			
Documentos			
Id.	Data da Assinatura	Documento	Tipo
15834 5113	04/11/2022 19:36	<u>Decisão</u>	Decisão

index: PETIÇÃO CÍVEL (241)-0601869-71.2022.6.00.0000-[Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa]-DISTRITO FEDERAL-BRASÍLIA



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601869-71.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

**RELATOR: MINISTRO ALEXANDRE DE MORAES
REQUERENTE: TRIBUNAL SUPERIOR ELEITORAL**

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, que detectou, nesta data, a realização de uma *live* de caráter sensacionalista, com a apresentação de acusações vagas e sem provas, que atingem a integridade e a normalidade do processo eleitoral, incentivando, com base em falsas afirmações de fraude, a recusa dos resultados e, eventualmente, uma ruptura institucional.

As manifestações em questão foram realizadas nos seguintes canais e perfis:

<https://www.youtube.com/c/LaDerechaDiario> (Youtube)

<https://instagram.com/canalhipocritas?igshid=YmMyMTA2M2Y=> (Instagram)

<https://instagram.com/laderechadiario?igshid=YmMyMTA2M2Y=> (Instagram)

(20) Vidotti (@vidz1979) / Twitter (Twitter)

BrazilWasStolen - Twitch (Twitch)

Considerando a gravidade e a notoriedade dos fatos narrados, dispensável a realização de diligência de constatação.

É o breve relato. Decido.

A legislação vigente confere à Justiça Eleitoral uma ferramenta de ampla aplicação, voltada à preservação da paridade de armas, da normalidade e da integridade do processo eleitoral, podendo abranger a comunicação em sentido amplo, por meio de medidas preventivas ou repressivas necessárias a evitar ou afastar a prática de atos que atentem contra as normas estruturantes da competição eleitoral.

À luz do que dispõe o § 2º do art. 41 da Lei das Eleições, o encargo em questão abarca não apenas as violações de propaganda, mas ainda todo tipo de ilicitude capaz de comprometer a higidez das eleições, sendo esse, precisamente, o quadro dos ataques institucionais levados a efeito no campo da desinformação.

A partir dos fatos relatados, estão presentes, em hipótese, os ilícitos previstos nos arts. 2º da Res.-TSE nº 23.714/2022 e 296 do Código Eleitoral, e 286 do Código Penal:

Art. 2º. É vedada a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos.

Art. 296. Promover desordem que prejudique os trabalhos eleitorais:

Pena – detenção até dois meses e pagamento de 60 a 90 dias-multa.

Art. 286. Incitar, publicamente, a prática de crime.

Pena – detenção, de três a seis meses, e multa.

O art. 2º da Res.-TSE nº 23.714/2022 visa a preservar as condições de normalidade do pleito, eliminando os riscos sociais associados à desinformação, a partir da disseminação generalizada de notícias falsas que prejudicam a aceitação pacífica dos resultados, em manifesta lesão à soberania popular (arts. 1º, parágrafo único e 14, “caput” e § 9º, da Constituição da República) e à estabilidade do processo democrático.

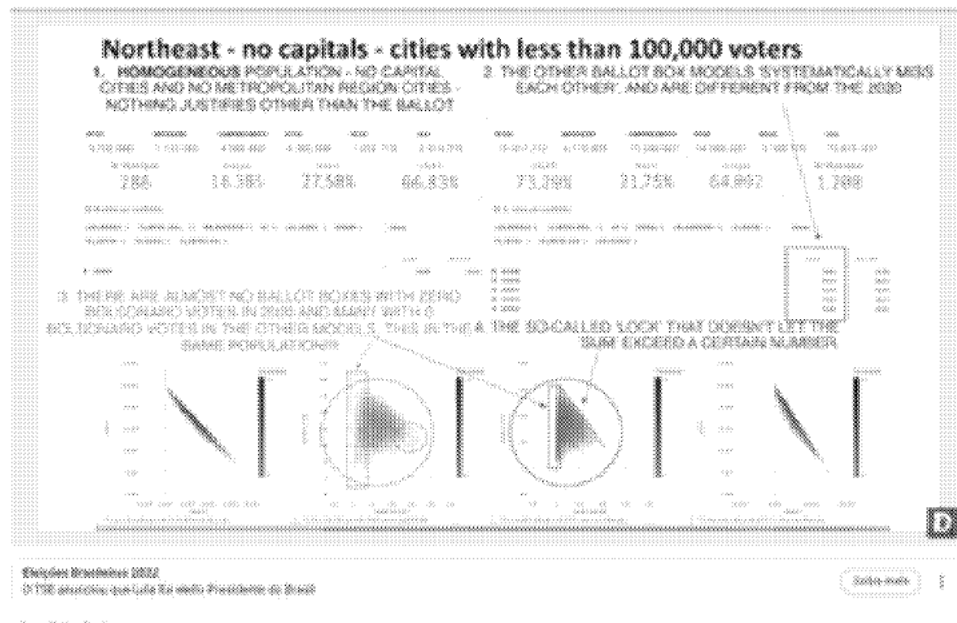
Em paralelo, a divulgação, consciente e deliberada de informações falsas sobre a atuação da Justiça Eleitoral ou das autoridades ou servidores que a compõem, atribuindo-lhes, direta ou indiretamente, comportamento fraudulento ou ilícito, implica na promoção de desordem

informativa que prejudica, substancialmente, a realização de seus correspondentes encargos institucionais, atraindo, em tese, a prática do crime previsto no art. 296 do Código Eleitoral.

Por fim, o incentivo público à intervenção militar, com a conseqüente anulação da vontade popular livremente externada nas urnas eletrônicas configura o delito de incitação ao crime, previsto no art. 286 do Código Penal, uma vez que a abolição violenta do Estado democrático de direito e a tentativa de golpe de Estado estão igualmente tipificadas naquele código, designadamente nos arts. 359-L e 359-M.

Além disso, é evidente que as manifestações públicas detectadas possuem potencial para tumultuar o processo eleitoral, na medida em que incentivam comportamentos ilegais e beligerantes, atraindo, como consequência, a possibilidade de alterações ou episódios potencialmente violentos.

Observem-se, nessa linha, algumas passagens relevantes, apenas a título exemplificativo, das quais se extrai potencial para a ocorrência de traumas ou alterações sociais:



Fonte: Reprodução de tela.



Vidotti
@vidz1979

...

Houve fraude nas urnas?

Como profissional de TI, sempre fui cético com a possibilidade. É uma mentira muito grande para ser mantida em segredo por muito tempo e para muitas pessoas.

Segue o fio... 🧵 (1/n)

Translate Tweet

12:45 AM · Nov 3, 2022 · Twitter Web App

10.9K Retweets 1,357 Quote Tweets 33.2K Likes

URGENTE

Convocação para coletiva de imprensa para canais de TV e acompanhamento ao vivo da apresentação da auditoria privada sobre as eleições no Brasil

No dia 4 de novembro, às 17h (horário de Buenos Aires), apresentaremos (e explicaremos) a auditoria privada sobre as anomalias nas urnas eletrônicas do 1º e 2º turno das eleições brasileiras.

Este relatório deve ser divulgado da Argentina, pois por ordem do TSE, nenhum meio de comunicação ou grupo privado de pessoas pode divulgar informações que ponham em dúvida o resultado eleitoral deste ano.

As anomalias encontradas e o relatório dos resultados serão explicados e apresentados durante esta live e coletiva de imprensa.

Também forneceremos toda a documentação com os conjuntos de dados, e instruções para que outros especialistas possam fazer a mesma análise, e até mesmo indivíduos que queiram fazer suas próprias pesquisas, já que isso foi feito com dados públicos do TSE.

Os links das diferentes live serão enviados minutos antes do início por motivos de segurança.

Muito obrigado

carull@carull.com · Seguir

carull@carull.com | #urgente #eleicoesbrasil #segurançadadados

Vejam @vidz1979 falando para mais informações 📺

Retweets: 12 · Ver tradução

lucianokawachi @lucianokawachi

12 · 180 respostas · Responder · Ver tradução

... Ver respostas (24)

opinioneselectorales @opinioneselectorales

12 · 4 respostas · Responder · Ver tradução

... Ver respostas (5)

reginakarateportugal @reginakarateportugal

12 · 48 respostas · Responder · Ver tradução

... Ver respostas (59)

andersonfatefatefatefatefate @andersonfatefatefatefate

12 · 160 respostas · Responder · Ver tradução

... Ver respostas (22)

isabel99 @isabel99

12 · 160 respostas · Responder · Ver tradução

... Ver respostas (22)

Cartão Curtido por @alexei1988 e outros 794.542 pessoas

NA LÍNGUA

Brasil Retweetado por @brasil

Trata-se de condutas ilegais de natureza grave, com grande potencial para tumultuar as eleições em andamento e que, como se sabe, terminam somente com o ato de diplomação. Fica assim autorizado o exercício do poder administrativo para fazer cessar ilícitos, conferido às autoridades eleitorais pelos arts. 249 do Código Eleitoral, 41 da Lei 9.504/1997, e 2º,

§ 1º, da Res.-TSE nº 23.714/2022.

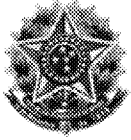
Ante o exposto, com base nos arts. 2º, § 1º da Res.-TSE nº 23.714/2022, 41, da Lei nº 9.504/97, 249 e 296 do Código Eleitoral, **DETERMINO** às plataformas Youtube, Twitter, Twitch e Instagram a imediata e definitiva remoção dos canais e perfis acima mencionados, sob pena de multa ora fixada no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação.

Cumpra-se com urgência.

Após, ENCAMINHEM-SE cópia eletrônica dos autos à Procuradoria-Geral Eleitoral para que promova as medidas cabíveis.

Brasília, 4 de novembro de 2022.

Marco Antonio Martin Vargas
Juiz Auxiliar da Presidência do Tribunal Superior Eleitoral



05/06/2023

Número: **0601964-04.2022.6.00.0000**

Classe: **PETIÇÃO CÍVEL**

Órgão julgador colegiado: **Colegiado do Tribunal Superior Eleitoral**

Órgão julgador: **Ministro Presidente Alexandre de Moraes**

Última distribuição : **23/11/2022**

Valor da causa: **R\$ 0,00**

Assuntos: **Propaganda Política - Propaganda Eleitoral - Divulgação de Notícia Sabidamente Falsa**

Objeto do processo: **Documentos extraídos do SEI 17074-2**

Segredo de Justiça? **NÃO**

Justiça gratuita? **NÃO**

Pedido de liminar ou antecipação de tutela? **SIM**

Partes	Advogados
TRIBUNAL SUPERIOR ELEITORAL (INTERESSADO)	

Outros participantes	
Procurador Geral Eleitoral (FISCAL DA LEI)	

Documentos			
Id.	Data da Assinatura	Documento	Tipo
159033471	05/06/2023 10:37	<u>Decisão</u>	Decisão



TRIBUNAL SUPERIOR ELEITORAL

PETIÇÃO CÍVEL (241) Nº 0601964-04.2022.6.00.0000 (PJe) - BRASÍLIA - DISTRITO FEDERAL

RELATOR: MINISTRO ALEXANDRE DE MORAES

INTERESSADO: TRIBUNAL SUPERIOR ELEITORAL

DECISÃO

Trata-se de procedimento iniciado a partir de informação encaminhada pela Assessoria Especial de Enfrentamento à Desinformação, acerca de perfil nas redes sociais, orientado para a divulgação de desinformação contra as eleições e apologia à intervenção militar, em detrimento da vontade popular registrada nas Eleições 2022.

Por intermédio da decisão de ID 158579784, determinei:

i) a reativação da conta dos perfis Wagner Pereira, José Crastechini, Rita de Cássia Serrão e Fernando Conrado no Twitter, mantendo-se, porém a remoção das postagens irregulares veiculadas; e

ii) a aplicação de MULTA DIÁRIA, no valor de R\$ 20.000,00 (vinte mil reais), a incidir na hipótese de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

Por fim, iii) comunique-se a Plataforma Digital Twitter para cumprimento imediato da presente decisão; e iv) diante da pertinência temática ao Inquérito 4.879, encaminhem-se os autos ao SUPREMO TRIBUNAL FEDERAL.

A Assessoria de Enfrentamento à Desinformação aponta o descumprimento da determinação por parte de Wagner Pereira e Rita de Cássia (ID 158986117):

1) Wagner Pereira:

Da análise dos conteúdos veiculados no perfil "wagnerP85638598" no Twitter, observa-se a veiculação de mensagens atentatórias à confiabilidade da Justiça Eleitoral e do sistema eletrônico de votação.

No dia 1º de maio de 2023, o perfil postou as seguintes mensagens:



Link: <https://twitter.com/wagnerP85638598/status/1653005684307382272>



Link: <https://twitter.com/wagnerP85638598/status/1653003581157437440>

Ademais, o perfil permanece a divulgar fatos que já foram desmentidos, como no seguinte retweet, datado de 3 de março do corrente ano, contendo vídeo no qual a Jovem Pan News teria divulgado a vitória de Bolsonaro nas eleições presidenciais de 2022:



Link da postagem: <https://twitter.com/vanitoc1/status/1627170054935543810>

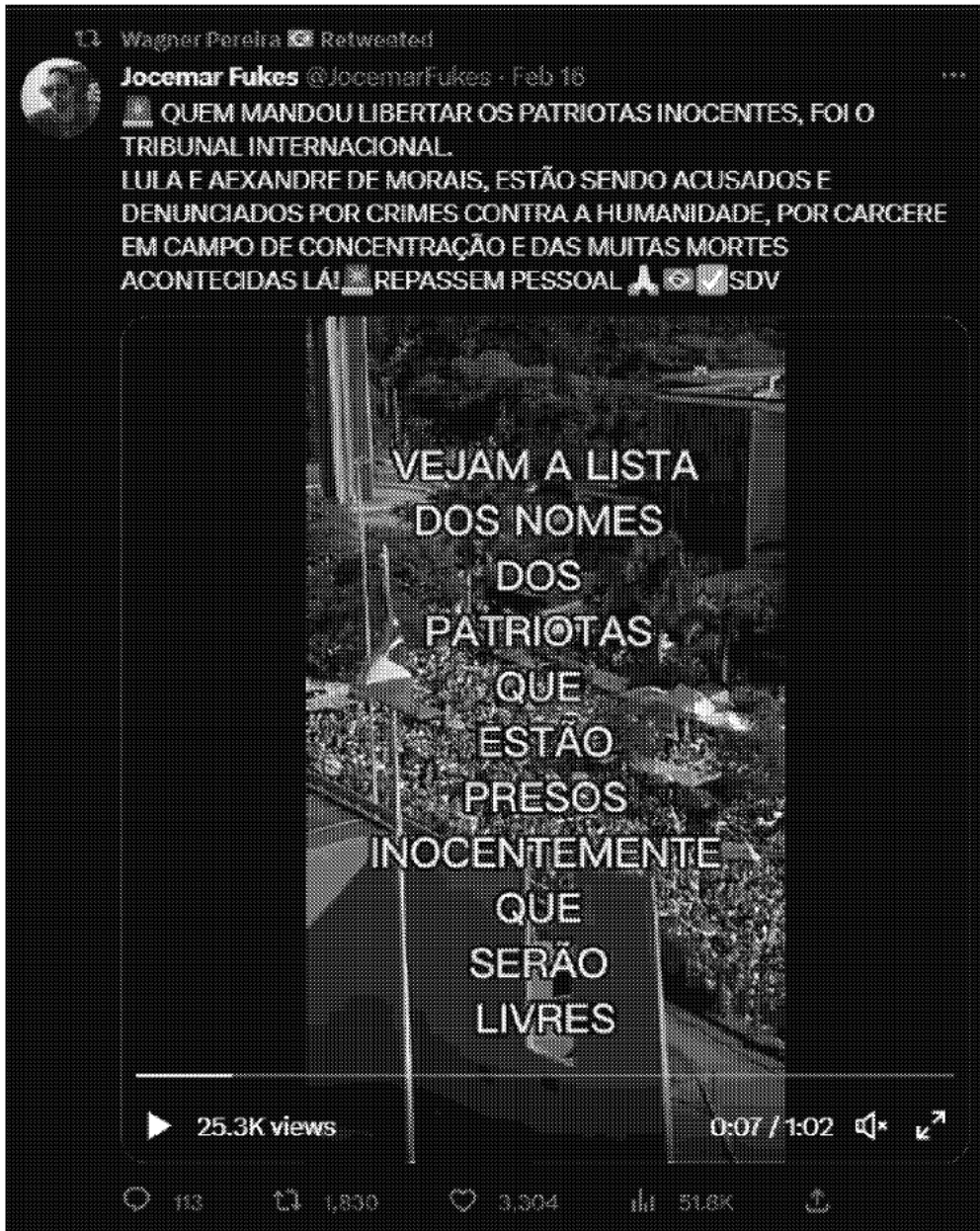
O vídeo, que circulou muito durante o período eleitoral de 2022, já foi desmentido por diversas agências de checagem de fatos e pelo próprio TSE:

LUPA: <https://lupa.uol.com.br/jornalismo/2022/10/05/grafico-55-bolsonaro-tse-resultado-no-parana>

AFP: <https://checamos.afp.com/doc.afp.com.32KT4AJ>

TSE: <https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/esclarecimento-video-que-aponta-55-dos-votos-para-um-dos-candidatos-nao-e-falha-do-tse-mas-resultado-no-parana/#>

No mesmo dia, em outra publicação, Wagner Pereira espalha notícia falsa também já desmentida por várias agências de checagem:



Link da postagem: <https://twitter.com/JocemarFukes/status/1626249091100319745>

Checagens de fatos:

ESTADÃO VERIFICA: <https://www.estadao.com.br/estadao-verifica/tribunal-internacional-presos-soltos-8-janeiro/>

AOS FATOS: <https://www.aosfatos.org/noticias/tribunal-internacional-nao-soltou-golpistas-presos/>

UOL CONFERE: <https://noticias.uol.com.br/confere/ultimas-noticias/2023/03/06/tribunal-internacional-soltura-presos-dia-8-checagem.htm>

LUPA: <https://lupa.uol.com.br/jornalismo/2023/02/15/tribunal-internacional-presos-atos>

BOATOS.ORG: <https://www.boatos.org/politica/tribunal-internacional-mandou->

[alexandre-de-moraes-libertar-patriotas-manifestacao-golpista-boato.html](#)

Por fim, importa mencionar que três das postagens que deram ensejo à decisão 158579784 permanecem ativas nos seguintes links:

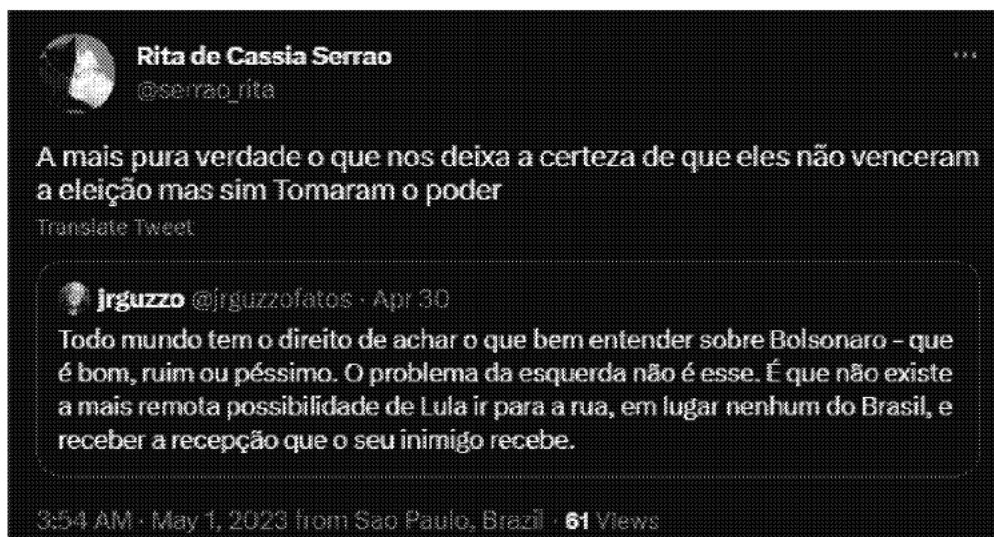
<https://twitter.com/wagnerP85638598/status/1587386556339322882>

<https://twitter.com/JocemarFukes/status/1589113618041143296>

<https://twitter.com/wagnerP85638598/status/1590272634482470916>

2) Rita de Cássia:

No perfil @serrao_rita no Twitter, consta postagem recente (de 1º de maio de 2023) levantando dúvidas sobre o processo eleitoral:



URL da postagem: https://twitter.com/serrao_rita/status/1652929384259411968

As postagens que deram ensejo à decisão 158579784 não foram encontradas.

URL do post: <https://twitter.com/fernandoconrado/status/1602299748526051328>

As postagens que deram ensejo à decisão 158579784 não foram encontradas.

É o breve relato.

Nos termos da decisão ID 158579784, ficou determinada a reativação da conta dos perfis Wagner Pereira, José Crastechini, Rita de Cássia Serrão e Fernando Conrado no Twitter, mantendo-se, porém a remoção das postagens irregulares veiculadas.

Ainda, na mencionada decisão, foi determinada a imposição de multa cominatória, consistente na abstenção de publicação, promoção, replicação e compartilhamento das notícias fraudulentas (fake news), sob pena de multa diária de R\$ 20.000,00 (vinte mil reais) no caso de reiteração de divulgação dos conteúdos bloqueados ou de publicação de outras mensagens instigadoras ou incentivadoras de golpe militar, atentatórias à JUSTIÇA ELEITORAL e ao Estado Democrático de Direito.

A partir da Informação ID 158986117, apresentada pela Assessoria Especial de Enfrentamento à Desinformação, constata-se a recalcitrância de Wagner Pereira e Rita de Cássia na propagação de desinformação contra as eleições, em franca apologia a atos antidemocráticos.

Trata-se de nítido descumprimento da medida imposta, o que enseja o reconhecimento da multa diária no valor de R\$ 20.000,00 (vinte mil reais), a incidir desde 1º/5/2023, conforme autoriza o art. 4º da Res.-TSE 23.714/2022, o qual prevê o combate à produção sistemática de desinformação sobre o processo eleitoral.

Ante o exposto, DETERMINO:

a) a expedição de ofício ao Twitter para que proceda a imediata remoção dos links abaixo relacionados, sob pena de multa no valor de R\$150.000,00 (cento e cinquenta mil reais) por hora de descumprimento, contada a partir do término da segunda hora após o recebimento da notificação:

<https://twitter.com/wagnerP85638598/status/1653005684307382272>

<https://twitter.com/wagnerP85638598/status/1653003581157437440>

<https://twitter.com/vanitoc1/status/1627170054935543810>

<https://twitter.com/JocemarFukes/status/1626249091100319745>

<https://twitter.com/wagnerP85638598/status/1587386556339322882>

<https://twitter.com/JocemarFukes/status/1589113618041143296>

<https://twitter.com/wagnerP85638598/status/1590272634482470916>

https://twitter.com/serrao_rita/status/1652929384259411968

b) a imposição de multa diária a Wagner Pereira e Rita de Cássia Serrão, no valor de R\$ 20.000,00 (vinte mil reais), a incidir desde 1º/5/2023 até a definitiva remoção dos conteúdos acima relacionados, bem como a IMEDIATA intimação dos envolvidos, inclusive pelos meios eletrônicos disponíveis, além da devida retirada do sigilo dos presentes autos.

Publique-se e cumpra-se com urgência. Após dê-se ciência ao Ministério Público Eleitoral.

Brasília, 1º de junho de 2023.

Ministro **ALEXANDRE DE MORAES**
Presidente



**THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION'S
SILENCE: THE CASE OF BRAZIL**

Part II

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



May 7, 2024

BRAZIL’S CENSORSHIP OF FREE SPEECH ONLINE

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government are conducting oversight of how and to what extent the Executive Branch has coerced or colluded with companies and other intermediaries to censor lawful speech.¹ As witnesses have testified to the Select Subcommittee, the United States must be careful to protect and defend freedom of speech in America, especially amid a wave of government censorship and other anti-democratic actions worldwide.²

On April 17, 2024, the Committee and Select Subcommittee issued a 540-page report regarding the Brazilian government’s censorship efforts and the Biden Administration’s silence on the issue.³ On the same day, the Committee and the Select Subcommittee wrote to the U.S. Department of State’s Under Secretary for Civilian Security, Democracy, and Human Rights, and the Special Envoy and Coordinator for Digital Freedom asking for a briefing “about how the State Department intends to respond to these attacks on free speech in Brazil,” and for relevant documents and communications between the State Department and the government of Brazil regarding the censorship orders.⁴

The Committee and Select Subcommittee’s report described how Brazil’s ruling leftist government targeted, and largely succeeded in censoring, conservative members of the federal legislature, members of the judiciary, journalists, radio stations, and even a gospel singer.⁵ These censorship efforts have been spearheaded by Alexandre de Moraes, a justice on the Supreme Federal Court in Brazil, and the President of the Superior Electoral Court in Brazil.⁶

Since that report, the Committee and Select Subcommittee have obtained new documents that shed additional light on this censorship regime, including an April 2024 order to X as well as nine orders to Rumble or entities owned by Rumble.⁷ The newly obtained documents tell a story

¹ See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

² See generally Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary, 118th Cong. (Nov. 30, 2023) (written testimony of Rupa Subramanya) (“Across the world right now, governments, in the name of the good, are considering or adopting measures like we have in Canada. In Dublin, they’re about to enact a draconian hate-crime bill that poses a dire threat to free speech. In Paris, President Emanuel Macron has called for censoring online speech. In Brussels, the EU’s Internal Market Commissioner is calling for a crackdown on “illegal content.” **In Brasilia, they’re fighting “fake news” and “disinformation” by clamping down on legitimate online speech.** To say nothing of Russia and China and Iran. America is so exceptional—indispensable really. Please do not succumb to the same illiberal, the same authoritarianism. Please keep fighting for what you know is right. Canada is watching. The *whole world* is watching.”) (bolded emphasis added; italicized emphasis in original).

³ See STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION’S SILENCE: THE CASE OF BRAZIL (Comm. Print Apr. 17, 2024).

⁴ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to the Hon. Uzra Zeya, Under Secretary for Civilian Security, Democracy, and Human Rights, and the Hon. Eileen Donahoe, Special Envoy and Coordinator for Digital Freedom (Apr. 17, 2024).

⁵ STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE ATTACK ON FREE SPEECH ABROAD AND THE BIDEN ADMINISTRATION’S SILENCE: THE CASE OF BRAZIL (Comm. Print Apr. 17, 2024), at 4.

⁶ *Id.* at 3-5.

⁷ See App’x.

similar to the one detailed in the Committee and Select Subcommittee’s first report. Brazilian authorities, particularly Moraes, have ordered social media companies to suspend or remove popular accounts on Rumble.⁸ On December 22, 2023, Rumble’s CEO, Chris Pavlovski, announced that Rumble would not comply with the censorship demands from Brazilian courts and instead would “disable access to Rumble for users in Brazil.”⁹

Though in a different form, secret government-directed censorship is not a problem limited to Brazil or other foreign governments; it is happening here in the United States.¹⁰ Like Brazil, the Biden Administration has attacked journalists, political opponents, and Americans across the political spectrum in an attempt to silence the Administration’s many critics.¹¹ These attacks on free speech abroad serve as a warning for America.¹² The Committee and Select Subcommittee will continue to conduct oversight and develop legislative remedies to protect the First Amendment.

⁸ *Id.*

⁹ See Chris Pavlovski (@chrispavloski), X (Dec. 22, 2023, 4:05 PM), <https://twitter.com/chrispavloski/status/1738304870434631800>.

¹⁰ STAFF OF THE H. COMM. ON THE JUDICIARY AND THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION (Comm. Print May 1, 2024).

¹¹ *Id.*

¹² See generally Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary, 118th Cong. (Nov. 30, 2023) (written testimony of Rupa Subramanya).

APPENDIX

X (Twitter) Exhibit	4
Ex. 1: Federal Supreme Court, Petition 12.227 (Apr. 17, 2024)	5
Rumble Exhibits.....	34
Ex. 2: Federal Supreme Court, Investigation 4.879 (Jan. 11, 2023).....	35
Ex. 3: Federal Supreme Court, Investigation 4.923 (June 14, 2023).....	43
Ex. 4: Federal Supreme Court, Investigation 4.923 (July 28, 2023)	55
Ex. 5: Federal Supreme Court, Petition 9.935 (Dec. 14, 2023)	60
Ex. 6: Federal Supreme Court, Petition 9.935 (Dec. 14, 2023)	65
Ex. 7: Federal Supreme Court, Petition 10.802 (Jan. 5, 2024)	70
Ex. 8: Federal Supreme Court, Petition 10.802 (Jan. 5, 2024)	75
Ex. 9: Department of Federal Police, Petition 10.800 (Jan. 15, 2024)	80
Ex. 10: Department of Federal Police, Petition 10.800 (Jan. 15, 2024)	83

X (Twitter) Exhibit

Exhibit 1
Federal Supreme Court, Petition 12.227
(Apr. 17, 2024)



Supremo Tribunal Federal

SIGILOSO

Ofício eletrônico nº 7106/2024

Brasília, 17 de abril de 2024.

Ao Senhor
Administrador do X BRASIL (ex-TWITTER) Ltda.

Petição nº 12227

Senhor Administrador,

Encaminho-lhe os termos da decisão de cópia anexa para adoção das providências necessárias ao seu cumprimento, para que, no prazo de 2 (duas) horas, proceda o bloqueio aos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta Suprema Corte e a integral preservação do seu conteúdo:

<https://twitter.com/rafaelmorenos>

Atenciosamente,

Ministro Alexandre de Moraes
Relator
Documento assinado digitalmente

PETIÇÃO 12.227 DISTRITO FEDERAL

RELATOR : MIN. ALEXANDRE DE MORAES
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
REQDO.(A/S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO

DECISÃO

Trata-se de representação da Polícia Federal, subscrita pelo Delegado de Polícia Federal PAULO HENRIQUE BUFÁICAL COBUCCI, pelas medidas cautelares de busca e apreensão, sequestro e bloqueio de bens, afastamento de sigilo bancário e bloqueio de contas e proibição de propagação de ideias e atos antidemocráticos em face de RAFAEL MORENO SOUZA SANTOS (CPF 359.972.878-07), *"relacionado com o financiamento do(s) acampamento(s) em frente ao quartel do Exército, que, com reivindicações ilegais, atentaram contra o Estado Democrático de Direito e desempenharam papel crucial nos eventos de invasão e na depredação dos edifícios-sedes dos Poderes da República, ocorridos no 08 de janeiro de 2023"*.

Consta da representação da Polícia Federal (fls. 3-29):

"No dia 08 de janeiro de 2023, grupos de manifestantes, atuando contra a ordem democrática invadiram e depredaram as sedes dos três Poderes da República, em Brasília/DF. Vários ônibus transportaram os grupos bolsonaristas até a frente do Quartel General do Exército.

Nesse contexto, em conformidade com o extraído da IPJ Nº 202/2023, produzida por ocasião da análise do afastamento do sigilo dos dados bancários de MARLUCIA RAMIRO (CPF: 063.942.408-26), investigada no âmbito dos atos antidemocráticos como integrante do núcleo "financiador/organizador", identificou-se uma série de transferências bancárias suspeitadas, indicando que RAFAEL MORENO SOUZA SANTOS (359.972.878-07) foi um dos arrecadadores de valores do ato antidemocrático de 08/01/2023, sendo relevante dizer que RAFAEL disponibilizou uma chave

PET 12227 / DF

PIX a fim de arrecadar dinheiro - tal fato foi exposto pelos veículos da mídia, <https://www.metropoles.com/colunas/guilherme-amado/arrecadador-de-ato-terrorista-jafoi-alvo-de-alexandre-de-moraes>.

Nessa mesma reportagem, no dia 08/01/23 RAFAEL teria divulgado vídeos enquanto participava de protesto em São Paulo. No ato, ao comemorar a invasão ao Congresso, RAFAEL teria solicitado doações para seu próprio PIX para auxiliar nas caravanas e alimentação dos patriotas em Brasília.

Conforme noticiado, RAFAEL MORENO SOUZA SANTOS esteve em São Paulo, no dia 08/01/23 estava em um protesto em São Paulo comemorando os atos de depredação em Brasília, proferindo, em vídeo, o seguinte: "Invadiram o Congresso, pessoal! Tomamos o Brasil de volta, pessoal! Agora é tudo nosso, tudo dominado!", gritava, em meio a faixas pedindo um golpe militar.

(...)

RAFAEL MORENO também foi investigado no inquérito Nº 4.781 STFDF, tendo sido alvo de medida de busca e apreensão nesse inquérito das Fake News, além de ter tido perfis bloqueados nas redes sociais Twitter e Facebook. Atualmente, Rafael Moreno administra ao menos dois perfis distintos no Instagram (@rafaelmorenoss e @roboconservador), de acordo com as imagens expostas (extraídas em 09 de fevereiro de 2024) a seguir:

(...)

Procedeu-se a análise do conteúdo das redes sociais em conjunto com o cruzamento de dados financeiros do investigado RAFAEL MORENO SOUZA SANTOS (CPF 359.972.878-07), conforme consta na Informação de Polícia Judiciária nº 36/2024.

Identificou-se, além dos perfis no Instagram, a página utilizada por RAFAEL MORENO SOUZA SANTOS na rede social Facebook.

(...)

Em ambas as redes sociais, Instagram e Facebook, os

PET 12227 / DF

perfis do investigado são abertos, em que RAFAEL se demonstra bastante ativo, realizando publicações, algumas recentes, como vídeos discursando em manifestações, publicações em favor do impeachment do ministro Alexandre de Moraes entre outras manifestações políticas contra o atual governo federal e contra as investigações referentes aos atentados de 08/01/2023.

Pesquisas em redes sociais permitiram encontrar outros dois perfis do usuário RAFAEL MORENO: @RafaelMorenoSS2 e @Monarquista, conforme denúncia do usuário do perfil denominado "PASTOR MALA" (@Prmalaoficial), de acordo imagem a seguir:

(...)

Nas análises dos referidos perfis (@RafaelMorenoSS, RafaelMorenoSS2 e @_Monarquista) observou-se que somente os perfis @RafaelMorenoSS e @Rafae1MorenoSS2 estavam identificados com nome e foto do referido denunciado RAFAEL MORENO, conforme imagem abaixo:

(...)

Sobre o financiamento dos atos antidemocráticos, há postagens no perfil @Rafae1MorenoSS2 que indicam movimentação para arrecadação de doações via PIX para alimentação e transporte de pessoas em Brasília, conforme imagem abaixo.

Ressalta-se que foram encontrados perfis de RAFAEL MORENO nas principais redes sociais: Instagram (106. mil seguidores), X (42 mil seguidores - PERFIL @RafaelMorenoSS e 4.196 seguidores - PERFIL @Rafae1MorenoSS2), Threads (13,4 mil seguidores), Facebook (4 mil seguidores - PERFIL rafaelmorenoss e 11 mil seguidores - PERFIL rafamorenoss).

(...)

Já na rede social Facebook, em postagem mais recente, por exemplo, RAFAEL faz postagem sobre suposto abuso de autoridade que a Polícia Federal teria praticado durante cumprimento de mandado de busca contra o Deputado Federal CARLOS JORDY.

PET 12227 / DF

(...)

Foi possível constatar que, no dia 01/11/2022, RAFAEL esteve em manifestação contra o resultado das eleições e convocou pessoas para comparecerem à rua. Já em publicação de 30/12/2022, chama as Forças Armadas de "Frouxas Armadas". Antes das eleições de 2022 fez publicações que demonstram radicalismo político, como texto em que diz que a disputa política entre Jair Bolsonaro e Lula seria uma guerra do bem contra o mal.

(...)

Prosseguindo com as pesquisas, apurou-se que, em pesquisas em fontes abertas, matérias jornalísticas indicam que à época dos atos antidemocráticos, RAFAEL MORENO teria arrecadado valores para auxiliar no financiamento de acampamentos em frente aos quartéis e caravanas de ônibus à Brasília. Entretanto, não foram mais encontradas as publicações em que RAFAEL solicita valores.

(...)

Segundo reportagem do dia 29/12/2022 (<https://globo.globo.com/politica/noticia/2022/12/a-tres-dias-da-posse-bo-lsonaristaseguem-fnanciando-atos-com-vaquinhas-rifas-e-premios-de-r-10-mil.html>), RAFAEL teria arrecado pelo menos 67 mil reais. De acordo com a matéria, RAFAEL afirma que o dinheiro arrecadado estaria sendo utilizado exclusivamente para alimentar manifestantes em Brasília e contribuir no custeio de algumas caravanas para lá.

Ainda de acordo com fontes abertas (<https://blogdobarroto.com.br/morador-de-natal-se-gaba-de-financiar-atos-golpistas-e-escapar-do-stf/>), RAFAEL MORENO manteve um financiamento coletivo para um protesto na posse de Lula (PT). O publicitário foi um dos citados no relatório final da CPMI dos atos golpistas, apresentado em outubro de 2023 pela senadora Eliziane Gama (PSD-MA). Segundo trechos do relatório, "Entre as fontes financeiras, destaca-se a vaquinha virtual mantida pelo publicitário Rafael Moreno de Souza Santos, que chegou a arrecadar mais de R\$ 60 mil reais por

PET 12227 / DF

meio de um site de financiamento coletivo", ratificou a senadora.

O publicitário não foi incluído na lista de pedidos de indiciamento da CPMI, mas a relatora indicou que era "necessário um maior aprofundamento das investigações em relação a Rafael Moreno de Souza Santos" e outros nomes.

A reportagem menciona que RAFAEL MORENO possui um apartamento em um condomínio no bairro Pajuçara, zona norte de Natal. No grupo de moradores no Whatsapp, ele se gaba de "fugir" do STF. Além disso, ele e a noiva passaram a defender pautas de extrema-direita após o protesto que interditou o trânsito na Ponte Newton Navarro em 13/11/2023.

(...)

No que se refere aos dados efetivamente levantados até o momento na investigação, foram localizadas movimentações bancárias de RAFAEL MORENO com outros investigados por envolvimento no financiamento dos atos antidemocráticos, que

reforçam as notícias de que RAFAEL MORENO também teria atuado de forma significativa com o financiamento dos atos que levaram aos ataques do dia 08/01/2023 em Brasília.

De acordo com a IPJ 202/2023, referente à análise bancária de MARLÚCIA RAMIRO, CPF 063.942.408-26, apontada como uma das organizadoras de caravanas de ônibus à Brasília, RAFAEL MORENO SOUZA SANTOS, CPF 359.972.878-07, entre 12/11/2022 e 30/12/2022, transferiu para MARLÚCIA um total de R\$ 4.610,00 em cinco transações bancárias.

Conforme o caso SIMBA - 002-PF008300-90, referente ao IPL 2023.0003935 - CINQ/CGRC/DICOR/PF (INQ 4920), que abrange o sigilo bancário do investigado JORGE ANTHONNY CHEDIK REZENDE FILHO (CPF 037.315.121-73), entre 05/11/2022 e 04/01/2023, foram identificadas oito transferências bancárias, no total de R\$ 22.443,43 - na forma apresentada pela tabela 1 - de RAFAEL MORENO SOUZA SANTOS para JORGE, outro envolvido no financiamento das ações que levaram aos atentados do dia 08/01/2023.

Ressalta-se que não foram localizadas outras razões

PET 12227 / DF

aparentes que justificassem as transferências de um total de mais de vinte cinco mil reais das contas de RAFAEL MORENO para os dois envolvidos apontados diretamente nos financiamentos de caravanas e acampamentos em frente ao QG do Exército.

(...)

Realizado o afastamento do sigilo bancário de MARLUCIA RAMIRO consoante o caso SIMBA 002-PF-008298-31 (RE 2023.0012028 e PET 11.022/DF), confeccionou-se a Informação de Polícia Judiciária nº 202/2023, na qual foi possível constatar diversas transações bancárias entre MARLUCIA RAMIRO e RAFAEL MORENO SOUZA SANTOS, conforme tabela 2 sinóptica a seguir.

(...)

Em 12/11/22, MARLUCIA RAMIRO recebe R\$1.800,00 de RAFAEL MORENO SOUZA SANTOS (359.972.878-07), o que pode indicar que RAFAEL angariou valores e depois os repassou para MARLUCIA RAMIRO, tendo em vista que RAFAEL disponibilizou uma chave PIX a fim de arrecadar dinheiro - tal fato foi exposto pelos veículos da mídia: <https://www.metropoles.com/colunas/guilhermeamado/arrecadador-de-ato-terrorista-ja-foi-alvo-de-alexandre-de-moraes>.

Portanto, ao considerar o período e diante da possibilidade de arrecadação de recursos via PIX, infere-se que RAFAEL tenha repassado parte dos valores arrecadados, por ele via PIX, para MARLUCIA, provavelmente destinando os valores ao financiamento indireto do transporte de manifestantes, tanto nas manifestações que ocorreram no mês de novembro/2022 quanto nos atos de vandalismo do dia 08/01/23.

Já em 23/11/22 e 24/11/22, RAFAEL envia R\$ 500,00 para MARLUCIA, que, por sua vez, repassa o valor para MARCOS PAULO BOLOTE (294.504.658-00). MARCOS, assim como MARLUCIA, possui endereço registrado na cidade de GUARULHOS/SP. Em uma pesquisa de mercado, junto a empresas de venda de passagens de ônibus, verificou-se que

PET 12227 / DF

uma passagem de GUARULHOS/SP a BRASÍLIA/DF está na média de R\$ 500,00. Assim, o contexto a que se refere, além do numerário remetido a MARCOS sugerem a sua utilização para compra de um bilhete de ônibus. Ainda, apurou-se que MARCOS é analista de sistemas e já foi proprietário de três empresas, uma de representação comercial, outra de comércio varejista de bebidas, e a terceira de atividades em teletendimento. Também há uma arma registrada em seu nome, uma TAURUS PT92 de calibre 9mm.

Mais adiante, em 03/12/22, cumpre destacar que RAFAEL realiza mais uma transferência para MARLUCIA, desta vez, no valor de R\$ 350,00. Logo em seguida, a investigada repassa R\$ 349,00 para JORGE ANTHONNY CHEDIK REZENDE FILHO (037.315.121-73), advogado que supostamente angariou recursos para o financiamento de tendas e alimentos no QGEx em Brasília/DF2 (RE 2023.0003098 - PET 10.872/DF) <<https://www.metropoles.com/brasil;advogado-de-bolsonarista-queplanejou-atentado-e-reu-por-organizacao-criminosa>>. Ressalte-se que, em 03/02/2023, a Polícia Federal realizou o cumprimento da ordem judicial de busca e apreensão, na residência de JORGE, porém o investigado não foi localizado e nada foi arrecadado naquela ocasião.

Importante consignar que MARLUCIA é investigada no âmbito do RE 2023.0012028 e PET 11.022/DF por supostamente ser organizadora das caravanas com destino a Brasília, além de possuir à época dos fatos empresa de nome fantasia "PÁTRIA AMADA", portadora do CNPJ 37.627.574/0001-02, cujo objeto social é transporte rodoviário coletivo de passageiros, sob regime de fretamento, com as atividades encerradas - sem motivo aparente - em 28/01/2023, logo após os atos antidemocráticos de 08 de janeiro de 2023.

Em face ao exposto, através do cruzamento de dados existentes e da análise das movimentações bancárias, das redes sociais e outras fontes abertas foi possível concluir que há indícios contundentes de que RAFAEL MORENO SOUZA SILVA (CPF 359.972.878-07) contribuiu com o financiamento de

PET 12227 / DF

atos que resultaram nos atentados do dia 08/01 /2023:

Entre os meses de novembro/2022 ao início de janeiro/2023, RAFAEL MORENO transferiu valores para dois investigados de financiamento dos atentados, aparentemente sem outras justificativas:

Para MARLÚCIA RAMIRO, CPF 063.942.408-26, transferiu R\$ 4.610,00 em cinco transações;

Para JORGE ANTHONNY CHEDIAK REZENDE FILHO, CPF 037.315.121-73, transferiu R\$ 22.443,43 em oito transações.

Matérias jornalísticas apontam que na época dos fatos, RAFAEL MORENO estaria angariando recursos para auxiliar no financiamento das caravanas de ônibus para Brasília e na manutenção de acampamentos em frente aos quartéis;

RAFAEL MORENO SOUZA SILVA, que se autointitula criador de conteúdo digital e conta com perfil de mais de cem mil seguidores no seu Instagram, demonstra-se ativo politicamente, participando de manifestações, onde fala em palanques, faz severas críticas ao atual governo e a membros do Judiciário, entre outras manifestações com teor nitidamente político. Esse fato, somado aos demais elementos de informação, corrobora com a hipótese de que RAFAEL tenha angariado recursos para financiar os atos que levaram ao dia 08/01/2023.

A Procuradoria-Geral da República encampou integralmente as medidas requeridas pela autoridade policial (fls. 72-79).

É o relatório. DECIDO.

I - CONSIDERAÇÕES INICIAIS

Nos termos relatados, as condutas do investigado noticiadas pela Polícia Federal ocorreram no curso dos atos antidemocráticos, nos quais grupos financiados por empresários insatisfeitos com o legítimo resultado do pleito, com violência e grave ameaça às pessoas, passaram a bloquear o tráfego em diversas rodovias do país, com o intuito de abolirem o

PET 12227 / DF

Estado Democrático de Direito, pleiteando um golpe militar e o retorno da Ditadura.

No caso específico de **RAFAEL MORENO SOUZA SANTOS**, suas condutas ocorreram no contexto dos atos ocorridos na Esplanada dos Ministérios em 8/1/2023, com destruição dos prédios do CONGRESSO NACIONAL, do PALÁCIO DO PLANALTO e, com muito mais raiva e ódio, do SUPREMO TRIBUNAL FEDERAL, fatos amplamente investigados em diversos procedimentos que tramitam nesta SUPREMA CORTE.

Segundo a autoridade policial, apura-se uma intricada rede, espalhada geograficamente por todo o país, que aparentemente operou com um modelo de financiamento coletivo, por meio de contribuições realizadas através de transferências PIX e concentradas em contas pertencentes a pessoas físicas e jurídicas encarregadas de adquirir suprimentos, alugar tendas e outros itens utilizados no dia a dia dos acampamentos golpistas.

A análise, conforme a IPJ 202/2023, revelou as movimentações bancárias dos envolvidos, financiadores das estruturas instaladas e mantidas em frente ao Quartel General do Exército. **RAFAEL MORENO SOUZA SANTOS** teria recebido diversas transferências suspeitas, indicando que foi um dos arrecadadores do ato antidemocrático de 8/1/2023.

Também constatou-se que **RAFAEL MORENO SOUZA SANTOS**, no dia 8/1/2023, ao comemorar a invasão do CONGRESSO NACIONAL, teria solicitado doações para seu PIX a fim de auxiliar nas caravanas e alimentação dos "patriotas" em Brasília/DF.

Relembro que na referida data de 8/1/2023 proferi decisões determinando as seguintes medidas, referendadas pelo Plenário do SUPREMO TRIBUNAL FEDERAL:

"I. Imposição de medida cautelar diversa da prisão, consistente na suspensão do exercício da função pública (art. 319, VI, do Código de Processo Penal) afastando **IBANEIS ROCHA** do cargo de Governador do Distrito Federal pelo prazo

PET 12227 / DF

inicial de 90 (noventa) dias;

II. Desocupação e dissolução total, em 24 (vinte e quatro) horas, dos acampamentos realizados nas imediações dos Quartéis Gerais e outras unidades militares para a prática de atos antidemocráticos e prisão em flagrante de seus participantes;

III. Apreensão e bloqueio de todos os ônibus identificados pela Polícia Federal, que trouxeram os terroristas para o Distrito Federal;

IV. Proibição imediata, até o dia 31 de janeiro, de ingresso de quaisquer ônibus e caminhões com manifestantes no Distrito Federal;

V. Adoção de providências pela Polícia Federal, TRIBUNAL SUPERIOR ELEITORAL e ANTT para identificação dos participantes dos atos investigados; e

VI. Expedição de ofício às empresas responsáveis pela administração de mídias sociais para o bloqueio de perfis que instigam e divulgam os atos investigados, com fornecimento dos dados cadastrais a esta SUPREMA CORTE e integral preservação de seu conteúdo.

VII. DECRETAÇÃO DA PRISÃO PREVENTIVA, com fundamento no art. 312 do Código de Processo Penal, de ANDERSON GUSTAVO TORRES e de FÁBIO AUGUSTO VIEIRA.

VIII. DETERMINAÇÃO DA REALIZAÇÃO DE BUSCA E APREENSÃO em todos os endereços indicados pela Polícia Federal ANDERSON GUSTAVO TORRES e de FÁBIO AUGUSTO VIEIRA."

Naquela ocasião, destaquei que os responsáveis pelos desprezíveis ataques terroristas à Democracia e às Instituições Republicanas serão responsabilizados, assim como os financiadores, instigadores e os anteriores e atuais agentes públicos coniventes e criminosos, que continuam na ilícita conduta da prática de atos antidemocráticos.

Os fatos narrados demonstram uma possível organização criminosa que tem por um de seus fins desestabilizar as instituições republicanas,

PET 12227 / DF

principalmente aquelas que possam contrapor-se de forma constitucionalmente prevista a atos ilegais ou inconstitucionais, como o CONGRESSO NACIONAL e o SUPREMO TRIBUNAL FEDERAL, utilizando-se de uma rede virtual de apoiadores que atuam, de forma sistemática, para criar ou compartilhar mensagens que tenham por mote final a derrubada da estrutura democrática e do Estado de Direito no Brasil.

Essa organização criminosa, ostensivamente, atenta contra a Democracia e o Estado de Direito, especificamente contra o Poder Judiciário e em especial contra o SUPREMO TRIBUNAL FEDERAL, pleiteando a cassação de seus membros e o próprio fechamento da Corte Máxima do País, com o retorno da Ditadura e o afastamento da fiel observância da Constituição Federal da República.

A Democracia brasileira não irá mais suportar a ignóbil política de apaziguamento, cujo fracasso foi amplamente demonstrado na tentativa de acordo do então primeiro-ministro inglês Neville Chamberlain com Adolf Hitler.

Absolutamente **TODOS** serão responsabilizados civil, política e criminalmente pelos atos atentatórios à Democracia, ao Estado de Direito e às Instituições, inclusive pela dolosa conivência por ação ou omissão motivada pela ideologia, dinheiro, fraqueza, covardia, ignorância, má-fé ou mau-caratismo.

A Democracia brasileira não será abalada, muito menos destruída, por criminosos terroristas. A defesa da Democracia e das Instituições é inegociável, pois como ainda lembrado pelo grande primeiro-ministro inglês, *construir pode ser a tarefa lenta e difícil de anos. Destruir pode ser o ato impulsivo de um único dia.*

II- BUSCA E APREENSÃO DOMICILIAR E PESSOAL

A inviolabilidade domiciliar constitui uma das mais antigas e importantes garantias individuais de uma Sociedade civilizada, pois engloba a tutela da intimidade, da vida privada, da honra, bem como a

PET 12227 / DF

proteção individual e familiar do sossego e tranquilidade, inclusive do local onde se exerce a profissão ou a atividade, desde que constitua ambiente fechado ou de acesso restrito ao público (HC nº 82.788/RJ, 2ª T, Rel. Min. CELSO DE MELLO). Esse fundamental direito, porém, não se reveste de caráter absoluto (RHC 117159, 1ª T, Rel. Min. LUIZ FUX) e não deve ser transformado em garantia de impunidade de crimes, que, eventualmente, em seu interior se pratiquem ou que possibilitem o armazenamento de dados probatórios necessários para a investigação (RT 74/88, 84/302); podendo ser, excepcionalmente, afastado durante a persecução penal do Estado, desde que presentes as hipóteses constitucionais e os requisitos legais (RE 603.616/RO, Repercussão Geral, Pleno, Rel. Min. GILMAR MENDES; HC 93.050-6/RJ, 2ª T, Rel. Min. CELSO DE MELLO; HC 97567, 2ª T, Rel. Min. ELLEN GRACIE).

Na espécie, estão presentes os requisitos do art. 240 do Código de Processo Penal, necessários ao deferimento de ordem judicial de busca e apreensão em seu endereço residencial, pois devidamente motivada em fundadas razões que, alicerçadas em indícios de autoria e materialidade criminosas, sinalizam a necessidade da medida para colher elementos de prova relacionados à prática de infrações penais em relação ao investigado.

Nesse sentido, se manifestou a Procuradoria-Geral da República (fls. 75-76):

“A digna autoridade policial justifica adequadamente a busca e apreensão domiciliar e pessoal contra o requerido, financiador da viagem e alimentação de indivíduos que praticaram os atos de vandalismo e de depredação em prédios públicos no dia 8.1.2023, com vistas a elucidar os responsáveis pelo financiamento dos atos criminosos investigados, mediante a captura do celular, computadores e mídias de armazenamento que podem auxiliar na identificar dos demais envolvidos e da forma de obtenção de recursos para o cometimento dos ilícitos investigados”.

PET 12227 / DF

Efetivamente, a solicitação está circunscrita à pessoa física vinculada aos fatos investigados, e os locais das busca serão devidamente indicados, limitando-se aos endereços pertinentes.

Nesse cenário, tenho por atendidos os pressupostos necessários ao afastamento da garantia constitucional da inviolabilidade do domicílio, bem como em relação a busca pessoal, encontrando-se justificada a ação invasiva na procura de outras provas das condutas ora postas sob suspeita.

III - BLOQUEIO DAS CONTAS BANCÁRIAS, ATIVOS FINANCEIROS E SEQUESTRO DE BENS

Em face das circunstâncias delineadas, é imprescindível a realização de diligências, inclusive com o afastamento excepcional de garantias individuais que não podem ser utilizadas como um verdadeiro escudo protetivo para a prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito (HC nº 70.814-5/SP, Rel. Min. CELSO DE MELLO, Primeira Turma, DJ de 24/6/1994).

A autoridade policial ressaltou que:

“O processo penal brasileiro admite o sequestro e bloqueio de bens móveis e imóveis dos investigados bastando, para isso, a existência de indícios de cometimento de ilícito e ainda, pondera-se que tais medidas, podem, indiretamente, assegurar a aplicação da lei penal.

O Relatório de danos ao patrimônio do Senado Federal conforme Nota Técnica nº 01/2023 – ATDGER aponta o montante estimado de R\$ 3.500.000,00 por levantamento realizado pelas áreas técnicas deste Senado Federal até o dia 09/01/2023.

Documento encaminhado por meio do Processo nº 221.490/2023 da DIRETORIA ADMINISTRATIVA da Câmara dos Deputados aponta o montante de R\$ 3.556.509,14 a título de

PET 12227 / DF

prejuízo causado a CÂMARA DOS DEPUTADOS.

O Ofício nº 023/GDG/2023 encaminhado pela Presidência do Supremo Tribunal Federal aponta o montante estimado em R\$ 11.413.654,84 por levantamento realizado pelas áreas técnicas do Senado Federal até o dia 09/01/2023. (...).

Verifica-se que no presente caso, conforme largamente explicado, há elementos robustos indicativos de que os investigados atuaram, ainda que indiretamente, a viabilizar os atos ocorridos em 08/01/2023.

O bloqueio/sequestro de valores deve ser adotado enquanto a investigação ainda está em sua fase sigilosa, considerando o grande risco de, uma vez tendo conhecimento da quantificação formulada neste procedimento, os investigados ocultarem seus recursos, visando assim evitar medidas constritivas em detrimento dos mesmos."

A medida também foi defendida pela Procuradoria-Geral da República (fl. 77):

"Vê-se, portanto, que o sequestro especial de bens do Decreto-Lei n. 3.240/1941, diferentemente do sequestro do Código de Processo Penal, não se presta à constrição apenas dos instrumentos, produtos ou do proveito dos crimes (art. 91, II, do Código Penal), mas também do patrimônio lícito, visando a possibilitar o ressarcimento do dano, como efeito da condenação (art. 91, inciso I, Código Penal). Tem-se um tratamento mais rigoroso para os autores de crimes que importam dano à Fazenda Pública, como forma de tutelar, de modo mais efetivo, o patrimônio público e, assim, o interesse da coletividade atingida por tais práticas delituosas.

No caso do representado, os elementos revelam fortes indícios da prática de crimes, sendo apontado como financiador e incitador de manifestações ilícitas, que antecederam e que conduziram à verificação dos eventos do dia 8.1.2023, com a invasão e a depredação dos edifícios sedes dos Poderes da República, com graves repercussões patrimoniais.

PET 12227 / DF

A autoridade policial indica documentos enviados por órgãos das sedes dos Poderes da República atacadas, a respeito dos prejuízos já apurados, em decorrência dos atos antidemocráticos, que contaram com o envolvimento dos representados.

Serão gastos milhões de reais para a reformados prédios, justificando que o bloqueio cautelar das contas bancárias e demais ativos financeiros do representado incida, pelo menos, até o valor indicado pela Polícia Federal, cobrindo também parte do dano moral e imaterial."

Assim, torna-se necessário, adequado e urgente o bloqueio das contas bancárias e demais ativos financeiros do investigado, diante da possibilidade de utilização de recursos para o financiamento de atos ilícitos e antidemocráticos, com objetivo de interromper a lesão ou ameaça a direito (art. 5º, XXXV, Constituição Federal), conforme anteriormente ressaltado.

IV - AFASTAMENTO DO SIGILO BANCÁRIO

Na visão ocidental de Democracia, governo pelo povo e a limitação no exercício do poder estão indissolavelmente combinados, sendo imprescindível a observância dos direitos e garantias individuais constitucionalmente consagrados, uma vez que, enquanto comandos proibitórios expressos direcionados ao Estado tem por primordial finalidade o afastamento de indevida ingerência estatal no âmbito da esfera jurídica individual, impedindo o ferimento da dignidade humana, vida, liberdade, propriedade e intimidade (MANOEL GONÇALVES FERREIRA FILHO, *Estado de direito e constituição*. São Paulo: Saraiva, 1988. p. 16 ss; JOSÉ ALFREDO OLIVEIRA BARACHO. *Teoria da Constituição*. *Revista de Informação Legislativa*. ano 15. n. 58. abr/jun. 1978; J. J. GOMES CANOTILHO, J. J. *Direito constitucional*. Coimbra: Almedina, 1993. p. 541 ss; PAOLO BARILE. *Diritti dell'uomo e libertà fondamentali*. Bolonha: II Molino. p. 13 ss).

PET 12227 / DF

A real efetividade dos direitos e garantias individuais é imprescindível para a preservação do Estado de Direito (RAFAEL BIELSA. *Estudios de Derecho Público Derecho Constitucional*. Tomo III. Buenos Aires: Arayú, 345), pois, conforme a sempre atual advertência de MADISON:

num governo livre, é preciso dar aos direitos civis a mesma garantia que aos direitos religiosos (Federalist papers, LI)

O art. 5º, incisos X e XII da Constituição Federal, consagrou a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; estendendo essa proteção constitucional aos sigilos de dados, inclusive o bancário, fiscal e telemático.

Nesse contexto, em regra, não podemos deixar de considerar que as informações bancárias, sejam as constantes nas próprias instituições financeiras, sejam as constantes na Receita Federal ou organismos congêneres do Poder Público, constituem parte da intimidade e vida privada da pessoa física ou jurídica. Não há dúvida, portanto, de que o desrespeito ao sigilo bancário constitucionalmente protegido, em princípio, acarretaria violação de garantias constitucionais (CELSO BASTOS. *Estudos e pareceres de direito público*. São Paulo: Revista dos Tribunais, 1993. p. 63 ss. VITAL RAMOS VASCONCELOS. Proteção constitucional ao sigilo. *Revista FMU-Direito*, nº6, p. 17 ss.).

A proclamação dos direitos individuais, entretanto, nasceu para reduzir a ação do Estado aos limites impostos pela Constituição, sem, contudo desconhecer a obrigatoriedade das condutas individuais operarem dentro dos limites impostos pelo direito, conforme salientado por QUIROGA LAVIÉ (*Derecho constitucional*. Buenos Aires: Depalma, 1993. p. 123 ss).

Os direitos e garantias individuais, conseqüentemente, não são absolutos e ilimitados, uma vez que encontram seus limites nos demais direitos igualmente consagrados pela Carta Magna (*Princípio da relatividade ou convivência das liberdades públicas*) e, quando houver conflito entre dois ou mais direitos ou garantias fundamentais, o intérprete deve

PET 12227 / DF

utilizar-se do *princípio da concordância prática ou da harmonização*, de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros, realizando uma redução proporcional do âmbito de alcance de cada qual (*contradição dos princípios*), sempre em busca do verdadeiro significado da norma e da harmonia do texto constitucional com sua finalidade precípua.

A própria Declaração dos Direitos Humanos das Nações Unidas, expressamente, em seu art. 29 afirma tanto a finalidade, quanto a relatividade dos direitos individuais:

toda pessoa tem deveres com a comunidade, posto que somente nela pode-se desenvolver livre e plenamente sua personalidade. No exercício de seus direitos e no desfrute de suas liberdades todas as pessoas estarão sujeitas às limitações estabelecidas pela lei com a única finalidade de assegurar o respeito dos direitos e liberdades dos demais, e de satisfazer as justas exigências da moral, da ordem pública e do bem-estar de uma sociedade democrática. Estes direitos e liberdades não podem, em nenhum caso, serem exercidos em oposição com os propósitos e princípios das Nações Unidas. Nada na presente Declaração poderá ser interpretado no sentido de conferir direito algum ao Estado, a um grupo ou uma pessoa, para empreender e desenvolver atividades ou realizar atos tendentes a supressão de qualquer dos direitos e liberdades proclamados nessa Declaração.

Os direitos e garantias individuais, portanto, não podem ser utilizados como um verdadeiro escudo protetivo da prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito (HC nº 70.814-5/SP, Rel. Min. CELSO DE MELLO, Primeira Turma, DJ, 24-6-1994), pois como ensinado por DUGUIT:

a norma de direito, por um lado, impõe a todos o respeito aos direitos de cada um, e em contrapartida, determina

PET 12227 / DF

uma limitação sobre os direitos individuais, para assegurar a proteção aos direitos gerais (*Fundamentos do direito*. São Paulo: Ícone Editora, 1996, p. 11 ss).

O afastamento da inviolabilidade do sigilo bancário só poderá ser decretado, nos termos da LC 105/01 e sempre em caráter de absoluta excepcionalidade, quando existentes fundados elementos de suspeita que se apoiem em indícios idôneos, reveladores de possível autoria de prática delituosa por parte daquele que sofre a investigação e estiverem presentes os seguintes requisitos, como tive oportunidade de destacar em voto proferido no MS 25.940/DF (PLENÁRIO 26/4/2018):

- (a) autorização judicial;
- (b) indispensabilidade dos dados constantes em determinada instituição financeira, Receita Federal ou Fazendas Públicas;
- (c) individualização dos investigados e do objeto da investigação;
- (d) obrigatoriedade da manutenção do sigilo em relação às pessoas estranhas à causa;
- (e) utilização de dados obtidos somente para a investigação que lhe deu causa, salvo nova autorização judicial.

Quanto ao ponto, assim se manifestou a Procuradoria-Geral da República (fl. 78):

“A representação pede, ainda, o afastamento do sigilo bancário com calço na necessidade de identificar a origem e o destino dos recursos movimentados pelo investigado, bem como apurar a rede de financiamento dos atos criminosos que culminaram com o 8.1.2023, na forma preconizada pelo art. 1º, §4º, da Lei Complementar n. 105/2021.

A medida invasiva das contas de RAFAEL MORENO SOUZA SANTOS deve compreender o período de 30.10.2022 a 21.2.2024, com a finalidade de identificar a movimentação

PET 12227 / DF

financeira ordinária e a sua evolução no ápice do movimento criminoso em 8.1.2023, cujos atos podem ter se repetido após a deflagração do movimento antidemocrático, não se revelando proporcional ou justificável abarcar período anterior a 30.10.2022, quando o resultado das eleições ainda não era conhecido.”

Efetivamente, há necessidade de afastamento do sigilo dos dados bancários do representado, notadamente em razão de sua provável relação com o financiamento dos atos antidemocráticos ocorridos no dia 8/1/2023.

A necessidade de fiel observância aos requisitos constitucionais e legais é obrigatória para o afastamento da garantia constitucional (HC 93.050-6/RJ, Rel. Min. CELSO DE MELLO, Segunda Turma, julgado em 10-6-2008; HC 84758, Rel. Min. CELSO DE MELLO, Tribunal Pleno, DJ 16-06-2006; HC 85.088/ES, Rel. Min. ELLEN GRACIE, Segunda Turma, DJ 30-9-2005; AI 655298 AgR, Rel. Min. BROS GRAU, Segunda Turma, julgado em 04/09/2007; MS 25812 MC, Rel. Min. CEZAR PELUSO, DJ 23/02/2006 AI 541265 AgR, Rel. Min. CARLOS VELLOSO, Segunda Turma, julgado em 04/10/2005; Inq. 899-1/DF, Rel. Min. CELSO DE MELLO, DJ 23-9-1994; MS 21.729-4/DF, Rel. Min. Presidente SEPÚLVEDA PERTENCE, DJ 13-8-1993), pois, como bem salientado por MIRKINE-GUETZÉVITCH:

encontra-se aí a garantia essencial das liberdades individuais; sua limitação não é possível senão em virtude da lei (*As novas tendências do direito constitucional*. São Paulo: Campanha Editora Nacional, 1933. p. 77).

No caso dos autos, os requisitos se mostram plenamente atendidos, pois patente a necessidade de afastamento do sigilo bancário e fiscal para a investigação da organização criminosa responsável pelos atos terroristas ocorridos na Praça dos Três Poderes.

PET 12227 / DF

V – BLOQUEIO DE PERFIS EM REDES SOCIAIS

A Polícia Federal representou pelo bloqueio dos canais/perfis/contas de titularidade do representado em redes sociais, bem como a imposição da proibição do seu uso para divulgar mensagens de texto ou vídeo, a fim de propagar ideias antidemocráticas (f. 28).

Em face das circunstâncias delineadas, imprescindível a realização de diligências, inclusive com o afastamento excepcional de garantias individuais que não podem ser utilizadas como um verdadeiro escudo protetivo para a prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito (HC nº 70.814-5/SP, Rel. Min. CELSO DE MELLO, Primeira Turma, DJ de 24/6/1994).

Efetivamente, a Polícia Federal indicou que o investigado se utilizou das redes sociais exatamente com o fim de instigar, divulgar e financiar atos criminosos e golpistas (fls. 3 a 13).

A Procuradoria-Geral da República manifestou-se favoravelmente ao bloqueio dos perfis e contas do investigado em redes sociais (fls. 77-78).

Assim, se torna necessário, adequado e urgente o bloqueio dos perfis do investigado, diante da possibilidade de sua utilização para instigar atos ilícitos e antidemocráticos, bem como a adoção das demais medidas pleiteadas pelo *Parquet*, com objetivo de interromper a lesão ou ameaça a direito (art. 5º, XXXV, Constituição Federal), conforme anteriormente ressaltado.

VI – DISPOSITIVO

Diante de todo o exposto, com fundamento nos artigos 240 e seguintes do Código de Processo Penal **DETERMINO**:

(1) A **BUSCA E APREENSÃO DOMICILIAR** de armas, munições, computadores, *tablets*, celulares e outros dispositivos eletrônicos, bem como de quaisquer outros materiais

20

PET 12227 / DF

relacionados aos fatos aqui descritos, em poder de RAFAEL MORENO SOUZA SANTOS (CPF 359.972.878-07), nos endereços a serem apresentados pela autoridade policial.

AUTORIZO, desde logo, a adoção das seguintes medidas pela autoridade policial:

(1.1) Prosseguir nas medidas de busca e apreensão em endereços contíguos (para o que deve adotar todas as medidas necessárias a verificar a existência de eventuais cômodos secretos ou salas reservadas em quaisquer dos endereços diligenciados), bem assim determinação para que lhe franqueiem acesso, cópias ou apreensão dos registros de controle de ingresso nos endereços relacionados, caso existam;

(1.2) Medidas de busca e apreensão em veículos automotores eventualmente encontrados no endereço e nos armários de garagem, quando as circunstâncias fáticas indicarem que o(a) investigado(a) faz uso de tais veículos, ainda que não estejam registrados em seu nome;

(1.3) acesso e a análise do conteúdo (dados, arquivos eletrônicos, mensagens eletrônicas e e-mails) armazenado em eventuais computadores, servidores, redes, inclusive serviços digitais de armazenamento 'em nuvem', ou em dispositivos eletrônicos de qualquer natureza, por meio de quaisquer serviços utilizados, incluindo aparelhos de telefonia celular que forem encontrados, bem assim para a apreensão, se necessário for, dos dispositivos de bancos de dados, DVDs, CDs ou discos rígidos;

(1.4) acesso e a análise do conteúdo dos computadores e demais dispositivos no local das buscas e de arquivos eletrônicos apreendidos, mesmo relativo a comunicações eventualmente registradas, inclusive dados armazenados 'em nuvem', registrando-se e preservando-se o código 'hash' dos arquivos eletrônicos;

(1.5) arrolamento, a avaliação e a custódia, em ambiente seguro, do dinheiro em espécie e dos bens de

PET 12227 / DF

elevado valor econômico apreendidos.

Expeçam-se os mandados, dirigidos à Polícia Federal, nos termos do art. 243 do Código de Processo Penal.

(2) A BUSCA E APREENSÃO PESSOAL de RAFAEL MORENO SOUZA SANTOS (CPF 359.972.878-07), inclusive, para que, caso não se encontre no local da realização da busca, proceda-se à apreensão de armas, munições, objetos e dispositivos eletrônicos de que tenha a posse, bem como a busca em quartos de hotéis, motéis e outras hospedagens temporárias onde o investigado tenha se instalado, caso estejam ausente de sua residência.

AUTORIZO, desde logo, a adoção das seguintes medidas pela autoridade policial:

(2.1) busca pessoal e a apreensão de materiais em veículos automotores, caso o investigado esteja em deslocamento;

(2.2) realização de busca pessoal em desfavor de quaisquer pessoas sobre as quais, presentes no recinto no momento do cumprimento da ordem judicial, recaia suspeita de que estejam na posse de armas proibidas, objetos ou papéis que interessem à investigação (art. 240, § 2º, do Código de Processo Penal), bem como para o uso da força estritamente necessária para romper eventual obstáculo à execução dos mandados, inclusive o arrombamento de portas e cofres eventualmente existentes no endereço, caso o(a) investigado(a) não esteja no local ou se recuse a abri-los;

(2.3) autorização para o acesso e a análise do conteúdo (dados, arquivos eletrônicos, mensagens eletrônicas e e-mails) armazenado em eventuais computadores, servidores, redes, inclusive serviços digitais de armazenamento 'em nuvem', ou em dispositivos eletrônicos de qualquer natureza, por meio de quaisquer serviços utilizados, incluindo aparelhos de telefonia celular que forem encontrados, bem assim para a

PET 12227 / DF

apreensão, se necessário for, dos dispositivos de bancos de dados, DVDs, CDs ou discos rígidos;

(2.4) acesso e a análise do conteúdo dos computadores e demais dispositivos no local das buscas e de arquivos eletrônicos apreendidos, mesmo relativo a comunicações eventualmente registradas, inclusive dados armazenados 'em nuvem';

(2.5) arrolamento, a avaliação e a custódia, em ambiente seguro, do dinheiro em espécie e dos bens de elevado valor econômico apreendidos.

Expeça-se os mandados, dirigidos à Polícia Federal, nos termos do art. 243 do Código de Processo Penal.

(3) o **BLOQUEIO IMEDIATO** das contas bancárias/ativos financeiros de **RAFAEL MORENO SOUZA SANTOS** (CPF 359.972.878-07), mediante expedição de ofício ao BANCO CENTRAL DO BRASIL e a CVM (para que o bloqueio se operacionalize nesse caso por meio do sistema SOF-CEI), incluindo posição de custódia de ações, títulos privados, títulos públicos e derivativos, aplicações em fundos de investimento, VGBL, PGBL, aplicações em LCA e LCI, aplicações em CDB' s, RDB' s, COE, ouro e afins, previdência privada, cartas de consórcio e criptomoedas.

DEVERÃO AS INSTITUIÇÕES FINANCEIRAS INFORMAR SOBRE O EFETIVO BLOQUEIO.

(4) O **BLOQUEIO** de veículos automotores por meio do Sistema RENAJUD e o bloqueio de bens imóveis por meio da Central Nacional de Indisponibilidade de Bens (CNIB) em relação a **RAFAEL MORENO SOUZA SANTOS** (CPF 359.972.878-07), mediante expedição de ofício ao Conselho Nacional de Justiça.

(5) o **AFASTAMENTO DO SIGILO BANCÁRIO** de todos os bens, direitos e valores mantidos em instituições financeiras, no período de 30/10/2022 a 21/2/2024 (Caso nº 002-PF-008298-31

PET 12227 / DF

e e-mail: paulo.phbc@pf.gov.br), em nome de RAFAEL MORENO SOUZA SANTOS (CPF 359.972.878-07).

Expeça-se ofício, em caráter sigiloso, ao Banco Central do Brasil, para que:

1. Realize consulta através do SISBAJUD e se identifique as instituições financeiras nas quais as referidas pessoas físicas investigadas mantêm relacionamento como titulares, representantes ou procuradores, tais como contas de depósito à vista, de poupança, de investimento, de depósitos a prazo e outros bens, direitos e valores, diretamente ou por seus representantes legais, bem como em relações em conjunto com terceiros;

2. Consigne no SISBAJUD que o atendimento à determinação judicial deve ser realizado prioritariamente pelo sistema SIMBA, através do Caso nº 002-PF-008298-31;

3. Encaminhe o ofício judicial exclusivamente às instituições financeiras com as quais o investigado mantém ou manteve relacionamento durante o período de 30/10/2022 a 21/2/2024, conforme resultado da consulta ao CCS e faça constar na comunicação o Código Identificador do Caso nº 002-PF-008298-31 e e-mail: paulo.phbc@pf.gov.br, para ser utilizado para validação e transmissão dos dados;

4. Para o cumprimento da decisão judicial as instituições financeiras observem o disposto na Carta Circular nº 3454/2010, do Banco Central do Brasil, que divulga *leiante* para que as instituições financeiras prestem informações relativas a movimentação financeira, do investigado citado inclusive na qualidade de procurador, referente ao período de 30/10/2022 a 21/2/2024;

5. As instituições financeiras envolvidas encaminhem os dados bancários via rede mundial de computadores, utilizando-se dos programas VALIDADOR BANCÁRIO SIMBA e TRANSMISSOR BANCÁRIO SIMBA, disponibilizados no sítio <http://www.pf.gov.br/servicos-pg/sigilo-bancario>;

6. As instituições financeiras envolvidas encaminhem os dados bancários no prazo máximo de 30 dias a partir do

PET 12227 / DF

recebimento do comunicado da decisão judicial;

7. Se encaminhe ofício judicial ao Banco Central do Brasil, através do protocolo digital desta instituição, solicitando a transmissão do CCS do investigado ao Código Identificador do Caso nº 002-PF-008298-31, contendo o prazo para cumprimento da ordem judicial e a data do recebimento do ofício judicial pelas instituições financeiras visando o preenchimento dos campos obrigatórios para transmissão do CCS pelo validador do SIMBA;

8. Seja autorizado a autoridade policial e a peritos criminais designados para atuar no caso, requisitar diretamente às instituições financeiras, dados e documentos de suporte das operações financeiras realizadas no período do afastamento do sigilo, bem como aqueles relacionados a cadastros dos clientes e análises de crédito feito nas próprias instituições pela área de *compliance* ou de controle internos;

9. Sejam fornecidos pela instituição financeira documentos relacionados à abertura da conta, fita de caixa, cheques (microfilmagem ou documento digitalizado), contratos de abertura de conta, extrato de cartão de crédito e demais documentos físicos de interesse da investigação em poder da instituição financeira através do SISBAJUD ou outro meio de interesse; e

10. Que sejam fornecidos pelo Banco Central do Brasil, em meio eletrônico, planilha eletrônica e dados tabulados, todos os registros no SISTEMA CÂMBIO existentes de operações de câmbio do investigado, no período cujo sigilo foi afastado, contendo os dados lançados no SISTEMA CÂMBIO (Dados Contratação e Dados Liquidação), especialmente: A) CONTRATAÇÃO: 1. Data do Evento; 2 Data do Movimento; 3. Data Limite Liquidação; 5. Tipo Registro; 6. Tipo Registro; 7. Tipo Operação; 8. Tipo Contrato; 9. Natureza do Fato; 10. Natureza Grupo; 11. IF Proprietária; 12. IF Contratante; 13. Corretora; 14. Correspondente; 15. Cliente; 16. Número Contrato; 17. Moeda; 18 Forma de Entrega da Moeda; 19. Outras Especificações; 20. RDE; 21. Valor Contratado na Moeda

PET 12227 / DF

Estrangeira (ME); 22. Valor Contratado USD; 23. Valor Liquidado USD; 24. Valor Liquidado ME; 25. Prazo Liquidação em Dias; 26. Percentual Adiantamento; 27. Taxa Câmbio; B) LIQUIDAÇÃO: 1. Data Contratação; 2. Data da Liquidação; 3. Tipo Registro; 4. Compra/Venda; 5. Tipo do Contrato; 6. Natureza; 7. Grupo; IF Proprietária; 8. Corretora; 9. Correspondente; 10. Cliente; 11. Pagador/Recebedor Exterior; 12. País Pagador/Recebedor Exterior; 13. Número do Contrato; 14. Moeda; 15. Forma de Entrega da Moeda; 15. Outras Especificações; 16. RDE; 17. Outras Especificações; 18. Valor Liquidado US\$; 19. Valor Liquidado Moeda, e outros conforme extraído do DW, bem como outros registros de manutenção de recursos no exterior, relacionados ao investigado.

(6) a INTIMAÇÃO das empresas META INC. e X BRASIL, para que, no prazo de 2 (duas) horas, proceda ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

INSTAGRAM

<https://www.instagram.com/rafaelmorenoss>

<https://www.instagram.com/roboconservador>

THREADS

<https://www.threads.net/@rafaelmorenoss>

FACEBOOK

<https://www.facebook.com/rafaelorenoss>

<https://www.facebook.com/rafamorenoss>

TWITTER

<https://twitter.com/rafaelmorenoss>

Deverá a autoridade policial: (a) apresentar os endereços para o

PET 12227 / DF

cumprimento das medidas, (b) apresentar e gerar, quando da coleta e do armazenamento dos materiais em ambiente virtual, os códigos de verificação e de autenticação (códigos *hash*), com vistas à adequada manutenção da cadeia de custódia e à validade dos vestígios digitais; e (c) analisar o material e o conteúdo eletrônico apreendidos de forma prioritária, apresentando relatório parcial no prazo máximo de 30 (trinta) dias.

Expeça-se o necessário.

Os ofícios destinados ao Banco Central do Brasil, Conselho Nacional de Justiça e empresas provedoras de redes sociais deverão ser encaminhados somente após o cumprimento das medidas de busca pela autoridade policial.

Ciência à Procuradoria-Geral da República.

Cumpra-se.

Brasília, 1º de abril de 2024.

Ministro ALEXANDRE DE MORAES

Relator

Documento assinado digitalmente

Rumble Exhibits

Exhibit 2
Federal Supreme Court, Investigation
4.879 (Jan. 11, 2023)

Investigation 4.879 Federal District

Rapporteur : Justice Alexandre de Moraes
Plaintiff(s) : Confidential
Prosecutor(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential
Suspect(s) : Confidential
Attorney(s) : Confidential

Brasília, January 11, 2023.

To Companies
FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
RUMBLE
TELEGRAM
TIK TOK
TWITTER
YOUTUBE

Re: Investigation 4.879

Dear Officer,

I inform you that a decision was rendered on the confidential case record above for IMMEDIATE execution, as follows:

In view of the foregoing, I ORDER the issuance of official letters to companies FACEBOOK, RUMBLE, TELEGRAM, TIK TOK, TWITTER and YOUTUBE for them to proceed with the blocking of the channels/profiles/accounts detailed below within two (2) hours, on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), and provide their registration data to this SUPREME COURT and the full preservation of their contents: [add all indicated links:

FACEBOOK

<https://www.facebook.com/people/Patriotas/100068182532776/>
<https://www.facebook.com/nikolasferreiradm>
<https://www.facebook.com/search/top?q=jos%C3%A9%20medeiros>
<https://www.facebook.com/people/Barbara-Te-Atualizei/100086379919151/>
<https://www.facebook.com/alanrickm>

INSTAGRAM

@monarkoficial
@patriotasb
@nikolasferreiradm
@josemedeirosmt
@alanrickm
@ana_lucia_bagueira
@teatualizeioficial

RUMBLE

<https://rumble.com/Monark>

TELEGRAM

t.me/patriotasb
<https://t.me/nikolasferreira>
<https://t.me/monarktalks>
<https://t.me/monarkk>
<https://t.me/profepaulamarisa>

TIK TOK

<https://www.tiktok.com/@nikolasferreiradm>
<https://www.tiktok.com/@teatualizei22>
<https://www.tiktok.com/@monarktalks>

TWITTER

@monark
@JoseMedeirosMT
@PATRIOTAS
@nikolas_dm
@taoquei1
@profpaulamarisa
@Alan_Rick

YOUTUBE

<http://youtube.com/patriotasbr>
<https://www.youtube.com/nikolasferreira>
<https://www.youtube.com/teatualizei>
<https://www.youtube.com/eZPaulaMarisa/featured>
<https://www.youtube.com/@MonarkTalksCortesOficial>
<https://www.youtube.com/@alanriek3>

Given the confidential nature of this case record, the required arrangements for its maintenance shall be taken.

With nothing further, I take this opportunity to renew my assurances of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

Document digitally signed

[REDACTED]

INQUÉRITO 4.879 DISTRITO FEDERAL

RELATOR	: MIN. ALEXANDRE DE MORAES
AUTOR(A/S)(ES)	: SOB SIGILO
PROC.(A/S)(ES)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO
INVEST.(A/S)	: SOB SIGILO
ADV.(A/S)	: SOB SIGILO

Brasília, 11 de janeiro de 2023.

Às empresas
 FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
 RUMBLE
 TELEGRAM
 TIK TOK
 TWITTER
 YOUTUBE

Ref: Inquérito 4.879

INQ 4879 / DF

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante do exposto, DETERMINO a expedição de ofício às empresas FACEBOOK, RUMBLE, TELEGRAM, TIK TOK, TWITTER e YOUTUBE, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo: [acrescentar todos os links indicados:

FACEBOOK

<https://www.facebook.com/people/Patriotas/100068182532776/>

<https://www.facebook.com/nikolasferreiradm>

<https://www.facebook.com/search/top?q=jos%C3%A9%20medeiros>

<https://www.facebook.com/people/Barbara-Te-Atualizei/100086379919151/>

<https://www.facebook.com/alanrickm>

INSTAGRAM

@monarkoficial

@patriotasb

@nikolasferreiradm

@josemedeirosmt

@alanrickm

@ana_lucia_bagueira

@teatualizeioficial

RUMBLE

<https://rumble.com/Monark>

INQ 4879 / DF

TELEGRAM

t.me/patriotasb

<https://t.me/nikolasferreira>

<https://t.me/monarktalks>

<https://t.me/monarkk>

<https://t.me/profepaulamarisa>

TIK TOK

<https://www.tiktok.com/@nikolasferreiradm>

<https://www.tiktok.com/@teatualizei22>

https://www.tiktok.com/@monarktalks_

TWITTER

@monark

@JoseMedeirosMT

@PATRIOTAS

@nikolas_dm

@taoquei1

@profpaulamarisa

@Alan_Rick

YOUTUBE

<http://youtube.com/patriotasbr>

<https://www.youtube.com/nikolasferreira0>

<https://www.youtube.com/teatualizei>

<https://www.youtube.com/c/PaulaMarisa/featured>

<https://www.youtube.com/@MonarkTalksCortesOficial>

<https://www.youtube.com/@alanrick3>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

INQ 4879 / DF

Relator

Documento assinado digitalmente

Cópia destinada à Polícia Federal

Exhibit 3
Federal Supreme Court, Investigation
4.923 (June 14, 2023)

[Coat of arms of Brazil]
Federal Supreme Court

URGENT

Electronic Official Letter No. 8064/2023

Brasília, June 14, 2023.

To
RUMBLE Manager in Brazil

Investigation No. 4923

PLAINTIFF(S) : FEDERAL PROSECUTION OFFICE

PROSECUTOR(S) : FEDERAL PROSECUTOR

SUSPECT(S) : IBANEIS ROCHA BARROS JÚNIOR

ATTORNEY(S) :

SUSPECT(S) : ANDERSON GUSTAVO TORRES

ATTORNEY(S) :

SUSPECT(S) : FERNANDO DE SOUSA OLIVEIRA

ATTORNEY(S) :

SUSPECT(S) : FÁBIO AUGUSTO VIEIRA

ATTORNEY(S) :

POLICE : FEDERAL POLICE CHIEF

AUTHORITY

(Management of Original Criminal Proceedings)

Mr. Manager,

I am forwarding you the terms of the decision attached hereto as a copy so that you can take the necessary measures to comply with it and block BRUNO MONTEIRO AIUB's account **within two (2) hours**, under penalty of a daily fine of one hundred thousand reais (BRL 100,000.00), with the provision of its registration data to this SUPREME COURT and the full preservation of their content:

RUMBLE:

<https://rumble.com/c/Monarkx>

Kind regards,

Justice Alexandre de Moraes

Rapporteur

Document digitally signed

Investigation 4.923 Federal District

Rapporteur : **Justice Alexandre de Moraes**

Plaintiff(s) : FEDERAL PROSECUTION OFFICE

Prosecutor(s) : FEDERAL PROSECUTOR

Suspect(s) : IBANEIS ROCHA BARROS JÚNIOR

Attorney(s) : [REDACTED]

Suspect(s) : ANDERSON GUSTAVO TORRES

Attorney(s) : [REDACTED]

Suspect(s) : FERNANDO DE SOUSA OLIVEIRA

Attorney(s) : [REDACTED]

Suspect(s) : FÁBIO AUGUSTO VIEIRA

Attorney(s) : [REDACTED]

Police : FEDERAL POLICE CHIEF

Authority

Decision

In a decision rendered on this case record on 1/8/2023, in view of the violent escalation of the criminal acts which resulted in the invasion of the buildings of the PALÁCIO DO PLANALTO, the NATIONAL CONGRESS, the FEDERAL SUPREME COURT with plundering of public property, as widely reported by the national press, I determined, among other measures, the issuance of an official letter to companies Facebook, Tik Tok and Twitter, for them to proceed with the blocking within two (2) hours of the indicated channels/profiles/accounts, which instigated and publicized the criminal acts under investigation, under penalty of a daily fine of one hundred thousand reais (BRL 100,000.00), with the provision of their registration data to this SUPREME COURT and the full preservation of their content.

The Special Advice on Confronting Disinformation of the SUPERIOR ELECTORAL COURT informs that, through a survey on social media open data, detected a publication made by the influencer and podcaster “Monark” on the digital platform Rumble, containing an interview with the Member of the Brazilian House of

Representatives FILIPE BARROS (PL- PR), in the wake of which false news are spread about the integrity of electoral institutions (Official Letter AEED/GAB-SPR/GAB-PRES no. 2419/2023).

This is the brief report. DECISION.

As I emphasized when the decision was rendered on 1/8/2023, the despicable terrorist attacks on Democracy and Republican Institutions will be held accountable, as will the financiers, instigators, and the former and current conniving and criminal public officials who continue in the illicit conduct of committing anti-democratic actions. On 1/8/2023, as is widely known nationally and internationally, the violent escalation of criminal acts resulted in the invasion of the buildings of PALÁCIO DO PLANALTO, the NATIONAL CONGRESS and the FEDERAL SUPREME COURT, with plundering of public property.

The role of the instigators of the acts, especially on social media, is of no less relevant circumstance, making it clear that the aforementioned communication means are an essential part of the criminal enterprise that resulted in the appalling acts witnessed on 1/8/2023, and in the subsequent acts scheduled for the following days, subject to decisions in this case record and in ADPF 519.

In this context, I have repeatedly emphasized that the Federal Constitution enshrines the binomial “FREEDOM and LIABILITY”; not irresponsibly allowing abuse to be carried out in the exercise of a constitutionally enshrined right; not allowing the use of “freedom of expression” as a protective shield for the practice of hateful, anti-democratic speech, threats, aggression, criminal offenses and all sorts of unlawful activities.

Freedom of expression is not Freedom of aggression!

Freedom of expression is not Freedom to destroy Democracy, Institutions and the dignity and honor of others!

Freedom of expression is not Freedom to propagate lying, aggressive, hateful and prejudiced speech!

In view of the pointed out circumstances, it is essential to carry out due diligence, including the exceptional removal of individual guarantees that cannot be used as a real protective shield for the practice of illegal activities, nor as an argument for removing or diminishing civil or criminal liability for criminal acts, under penalty of disrespecting a true Rule of Law (HC No. 70.814-5/SP, Reporting Justice CELSO DE MELLO, First Panel, Court Gazette dated June 24, 1994).

Thus, as reported, the decision rendered on 1/8/2023 determined the blocking of several profiles/channels owned by BRUNO AIUB MONTEIRO, known as “Monark”, on the social networks Instagram (@monarkoficial), Rumble (<https://rumble.com/Monark>), Telegram (<https://t.me/monarktalks> and <https://t.me/monarkk>), Tik Tok (https://www.tiktok.com/@monarktalks_) Twitter (@monark) and Youtube (<https://www.youtube.com/@MonarkTalksCortesOficial>).

However, in a new channel created on the Rumble platform (<https://rumble.com/oMonarkx>), which already has 287 thousand followers, BRUNO MONTEIRO AIUB, as reported by AEED/TSE, started again to publish fraudulent news about the actions of this SUPREME COURT and the SUPERIOR ELECTORAL COURT, in the following terms:

“Monark says: 'And it's not the guy who's going there, fighting and putting in place... because, every time the Supreme Court makes a move like that, it spends its political capital. This takes a toll on it. [...] So, why is it (Supreme) willing to pay this cost? **Why is it (Supreme) willing to guarantee non-transparency in elections? We see the TSE censoring people, we see Alexandre de Moraes arresting people, you see a lot of things happening, and at the same time they are preventing the transparency of the ballot boxes? You become wary, what monkey business is happening at the ballot boxes there? Why? Why doesn't our political system want to let the Brazilian people have more certainty? What is the interest? Manipulate the ballot boxes? Manipulate the elections?** That's what I keep thinking...’.”

Furthermore, AEED/TSE point out to the creation of several other profiles, in complete disregard of the previously rendered decision:

Twitter: <https://twitter.com/MonarkVoltou> (16.2 thousand followers)

Instagram: <https://www.instagram.com/monark.talks/> (101 thousand followers)

Telegram: <https://t.me/monarktalks>

Discord: <https://discord.gg/8NKCauHf9>

Thus, it becomes necessary, appropriate and urgent to interrupt the possible spread of speeches with hateful content, subversion of order and encouragement of the breakdown of institutional and democratic normality by blocking social network accounts, to stop the harm or threat to right (article 5, XXXV, Federal Constitution), as previously highlighted.

In view of the foregoing, I ORDER the issuance of official letters to companies DISCORD, META INC., RUMBLE, TELEGRAM and TWITTER, for them to proceed with the blocking of the channels/profiles/accounts detailed below within two (2) hours, on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), and provide their registration data to this SUPREME COURT and the full preservation of their contents: [add all indicated links:

DISCORD

<https://discord.gg/8NKCauHf9>

META INC.

<https://www.instagram.com/monark.talks/>

RUMBLE

<https://rumble.com/c/Monarkx>

TELEGRAM

<https://t.me/monarktalks>

TWITTER

<https://twitter.com/MonarkVoltou>

I FURTHER ORDER THE IMPOSITION OF A PROVISIONAL MEASURE against BRUNO MONTEIRO AIUB, consisting of abstaining from publishing, promoting, replicating and sharing fraudulent news (fake news) subject of this decision, under penalty of a DAILY FINE OF ten thousand reais (BRL 10,000.00) in case of non-compliance.

Insert Official Letter AEED/GAB-SPR/GAB-PRES No. 2419/2023 in the case record.

Be it notified to the police authority.

For the knowledge of the Attorney General's Office.

Be it published.

Brasília, June 13, 2023.

Justice ALEXANDRE DE MORAES

Rapporteur

Document digitally signed

[REDACTED]



Supremo Tribunal Federal

URGENTE

Ofício eletrônico nº 8064/2023

Brasília, 14 de junho de 2023.

Ao Senhor
Administrador do RUMBLE no Brasil

Inquérito nº 4923

AUTOR(A/S)(ES) : MINISTÉRIO PÚBLICO FEDERAL
PROC.(A/S)(ES) : PROCURADOR-GERAL DA REPÚBLICA
INVEST.(A/S) : IBANEIS ROCHA BARROS JÚNIOR
ADV.(A/S) : CLEBER LOPES DE OLIVEIRA (15068/DF, 50206/GO) E OUTRO(A/S)
INVEST.(A/S) : ANDERSON GUSTAVO TORRES
ADV.(A/S) : EUMAR ROBERTO NOVACKI (64600/DF)
INVEST.(A/S) : FERNANDO DE SOUSA OLIVEIRA
ADV.(A/S) : DANILO DAVID RIBEIRO (15072/DF, 14768/ES) E OUTRO(A/S)
INVEST.(A/S) : FÁBIO AUGUSTO VIEIRA
ADV.(A/S) : JOAO PAULO DE OLIVEIRA BOAVENTURA (31680/DF, 68794/GO, 202448/MG) E OUTRO(A/S)
AUT. POL. : DELEGADO DE POLÍCIA FEDERAL

(Gerência de Processos Originários Criminais)

Senhor Administrador,

Encaminho-lhe os termos da decisão de cópia anexa para adoção das providências necessárias ao seu cumprimento, para que, **no prazo de 2 (duas) horas**, proceda ao bloqueio da conta de BRUNO MONTEIRO AIUB, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

RUMBLE: <https://rubble.com/c/Monarkx>

Atenciosamente,

Ministro Alexandre de Moraes
Relator

Documento assinado digitalmente

INQ 4923 / DF

instituições eleitorais (Ofício AEED/GAB-SPR/GAB-PRES nº 2419/2023).

É o breve relato. DECIDO.

Conforme ressaltai por ocasião da decisão proferida em 8/1/2023, os desprezíveis ataques terroristas à Democracia e às Instituições Republicanas serão responsabilizados, assim como os financiadores, instigadores e os anteriores e atuais agentes públicos coniventes e criminosos, que continuam na ilícita conduta da prática de atos antidemocráticos. Na data de 8/1/2023, como é de amplo conhecimento nacional e internacional, a escalada violenta dos atos criminosos resultou na invasão dos prédios do PALÁCIO DO PLANALTO, do CONGRESSO NACIONAL e do SUPREMO TRIBUNAL FEDERAL, com depredação do patrimônio público.

O papel dos instigadores dos atos, especialmente nas redes sociais, não é circunstância de menor relevância, ficando claro que os referidos meios de comunicação são parte essencial da empreitada criminosa que resultou nos estarrecedores atos testemunhados no dia 8/1/2023, e nos subsequentes atos programados para os dias seguintes, objeto de decisões nestes autos e na ADPF 519.

Nesse contexto, tenho reiteradamente enfatizado que a Constituição Federal consagra o binômio “LIBERDADE e RESPONSABILIDADE”; não permitindo de maneira irresponsável a efetivação de abuso no exercício de um direito constitucionalmente consagrado; não permitindo a utilização da “liberdade de expressão” como escudo protetivo para a prática de discursos de ódio, antidemocráticos, ameaças, agressões, infrações penais e toda a sorte de atividades ilícitas.

Liberdade de expressão não é Liberdade de agressão!

Liberdade de expressão não é Liberdade de destruição da Democracia, das Instituições e da dignidade e honra alheias!

Liberdade de expressão não é Liberdade de propagação de discursos mentirosos, agressivos, de ódio e

INQ 4923 / DF

preconceituosos!

Em face das circunstâncias apontadas, imprescindível a realização de diligências, inclusive com o afastamento excepcional de garantias individuais que não podem ser utilizadas como um verdadeiro escudo protetivo para a prática de atividades ilícitas, tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de desrespeito a um verdadeiro Estado de Direito (HC nº 70.814-5/SP, Rel. Min. CELSO DE MELLO, Primeira Turma, DJ de 24/6/1994).

Desse modo, conforme relatado, por meio da decisão proferida em 8/1/2023, foi determinado o bloqueio de diversos perfis/canais de titularidade de BRUNO AIUB MONTEIRO, conhecido como “Monark”, nas redes sociais Instagram (@monarkoficial), Rumble (<https://rumble.com/Monark>), Telegram (<https://t.me/monarktalks> e <https://t.me/monarkk>), Tik Tok (https://www.tiktok.com/@monarktalks_) Twitter (@monark) e Youtube (<https://www.youtube.com/@MonarkTalksCortesOficial>).

Entretanto, em novo canal criado na plataforma Rumble (<https://rumble.com/c/Monarkx>), que já conta com 287 mil seguidores, BRUNO MONTEIRO AIUB, conforme relatado pela AEED/TSE, voltou a divulgar notícias fraudulentas acerca da atuação desta SUPREMA CORTE e do TRIBUNAL SUPERIOR ELEITORAL, nos seguintes termos:

“Monark diz: ‘E não é o cara que tá indo lá, lutando e colocando... porque, toda vez que o Supremo faz um movimento desse, ele gasta fichas políticas. Isso tem um custo pra ele. [...] Então, porque ele (Supremo) está disposto a pagar este custo? **Por que ele (Supremo) está disposto a garantir uma não-transparência nas eleições? A gente vê o TSE censurando gente, a gente vê o Alexandre de Moraes prendendo pessoas, você vê um monte de coisa acontecendo, e ao mesmo tempo eles impedindo a transparência das urnas? Você fica desconfiado, que maracutaia está acontecendo nas urnas ali?**”

INQ 4923 / DF

Por quê? Por que o nosso sistema político não quer deixar o povo brasileiro ter mais segurança? Qual é o interesse? Manipular as urnas? Manipular as eleições? É isso que eu fico pensando...’.”

Além disso, a AEED/TSE indicou a criação de diversos outros perfis, em completo desrespeito à decisão anteriormente proferida:

Twitter: <https://twitter.com/MonarkVoltou> (16,2 mil seguidores)

Instagram: <https://www.instagram.com/monark.talks/> (101 mil seguidores)

Telegram: <https://t.me/monarktalks>

Discord: <https://discord.gg/8NKCauHf9>

Assim, se torna necessária, adequada e urgente a interrupção de eventual propagação dos discursos com conteúdo de ódio, subversão da ordem e incentivo à quebra da normalidade institucional e democrática mediante bloqueio de contas em redes sociais, com objetivo de interromper a lesão ou ameaça a direito (art. 5º, XXXV, Constituição Federal), conforme anteriormente ressaltado.

Diante do exposto, DETERMINO a expedição de ofício às empresas DISCORD, META INC., RUMBLE, TELEGRAM e TWITTER, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo: [acrescentar todos os links indicados:

DISCORD

<https://discord.gg/8NKCauHf9>

META INC.

<https://www.instagram.com/monark.talks/>

INQ 4923 / DF

RUMBLE

<https://rumble.com/c/Monarkx>

TELEGRAM

<https://t.me/monarktalks>

TWITTER

<https://twitter.com/MonarkVoltou>

DETERMINO, AINDA, A IMPOSIÇÃO DE MEDIDA CAUTELAR em face de BRUNO MONTEIRO AIUB, consistente na abstenção de publicação, promoção, replicação e compartilhamento das notícias fraudulentas (*fake news*) objeto da presente decisão, sob pena de MULTA DIÁRIA DE R\$ 10.000,00 (dez mil reais) no caso de descumprimento.

Junte-se aos autos o Ofício AEED/GAB-SPR/GAB-PRES nº 2419/2023.

Comunique-se à autoridade policial.

Ciência à Procuradoria-Geral da República.

Publique-se.

Brasília, 13 de junho de 2023.

Ministro ALEXANDRE DE MORAES

Relator

Documento assinado digitalmente

Exhibit 4
Federal Supreme Court, Investigation
4.923 (July 28, 2023)

Investigation 4.923 Federal District

Rapporteur : Justice Alexandre de Moraes

Plaintiff(s) : Federal Prosecution Office

Prosecutor(s) : Federal Prosecutor

Suspect(s) : Ibaneis Rocha Barros Júnior

Attorney(s) : [REDACTED]

Suspect(s) : Anderson Gustavo Torres

Attorney(s) : [REDACTED]

Suspect(s) : Fernando de Sousa Oliveira

Attorney(s) : [REDACTED]

Suspect(s) : Fábio Augusto Vieira

Attorney(s) : [REDACTED]

Police : Federal Police Chief

Authority

Brasilia, July 28, 2023.

To company
RUMBLE

Re.: Investigation 4.923

Dear Officer,

I inform you that a decision was rendered on the confidential case record above for IMMEDIATE execution, as follows:

I FURTHER ORDER the companies/providers listed below to proceed with the blocking of the channels/profiles/accounts detailed below on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), and provide their registration data to this SUPREME COURT and the full preservation of their contents:

RUMBLE

<https://rumble.eom/c/MONARKS>

https://rumble.com/c/Monarky_ (Monarky)

<https://rumble.eom/c/c-1516765> (CorteMonark)

<https://rumble.eom/c/MONARKTALKSCUTS> (Monark Talk Cuts)

<https://rumble.com/user/Monarkx> (MonarkX)

THE PLATFORMS SHALL FURTHER:

(a) IMMEDIATELY SUSPEND the transfer of any amounts arising from monetization, services used for donations, payment for advertising and registration of supporters, and those arising from monetized lives, including those carried out through the provision of transmission keys to the channels/profiles indicated above

(b) SUSPEND the transfer of any amounts arising from the monetization of services used for donations, payment for advertising and registration of supporters and arising from monetized broadcast of the program entitled “MONARK TALKS”; and

(c) indicate the individual amounts earned by the channels, profiles and pages mentioned above, with reports to be presented within five (5) days.

Given the confidential nature of this case record, the required arrangements for its maintenance shall be taken.

With nothing further, I take this opportunity to renew my assurances of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

document digitally signed

[REDACTED]

INQ 4923 / DF

https://rumble.com/c/Monarky_ (Monarky)
<https://rumble.com/c/c-1516765> (CorteMonark)
<https://rumble.com/c/MONARKTALKSCUTS> (Monark
Talk Cuts)
<https://rumble.com/user/Monarkx> (MonarkX)

DEVERÃO AS PLATAFORMAS, AINDA:

(a) SUSPENDER, imediatamente, o repasse de quaisquer valores oriundos de monetização, dos serviços usados para doações, do pagamento de publicidade e da inscrição de apoiadores, e advindos de monetização oriunda de lives, inclusive as realizadas por meio de fornecimento de chaves de transmissão aos canais/perfis acima indicados

(b) SUSPENDER o repasse de quaisquer valores oriundos de monetização, dos serviços usados para doações, do pagamento de publicidade e da inscrição de apoiadores, e advindos de monetização oriunda de veiculação do programa intitulado "MONARK TALKS"; e

(c) indicar, de forma individualizada, os valores auferidos pelos canais, perfis e páginas referidos acima, com relatórios a serem apresentados em 5 (cinco) dias.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Exhibit 5
Federal Supreme Court, Petition 9.935
(Dec. 14, 2023)

Petition 9.935 Federal District

Rapporteur : Justice Alexandre de Moraes
Petitioner(s) : Confidential
Attorney(s) : Confidential
Respondent(s) : Confidential
Attorney(s) : Confidential

Brasília, December 14, 2023.

To company
RUMBLE

Re: Petition 9.935

Dear Officer,

I inform you that a decision was rendered on the confidential case record above for IMMEDIATE execution, as follows:

In view of the foregoing, I ORDER, in integrative manner in relation to decisions of 1/13/2022, 2/10/2022, 2/13/2022, 2/15/2022, 2/17/2022, 2/23/2022, 3/8/2022, 3/18/2022, 3/23/2022, 4/4/2022, 5/20/2022, 6/7/2022, 6/27/2022, 10/5/2022, 10/20/2022, 11/5/2022, 11/6/2022, 11/15/2022, 11/18/2022, 2/23/2023, 3/15/2023, 4/26/2023, 6/21/202, 9/22/2023, 9/27/2023 and 10/20/2012, that a notice be served on companies TWITTER, META, TELEGRAM, RUMBLE and LOCALS for them to proceed with the blocking of the channels/profiles/accounts detailed below within two (2) hours, on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), with the provision of their registration data to this SUPREME COURT, and full preservation of their contents:

RUMBLE

<https://rumble.com/c/canaltercalivre>

I FURTHER ORDER SAID COMPANIES to immediately suspend the transfer of amounts arising from monetization, services used for donations, payment of advertising and registration of supporters, and arising from monetized lives, including those made through the provision of transmission keys to the channels/profiles mentioned above, informing this SUPREME COURT of all transfers made up to the date of receipt of the court order.

Given the confidential nature of this case record, the required arrangements for its maintenance shall be taken.

With nothing further, I take this opportunity to renew my assurances of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

document digitally signed

[REDACTED]

PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 14 de dezembro de 2023.

À empresa
RUMBLE

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação às decisões de 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 3/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/202, 22/9/2023, 27/9/2023 e 20/10/2012, a intimação das empresas TWITTER, META, TELEGRAM, RUMBLE e LOCALS, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

RUMBLE

<https://rumble.com/c/canaltercalivre>

DETERMINO ÀS REFERIDAS EMPRESAS, ainda, a

PET 9935 / DF

suspensão imediata do repasse de valores oriundos de monetização, dos serviços usados para doações, do pagamento de publicidades e da inscrição de apoiadores, e advindos de monetização oriunda de *lives*, inclusive as realizadas por meio de fornecimento de chaves de transmissão aos canais/perfis acima referidos, informando a esta SUPREMA CORTE todos os repasses efetuados até a data do recebimento da ordem judicial.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à empresa RUMBLE

Exhibit 6
Federal Supreme Court, Petition 9.935
(Dec. 14, 2023)

Petition 9.935 Federal District

Rapporteur : **Justice Alexandre de Moraes**
Petitioner(s) : CONFIDENTIAL
Attorney(s) : CONFIDENTIAL
Respondent(s) : CONFIDENTIAL
Attorney(s) : CONFIDENTIAL

Brasília, December 14, 2023.

To company
LOCALS

Re: Petition 9.935

Dear Officer,

I inform you that a decision was rendered on the confidential case record above for IMMEDIATE execution, as follows:

In view of the foregoing, I ORDER, in supplementary and integrative manner in relation to decisions of 1/13/2022, 2/10/2022, 2/13/2022, 2/15/2022, 2/17/2022, 2/23/2022, 3/8/2022, 3/18/2022, 3/23/2022, 4/4/2022, 5/20/2022, 6/7/2022, 6/27/2022, 10/5/2022, 10/20/2022, 11/5/2022, 11/6/2022, 11/15/2022, 11/18/2022, 2/23/2023, 3/15/2023, 4/26/2023, 6/21/202, 9/22/2023, 9/27/2023 and 10/20/2012, that a notice be served on companies TWITTER, META, TELEGRAM, RUMBLE and LOCALS to proceed with the blocking of the channels/profiles/accounts detailed below within two (2) hours, on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), with the provision of their registration data to this SUPREME COURT, and preservation of their contents:

LOCALS

<https://terca.locals.com/>

I FURTHER ORDER SAID COMPANIES to immediately suspend the transfer of amounts arising from monetization, services used for donations, payment of advertising and registration of supporters, and arising from monetized lives, including those made through the provision of transmission keys to the channels/profiles mentioned above, informing this SUPREME COURT of all transfers made up to the date of receipt of the court order.

Given the confidential nature of this case record, the required arrangements for its maintenance shall be taken.

With nothing further, I take this opportunity to renew my assurances of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

document digitally signed



PETIÇÃO 9.935 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 14 de dezembro de 2023.

À empresa
LOCALS

Ref: Petição 9.935

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo em relação às decisões de 13/1/2022, 10/2/2022, 13/2/2022, 15/2/2022, 17/2/2022, 23/2/2022, 8/3/2022, 18/3/2022, 23/3/2022, 4/4/2022, 20/5/2022, 7/6/2022, 27/6/2022, 5/10/2022, 20/10/2022 5/11/2022, 6/11/2022, 15/11/2022, 18/11/2022, 23/2/2023, 15/3/2023, 26/4/2023, 21/6/202, 22/9/2023, 27/9/2023 e 20/10/2012, a intimação das empresas TWITTER, META, TELEGRAM, RUMBLE e LOCALS, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

LOCALS

<https://terca.locals.com/>

DETERMINO ÀS REFERIDAS EMPRESAS, ainda, a

PET 9935 / DF

suspensão imediata do repasse de valores oriundos de monetização, dos serviços usados para doações, do pagamento de publicidades e da inscrição de apoiadores, e advindos de monetização oriunda de *lives*, inclusive as realizadas por meio de fornecimento de chaves de transmissão aos canais/perfis acima referidos, informando a esta SUPREMA CORTE todos os repasses efetuados até a data do recebimento da ordem judicial.

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro **ALEXANDRE DE MORAES**

Relator

documento assinado digitalmente

Cópia destinada à empresa LOCALS

Exhibit 7
Federal Supreme Court, Petition 10.802
(Jan. 5, 2024)

Petition 10.802 Federal District

Rapporteur : **Justice Alexandre de Moraes**
Petitioner(s) :CONFIDENTIAL
Attorney(s) :CONFIDENTIAL
Respondent(s) :CONFIDENTIAL
Attorney(s) :CONFIDENTIAL

Brasília, January 5, 2024

To company
RUMBLE

Re: Petition 10802

Dear Officer,

I inform you that a decision was rendered on the confidential case record above for IMMEDIATE execution, as follows:

In view of the foregoing, I ORDER, in supplementary and integrative manner to the decisions of 12/30/2022, 5/3/2023, 5/17/2023 and 5/19/2023, that a notice be served on social networks TWITTER, INSTAGRAM, TIKTOK, TELEGRAM, GETTR, RUMBLE and LOCALS, for them to proceed with the blocking of the channels/profiles/accounts detailed below within two (2) hours, on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), with the provision of their registration data and identification of the user to this SUPREME COURT, and the full preservation of their content:

RUMBLE

<https://rumble.com/c/REALPFIGUEIREDO>

Given the confidential nature of this case record, the required arrangements for its maintenance shall be taken.

With nothing further, I take this opportunity to renew my assurances of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

document digitally signed



PETIÇÃO 10.802 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 5 de janeiro de 2024.

À empresa
RUMBLE

Ref: Petição 10.802

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo às decisões de 30/12/2022, 3/5/2023, 17/5/2023 e 19/5/2023, a intimação das redes sociais TWITTER, INSTAGRAM, TIKTOK, TELEGRAM, GETTR, RUMBLE e LOCALS, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário, a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

RUMBLE

<https://rumble.com/c/REALPFIGUEIREDO>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

PET 10802 / DF

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Rumble

Exhibit 8
Federal Supreme Court, Petition 10.802
(Jan. 5, 2024)

Petition 10.802 Federal District

Rapporteur : **Justice Alexandre de Moraes**
Petitioner(s) :CONFIDENTIAL
Attorney(s) :CONFIDENTIAL
Respondent(s) :CONFIDENTIAL
Attorney(s) :CONFIDENTIAL

Brasília, January 5, 2024

To company
LOCALS

Re.: Petition 10.802

Dear Officer,

I inform you that a decision was rendered on the confidential case record above for IMMEDIATE execution, as follows

In view of the foregoing, I ORDER, in supplementary and integrative manner to the decisions of 12/30/2022, 5/3/2023, 5/17/2023 and 5/19/2023, that a notice be served on social networks TWITTER, INSTAGRAM, TIKTOK , TELEGRAM, GETTR, RUMBLE and LOCALS, for them to proceed with the blocking of the channels/profiles/accounts detailed below within two (2) hours, on pain of a daily fine of one hundred thousand reais (BRL 100,000.00), with the provision of their registration data and identification of the user to this SUPREME COURT, and the full preservation of their content:

LOCALS

<https://realpfigueiredo.locals.com/>

Given the confidential nature of this case record, the required arrangements for its maintenance shall be taken.

With nothing further, I take this opportunity to renew my assurances of high esteem and consideration.

Justice **ALEXANDRE DE MORAES**

Rapporteur

Document digitally signed

[REDACTED]

PETIÇÃO 10.802 DISTRITO FEDERAL

RELATOR : **MIN. ALEXANDRE DE MORAES**
REQTE.(S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**
REQDO.(A/S) : **SOB SIGILO**
ADV.(A/S) : **SOB SIGILO**

Brasília, 5 de janeiro de 2024.

À empresa
LOCALS

Ref: Petição 10.802

Senhor Diretor,

Comunico-lhe que foi proferida decisão nos autos sigilosos em epígrafe, para IMEDIATO cumprimento, nos seguintes termos:

Diante de todo o exposto, DETERMINO, em caráter complementar e integrativo às decisões de 30/12/2022, 3/5/2023, 17/5/2023 e 19/5/2023, a intimação das redes sociais TWITTER, INSTAGRAM, TIKTOK, TELEGRAM, GETTR, RUMBLE e LOCALS, para que, no prazo de 2 (duas) horas, procedam ao bloqueio dos canais/perfis/contas abaixo discriminados, sob pena de multa diária de R\$ 100.000,00 (cem mil reais), com o fornecimento de seus dados cadastrais, identificando o usuário, a esta SUPREMA CORTE e a integral preservação de seu conteúdo:

LOCALS

<https://realpfigueiredo.locals.com/>

Diante do caráter sigiloso destes autos, deverão ser adotadas as providências necessárias para a sua manutenção.

PET 10802 / DF

Sem mais para o momento, aproveito a oportunidade para renovar meus protestos de elevada estima e consideração.

Ministro ALEXANDRE DE MORAES

Relator

documento assinado digitalmente

Cópia destinada à Locals

Exhibit 9
Department of Federal Police, Petition
10.800 (Jan. 15, 2024)

[Coat of arms of Brazil]

FEDERAL POLICE

INVESTIGATION COORDINATION IN HIGHER COURTS - CINQ/CGRC/DICOR/PF

Address: [Redacted]
[Redacted]
[Redacted]

Official Letter No. 13010/2024 - CINQ/CGRC/DICOR/PF

Brasília/DF, January 15, 2024.

To
Rumble Brasil

Subject : Information (request)

Re: PET 10800 - STF (RE 2023.0107427 - CINQ/CGRC/DICOR/PF)

Sirs,

For purposes of producing evidence in the case record of PET 10800 - STF, I request you to make available, within 48 hours, the registration data related to the accounts and respective users: Tudo Consta (<https://rumble.com/c/c-2327224>), as recommended in article 3, IV of Law no. 12.850/2013.

Kind regards,

Document signed electronically on 1/15/2024 at 10:52 am [Redacted]
[Redacted]
[Redacted]
[Redacted]



POLÍCIA FEDERAL

COORDENAÇÃO DE INQUÉRITOS NOS TRIBUNAIS SUPERIORES - CINQ/CGRC/DICOR/PF

Endereço: [REDACTED]

Ofício nº 13010/2024 - CINQ/CGRC/DICOR/PF

Brasília/DF, 15 de janeiro de 2024.

À
Rumble Brasil

Assunto: Informações (solicita)

Referência: PET 10800 - STF (RE 2023.0107427 - CINQ/CGRC/DICOR/PF)

Senhores,

Visando instruir os autos da PET 10800 - STF, solicito a Vossa Senhoria que disponibilizem, no prazo de 48 horas, os dados cadastrais pertinentes às contas e respectivos usuários: Tudo Consta (<https://rumhle.com/c/c-2327224>), conforme preconizado pelo art. 3º, IV da Lei n.º 12.850/2013.

Atenciosamente,

[REDACTED]

Exhibit 10
Department of Federal Police, Petition
10.800 (Jan. 15, 2024)

[Coat of arms of Brazil]

FEDERAL POLICE

INVESTIGATION COORDINATION IN HIGHER COURTS - CINQ/CGRC/DICOR/PF

Address:

[Redacted address]

Official Letter No. 13075/2024 - CINQ/CGRC/DICOR/PF

Brasília/DF, January 15, 2024.

To

Locals Brasil

Subject: Information (request)

Re: PET 10800 - STF (RE 2023.0107427 - CINQ/CGRC/DICOR/PF)

Sirs,

For purposes of producing evidence in the case record of PET 10800 - STF, I request you to make available, within 48 hours, the registration data related to the accounts and respective users: Rodrigo Constantino (<https://rodrigoconstantino.locals.com/>), as recommended in article 3, IV of Law no. 12.850/2013.

Kind regards,

Document signed electronically on 1/15/2024 at 10:51a.m

[Redacted signature]

[Redacted signature line]

[Redacted signature line]

[Redacted signature line]

[Redacted signature line]



POLÍCIA FEDERAL

COORDENAÇÃO DE INQUÉRITOS NOS TRIBUNAIS SUPERIORES - CINQ/CGRC/DICOR/PF

Endereço: Setor Comercial Norte, Quadra 4, Bloco A, Torre B, 5º andar - Asa Norte - Edifício Multibrasil Corporate

- CEP: 70714-903 - Brasília/DF

Ofício nº 13075/2024 - CINQ/CGRC/DICOR/PF

Brasília/DF, 15 de janeiro de 2024.

À
Locals Brasil

Assunto: Informações (solicita)

Referência: PET 10800 - STF (RE 2023.0107427 - CINQ/CGRC/DICOR/PF)

Senhores,

Visando instruir os autos da PET 10800 - STF, solicito a Vossa Senhoria que disponibilizem, no prazo de 48 horas, os dados cadastrais pertinentes às contas e respectivos usuários: Rodrigo Constantino (<https://rodrigoconstantino.locals.com/>), conforme preconizado pelo art. 3º, IV da Lei n.º 12.850/2013.

Atenciosamente,

Documento eletrônico assinado em 15/01/2024, às 10h51,

IV. The Select Subcommittee filed briefs to help support Americans' First Amendment rights in court

In August 2023, 12 Members of Congress, including 9 Members of the Select Subcommittee, filed an amicus brief in support of the plaintiffs-appellees in *Missouri v. Biden*, a federal lawsuit then-pending in the U.S. Court of Appeals for the Fifth Circuit challenging the constitutionality of the federal government's wide-ranging censorship enterprise.⁷³ During oral argument, the panel of Fifth Circuit judges discussed the amicus brief and whether the Fifth Circuit could take "judicial notice" of the exhibits included in the Members' amicus brief.⁷⁴ After the Fifth Circuit affirmed the lower court's ruling and the case was appealed to the Supreme Court, 45 Members of Congress, including 11 Members of the Select Subcommittee, filed another amicus brief in the case (now *Murthy v. Missouri*) in support of those challenging the federal government's censorship regime.⁷⁵

The Select Subcommittee's brief before the Supreme Court outlined how the Biden-Harris Administration coerced and colluded with Big Tech companies to "distort[] the free marketplace of ideas promised by the First Amendment" and "bring[] the weight of federal authority to bear on any speech it dislike[d]—including memes and jokes" during the COVID pandemic.⁷⁶ The brief also detailed the FBI's months-long 2020 campaign to suppress true allegations of Biden family influence peddling, as well as CISA's efforts to censor conservative speech before and after the 2020 presidential election.⁷⁷

The Select Subcommittee's efforts ensured that the Supreme Court considered this voluminous evidence of federal censorship efforts as the Court decided a critically important free speech case. Justice Alito's dissenting opinion, joined by Justices Thomas and Gorsuch, concluded that the Select Subcommittee proved that the Biden-Harris White House "engaged in a covert scheme of censorship" and referenced or cited the Select Subcommittee's May 1, 2024 interim report 17 times.⁷⁸ Justice Alito cited the Select Subcommittee's work to show that Facebook changed its policies about the lab leak theory because of pressure from the Biden-

⁷³ Brief for Reps. Jim Jordan, et. al, as Amici Curiae Supporting Plaintiffs-Appellees and Affirmance, *Missouri v. Biden*, 83 F.4th 350 (5th Cir. Oct. 3, 2024) (No. 23-30445).

⁷⁴ Matt Taibbi, *In Landmark Censorship Case, Judges Grill the Feds*, RACKET NEWS (Aug. 11, 2023) (noting that "[a] secondary goal [for the administration] had to be stifling judicial curiosity about a just-filed amicus brief from Judiciary Chair Jim Jordan and other House members containing 'Facebook Files' documents. But those dreams went up in smoke fast. [] Seven minutes in [] [Judge] Willett cut Tenny [the Biden Administration's lawyer] off. . . . Before long judges were rattling off greatest hits of both the *Missouri v. Biden* evidence and Facebook Files material[.]").

⁷⁵ Brief for Rep. Jim Jordan, et. al, as Amici Curiae in Support of Respondents, *Murthy v. Missouri*, 603 U.S. 43 (2024) (No. 23-411).

⁷⁶ *Id.* at 3.

⁷⁷ *See id.* at 7, 16.

⁷⁸ *See, e.g.,* *Murthy v. Missouri*, 603 U.S. 43, 78 n. 2 (2024) (Alito, J., dissenting) (citing "Interim Staff Report of the House Judiciary Committee, The Censorship-Industrial Complex: How Top Biden White House Officials Coerced Big Tech To Censor Americans, True Information, and Critics of the Biden Administration, p. 398 (May 1, 2024) (Committee Report), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/Censorship-Industrial-Complex-WH-Report_Appendix.pdf"); *id.* at 84, n.7 (Alito, J., dissenting) ("Notes recounting these calls were released by the House Judiciary Committee after the District Court entered the preliminary injunction and were published in a Committee Report. *See* Committee Report; Fed. Rule Evid. 201.").

Harris Administration.⁷⁹ Justice Alito specifically noted that “[i]nternal Facebook emails paint a clear picture of subservience.”⁸⁰ As a result, Justice Alito concluded that the Biden-Harris White House “engaged in a covert scheme of censorship that came to light only after the plaintiffs demanded their emails in discovery and a congressional Committee obtained them by subpoena,” citing the Executive Summary of the Committee’s and Select Subcommittee’s May 1, 2024 report on the Biden-Harris White House’s censorship campaign.⁸¹

* * *

The Select Subcommittee has uncovered both foreign and domestic threats to Americans’ First Amendment right to speak freely. Time and again, federal agencies and government bureaucrats have sought to silence citizens whose perspectives they disagreed with—often working with Big Tech companies and third parties to do so. After identifying these gross, illegal abuses of state power, the Select Subcommittee proposed legislative solutions—such as H.R. 4848, the Censorship Accountability Act; H.R. 4791, the Free Speech Protection Act; and H.R. 9605, the No Censors on our Shores Act—to ensure that government censors, foreign and domestic, are prevented from, or at least held accountable for, silencing the voices of the American people. The Committee on the Judiciary has passed the two bills in its jurisdiction, H.R. 4848 and H.R. 9605, and the House should consider them expeditiously.

⁷⁹ *Id.* at 2 (Alito, J., dissenting) (citing to Committee Report at 398, 463).

⁸⁰ *Id.* at 8 (Alito, J., dissenting).

⁸¹ *Id.* at 30 (Alito, J., dissenting) (citing to Committee Report at 1-2).

No. 23-30445

United States Court of Appeals for the Fifth Circuit

STATE OF MISSOURI; STATE OF LOUISIANA; AARON KHERIATY; MARTIN KULL-
DORFF; JAYANTA BHATTACHARYA; JILL HINES,
PLAINTIFFS-APPELLEES,

v.

JOSEPH R. BIDEN, JR.; VIVEK H. MURTHY; XAVIER BECERRA; DEPARTMENT OF
HEALTH & HUMAN SERVICES; ANTHONY FAUCI, ET AL.,
DEFENDANTS-APPELLANTS.

*APPEAL FROM THE U.S. DISTRICT COURT FOR THE WESTERN DISTRICT OF LOUISIANA,
NO. 22-CV-1213, HON. TERRY A. DOUGHTY, PRESIDING*

**BRIEF OF REPRESENTATIVES JIM JORDAN, KELLY ARMSTRONG,
ANDY BIGGS, DAN BISHOP, KAT CAMMACK, RUSSELL FRY, LANCE
GOODEN, HARRIET HAGEMAN, MIKE JOHNSON, THOMAS MASSIE,
BARRY MOORE, AND ELISE STEFANIK AS *AMICI CURIAE*
SUPPORTING PLAINTIFFS-APPELLEES AND AFFIRMANCE**

GENE P. HAMILTON
America First Legal Foundation
611 Pennsylvania Ave. SE #231
Washington, D.C. 20003
(202)964-3721
gene.hamilton@aflegal.org

CHRISTOPHER MILLS
Spero Law LLC
557 East Bay Street
#22251
Charleston, SC 29413
(843) 606-0640
cmills@spero.law

Counsel for *Amici Curiae*

CERTIFICATE OF INTERESTED PARTIES

State of Missouri, et al. v. Joseph R. Biden, Jr., et al., No. 23-30445:

The undersigned counsel of record certifies that the following listed persons and entities as described in the fourth sentence of Rule 28.2.1, in addition to those listed in the briefs of the parties, have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

Amicus: Jim Jordan is a Member of Congress who represents the Fourth District of Ohio in the United States House of Representatives.

Amicus: Kelly Armstrong is a Member of Congress who represents North Dakota in the United States House of Representatives.

Amicus: Andy Biggs is a Member of Congress who represents the Fifth District of Arizona in the United States House of Representatives.

Amicus: Dan Bishop is a Member of Congress who represents the Eighth District of North Carolina in the United States House of Representatives.

Amicus: Kat Cammack is a Member of Congress who represents the Third District of Florida in the United States House of Representatives.

Amicus: Russell Fry is a Member of Congress who represents the Seventh District of South Carolina in the United States House of Representatives.

Amicus: Lance Gooden is a Member of Congress who represents the Fifth District of Texas in the United States House of Representatives.

Amicus: Harriet Hageman is a Member of Congress who represents Wyoming in the United States House of Representatives.

Amicus: Mike Johnson is a Member of Congress who represents the Fourth District of Louisiana in the United States House of Representatives.

Amicus: Thomas Massie is a Member of Congress who represents the Fourth District of Kentucky in the United States House of Representatives.

Amicus: Barry Moore is a Member of Congress who represents the Second District of Alabama in the United States House of Representatives.

Amicus: Elise Stefanik is a Member of Congress who represents the Twenty-First District of New York in the United States House of Representatives.

Counsel for Amici: Christopher E. Mills of Spero Law LLC; Gene P. Hamilton of America First Legal Foundation.

/s/ Christopher Mills

Christopher Mills

Counsel for *Amici Curiae*

August 7, 2023

TABLE OF CONTENTS

	Page
Certificate of Interested Parties.....	i
Table of Authorities	iv
Interest of <i>Amici Curiae</i>	1
Introduction	3
Argument.....	6
I. The United States has coerced speech about COVID.....	6
II. The United States has coerced speech about Biden Family influence peddling.	14
III. The United States has coerced speech about elections.	22
A. Cybersecurity and Infrastructure Security Agency (CISA).....	23
B. The Election Integrity Partnership (EIP)	26
Conclusion	31

TABLE OF AUTHORITIES

CASES	Page(s)
<i>Anderson v. Bessemer City</i> , 470 U.S. 564 (1985).....	4
<i>Arizona Free Enter. Club’s Freedom Club PAC v. Bennett</i> , 564 U.S. 721 (2011).....	4, 5
<i>Barr v. Am. Ass’n of Pol. Consultants, Inc.</i> , 140 S. Ct. 2335 (2020).....	5
<i>Dennis v. United States</i> , 341 U.S. 494 (1951).....	4
<i>Direct Biologics, LLC v. McQueen</i> , 63 F.4th 1015 (5th Cir. 2023).....	4
<i>Kennedy v. Warren</i> , 66 F.4th 1199 (9th Cir. 2023).....	4
<i>McIntyre v. Ohio Elections Comm’n</i> , 514 U.S. 334 (1995).....	22
<i>Missouri v. Biden</i> , 2023 WL 4335270 (W.D. La. July 4, 2023).....	4, 6, 13, 13, 14
<i>Norwood v. Harrison</i> , 413 U.S. 455 (1973).....	31
<i>Snyder v. Phelps</i> , 562 U.S. 443 (2011).....	3, 5
<i>Texas v. Johnson</i> , 491 U.S. 397 (1989).....	3

STATUTES

6 U.S.C. § 652.....23

OTHER AUTHORITIES

Betsy Klein, *White House Reviewing Section 230 Amid Efforts to Push Social Media Giants to Crack Down on Misinformation*, CNN (Jul. 20, 2021)13

Bruce Golding, *Zuckerberg Says Facebook Censored the Post’s Hunter Biden Stories Because FBI Warned of Russian Misinfo ‘Dump,’* NEW YORK POST (Aug. 26, 2022)16

CENTER FOR INTERNET SEC., *EI-ISAC* 25, 25

CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, MIS-, DIS-, AND MALINFORMATION23

Declaration of Yoel Roth17

Deposition of Brian Scully24

Deposition of Elvis Chan 17, 19, 20, 21

DEP’T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY OPERATIONS AND SUPPORT FISCAL YEAR 2024 CONGRESSIONAL JUSTIFICATION (2023)25

ELECTION INTEGRITY P’SHIP, *The Long Fuse: Misinformation and the 2020 Election* (2021) 26, 27, 30

Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun Email Reveals how Hunter Biden Introduced Ukrainian Businessman to VP Dad*, NEW YORK POST (Oct. 14, 2020)15

Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 27, 2023) 28, 29, 30

Letter from Rep. Jordan, Chairman, House Comm on the Jud., to the Hon. Christopher Wray, Director, FBI (July 20, 2023) 14, 15, 16, 17, 18, 20, 21

Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM)29

Miranda Devine, *Media Helped Hide the Real Joe Biden by Censoring Hunter Stories*, NEW YORK POST (Nov. 28, 2021)22

Nandita Bose and Elizabeth Culliford, *Biden Says Facebook, Others ‘Killing People’ by Carrying COVID Misinformation*, REUTERS (Jul. 16, 2021)10

OFFICE OF INSPECTOR GEN., DEP’T OF HOMELAND SEC., OIG-22-58, DHS NEEDS A UNIFIED STRATEGY TO COUNTER DISINFORMATION CAMPAIGNS, (Aug. 10, 2022)23

Press Release, Dep’t of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017)23

Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 27, 2023, 12:03 PM)7

Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 28, 2023, 12:03 PM)7

Rep. Jim Jordan (@Jim_Jordan), TWITTER (Aug. 3, 2023, 11:00 AM)7

Rep. Jim Jordan (@Jim_Jordan), TWITTER (Aug. 7, 2023, 10:11 AM)7

Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*,
THE WALL STREET JOURNAL (July 28, 2023)14

Sen. Ted Cruz (@tedcruz), TWITTER (Oct. 27, 2022, 12:34 PM)26

STAFF OF THE H. COMM. ON THE JUD., 118TH CONG., INTERIM STAFF REPORT: THE
WEAPONIZATION OF CISA22

STAFF OF H. COMM. ON THE JUD., SELECT SUBCOMM. ON THE WEAPONIZATION OF
THE FED. GOV’T, & PERMANENT SELECT COMM. ON INTEL., 118TH CONG., THE
HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS
AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS (2023)15

STANFORD INTERNET OBSERVATORY, *Background on the SIO’s Projects on So-
cial Media* (Mar. 17, 2023)30

Steven Nelson, *The Post’s FB Traffic Tanked After WH Aide’s False Claim of
‘Churning Out Articles Every Day About People Dying’ From COVID Vax*,
NEW YORK POST (Aug. 4, 2023)9

U.S. DEP’T OF STATE, *About Us—Global Engagement Center*29

INTEREST OF AMICI CURIAE

Representatives Jim Jordan, Kelly Armstrong, Andy Biggs, Dan Bishop, Kat Cammack, Russell Fry, Lance Gooden, Harriet Hageman, Mike Johnson, Thomas Massie, Barry Moore, and Elise Stefanik are Members of the United States House of Representatives and Members of the House Judiciary Committee and/or the Select Subcommittee on the Weaponization of the Federal Government. The Judiciary Committee is authorized by the House to conduct oversight and legislate on matters concerning civil liberties, the separation of powers, and the judiciary. Each Member of Congress has taken an oath to uphold the Constitution and laws of the United States. As Members of the House Judiciary Committee and/or the Weaponization Subcommittee, each Member has an institutional interest in protecting First Amendment rights from encroachment by the executive branch, protecting the rule of law, and holding the executive branch accountable when it overreaches. This interest also includes ensuring that the courts police those constitutional boundaries.

Each Member signatory is concerned that the Biden Administration has violated the Constitution and abridged Americans' civil liberties. The House Judiciary Committee and the Weaponization Subcommittee have been conducting an ongoing investigation into how and to what extent the executive branch has coerced or colluded with social media companies to censor speech. Very recent evidence, obtained in said investigation in the weeks after the district court's preliminary injunction

ruling, further corroborates the district court’s findings. Thus, each Member signatory has a substantial interest in this case and offers a unique perspective by virtue of his or her role in Congress.¹

¹ All parties consented to the filing of this brief. Pursuant to Fed. R. App. P. 29(a)(4)(E), no party’s counsel authored this brief in whole or in part; no party or party’s counsel contributed money that was intended to fund preparing or submitting the brief; and, no person—other than the *amici curiae*, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief.

INTRODUCTION

Wielding threats of intervention, the executive branch of the federal government has engaged in a sustained effort to coerce private parties into censoring speech on matters of public concern. On issue after issue, the Biden Administration has distorted the free marketplace of ideas promised by the First Amendment, bringing the weight of federal authority to bear on any speech it dislikes—including memes and jokes. Of course, Big Tech companies often required little coercion to do the Administration’s bidding on some issues. Generally eager to please their ideological allies and overseers in the federal government, these companies and other private entities have repeatedly censored accurate speech on important public issues. When the censors were too slow to suppress speech that the partisans in the Administration disliked, the federal government prodded them back into action with continual and increasing pressure.

Official pressure to suppress speech violates the First Amendment. “[A] principal function of free speech under our system of government is to invite dispute. It may indeed best serve its high purpose when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger.” *Texas v. Johnson*, 491 U.S. 397, 408–09 (1989) (cleaned up). No doubt, the government may find some individuals’ speech “misguided, or even hurtful,” but “the point of all speech protection is to shield just those choices of content.” *Snyder v. Phelps*, 562

U.S. 443, 458 (2011) (cleaned up). “The First Amendment embodies our choice as a Nation that, when it comes to such speech, the guiding principle is freedom—the unfettered interchange of ideas—not whatever the State may view as fair.” *Arizona Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721, 750 (2011) (cleaned up). The First Amendment is founded on “the hypothesis that speech can rebut speech, propaganda will answer propaganda, [and] free debate of ideas will result in the wisest governmental policies.” *Dennis v. United States*, 341 U.S. 494, 503 (1951). Thus, the First Amendment stands against any governmental effort to coerce or otherwise burden the free speech of private entities—even if that action falls short of outright suppression. *Cf. Kennedy v. Warren*, 66 F.4th 1199, 1213 (9th Cir. 2023) (Bennett, J., concurring) (“[W]e do not require a government official to list specific consequences in order to find a constitutional violation.”).

The district court found, as a matter of fact, that “the United States Government, through the White House and numerous federal agencies, pressured and encouraged social-media companies to suppress free speech.” *Missouri v. Biden*, 2023 WL 4335270, at *44 (W.D. La. July 4, 2023). These factual findings “must be left undisturbed unless clearly erroneous.” *Direct Biologics, LLC v. McQueen*, 63 F.4th 1015, 1020 (5th Cir. 2023) (cleaned up). “Where there are two permissible views of the evidence, the factfinder’s choice between them cannot be clearly erroneous.” *Anderson v. Bessemer City*, 470 U.S. 564, 574 (1985).

The district court’s findings are easily “permissible”; they are clearly correct. Beyond the ample evidence cited by the district court and the Plaintiffs, even more recent evidence obtained by the House Judiciary Committee and the Weaponization Subcommittee confirms the district court’s conclusions.

That evidence shows that the Biden Administration has relentlessly pressured private entities—sometimes in cooperation with other private entities—to censor speech that the Administration disliked. As detailed below, this official coercion has undermined the marketplace of ideas on issues of public importance ranging from COVID to federal elections to Biden family misdeeds. And the suppression “does not simply have an effect on speech, but is directed at certain content and is aimed at particular speakers”: conservative voices opposed to the current Administration. *Barr v. Am. Ass’n of Pol. Consultants, Inc.*, 140 S. Ct. 2335, 2347 (2020). “This sort of ‘beggar thy neighbor’ approach to free speech—restricting the speech of some elements of our society in order to enhance the relative voice of others—is wholly foreign to the First Amendment.” *Bennett*, 564 U.S. at 741 (cleaned up). Likewise foreign to the First Amendment are governmental efforts to coerce the speech of private Americans. “As a Nation we have chosen a different course—to protect even hurtful speech on public issues to ensure that we do not stifle public debate.” *Snyder*, 562 U.S. at 461.

Because the Biden Administration has repeatedly used government coercion to stifle public debate—and the district court’s injunction rightfully halts the Administration’s unlawful conduct—the Court should affirm.

ARGUMENT

I. The United States has coerced speech about COVID.

As the district court found, the federal government “suppressed alternative views” about COVID-related matters, including the origination of the virus, the efficacy of vaccines and masks, and the adverse effects of lockdowns, effectively forcing social media companies to enforce the government’s view as “the truth.” *Biden*, 2023 WL 4335270, at *49–50. The district court listed over twenty examples of the government engaging in coercive acts directed toward social media companies to bring about censorship. *Id.* at *45–47. And the government’s pressure campaign worked. Facebook agreed to moderate certain COVID-related speech in response to pressure from the Biden Administration, telling the government that Facebook would rely on their “authorities” to determine what content to censor. *Id.* at *5, *6, *50. The district court described the government’s direction of Facebook’s content choices as a “partner[ship].” *Id.* at *47.

Very recent evidence corroborates the district court’s findings. The House Judiciary Committee subpoenaed internal documents from Meta, the parent entity of Facebook and Instagram. The documents obtained thus far confirm that the

companies censored information and altered their content moderation policies because of pressure from the Biden Administration to rid their platforms of purported “misinformation.”²

This pressure was direct and coercive. For example, the Administration tried to suppress discussion of COVID’s origins: when a Facebook executive asked in July 2021 why the company censored the COVID lab leak theory, an executive in charge of content policy development said, “[b]ecause we were under pressure from the [A]dministration” to do so.³ The same Facebook executive confessed that the company “shouldn’t have done it.”⁴

Yet Facebook continued to do the Administration’s bidding, repeatedly removing and reducing content the federal government disfavored. The Biden White House’s successful months-long campaign to censor views expressing or supporting vaccine hesitancy is the clearest example of how the government coerced social

² Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 27, 2023, 12:03 PM), <https://tinyurl.com/5nz8sn3b> (“THE FACEBOOK FILES PART 1”); Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 28, 2023, 12:03 PM), <https://tinyurl.com/3z5npf92> (“THE FACEBOOK FILES PART 2”); Rep. Jim Jordan (@Jim_Jordan), TWITTER (Aug. 3, 2023, 11:00 AM), <https://tinyurl.com/4kjvehbb> (“THE FACEBOOK FILES PART 3”); Rep. Jim Jordan (@Jim_Jordan), TWITTER (Aug. 7, 2023, 10:11 AM), <https://tinyurl.com/yebawzjr> (“THE FACEBOOK FILES PART 4”).

³ Ex. 1 (E-mail from Nick Clegg to Facebook employees (July 14, 2021, 11:46 AM)). All Exhibit cites are to this brief’s Appendix.

⁴ *Id.*

media companies to change the scope and enforcement of their content moderation policies.

In an internal email, a Facebook employee explained to CEO Mark Zuckerberg and COO Sheryl Sandberg: “We are facing continued pressure from external stakeholders, including the [Biden] White House and the press, to *remove* more COVID-19 vaccine discouraging content.”⁵

Mark, Sheryl:

We are seeking your guidance on whether to take more aggressive action against certain vaccine discouraging content.

We are facing continued pressure from external stakeholders, including the White House and the press, to *remove* more COVID-19 vaccine discouraging content. For example, we recently shared with the White House a list of the top 100 vaccine-related posts on FB in the U.S. for the week of 4/5-4/11. While authoritative information dominated the list, the White House was concerned that the #3 post was a vaccine discouraging humorous meme, and they called on us to delete the meme.

Another Facebook executive notified his team that a senior advisor to President Biden was “outraged” “that [Facebook] did not remove” a meme that bothered the Administration.⁶ Likewise, to appease the Administration, Facebook demoted a Tucker Carlson video critical of the COVID vaccine, even though Facebook admitted that the video did not violate company policy.⁷

⁵ Ex. 2 (E-mail from Facebook employee to Facebook employees (Apr. 27, 2021, 11:58 AM)) (emphasis in original).

⁶ Ex. 3 (E-mail from Nick Clegg to Facebook employees (Apr. 19, 2021, 9:40 AM)).

⁷ *Id.*

Tucker Carlson was not the only prominent critic of President Biden to be targeted by the Administration’s censorship efforts. According to Facebook’s internal notes of meetings with White House senior advisors, White House officials questioned whether Facebook’s enforcement of its content moderation policies against the *New York Post* was aggressive enough.⁸ Similarly, in April 2021, a White House official questioned whether Facebook could “change [its] algorithm so that people were more likely to see [the *New York Times*], [the *Wall Street Journal*], any authoritative news source over [the] Daily Wire, Tomi Lahren, polarizing people.”⁹ The White House’s requests were rooted in the paternalistic notion that Americans cannot decide for themselves what information should or should not be believed. As a White House staffer condescendingly remarked in a meeting with Facebook in April 2021, “[i]f someone in rural Arkansas sees something on [Facebook], it’s the

⁸ Ex. 4 (Facebook employee’s notes of a call between White House personnel and Facebook employees on March 26, 2021). The *New York Post*’s traffic on Facebook subsequently plummeted by over 50 percent before rebounding to “normal levels” by fall 2021. Steven Nelson, *The Post’s FB Traffic Tanked After WH Aide’s False Claim of ‘Churning Out Articles Every Day About People Dying’ From COVID Vax*, NEW YORK POST (Aug. 4, 2023), <https://tinyurl.com/rrmtzkk>.

⁹ Ex. 5 (Facebook employee’s notes of a call between White House personnel and Facebook employees on April 14, 2021).

truth.”¹⁰ In a June 2021 meeting, the White House pushed Facebook to “reduce the spread of bad information,” *i.e.*, “bad” information according to the White House.¹¹

Not only did the Biden Administration privately coerce Facebook and other companies into censoring information, it also engaged in a public relations campaign against the companies to pressure them into submission. In July 2021, President Biden publicly denounced these companies, particularly Facebook, claiming they were “killing people” by not censoring alleged “misinformation” to the government’s satisfaction.¹² Facebook employees internally lamented that the Biden White House’s “definition of ‘misinfo’ is completely unclear.”¹³ Following the White House’s pressure, Facebook leadership—internally admitting that the move was “stemming from the continued criticism of our approach from the [Biden] administration”—directed employees to “brainstorm some additional policy levers we can

¹⁰ Ex. 6 (Facebook employee’s notes of a call between White House personnel and Facebook employees on April 5, 2021).

¹¹ Ex. 7 (Facebook employee’s notes of a call between White House personnel and Facebook employees on June 15, 2021).

¹² Nandita Bose and Elizabeth Culliford, *Biden Says Facebook, Others ‘Killing People’ by Carrying COVID Misinformation*, REUTERS (Jul. 16, 2021), <https://ti.nyurl.com/zpt53rna>.

¹³ Ex. 8 (E-mail from Facebook employee to Facebook employees (July 16, 2021, 8:14 PM)).

pull to be more aggressive against . . . misinformation.”¹⁴ Ultimately, the company decided to adopt four new, more aggressive policy options one month later.¹⁵

Likewise, before meeting with the Biden Administration’s Office of the Surgeon General (OSG), a Facebook employee said that Sheryl Sandberg “is keen that we continue to explore some moves that we can make to show that we are trying to be responsive to the [White House].”¹⁶ The email continued: “My sense is that our current course—in effect explaining ourselves more fully, but not shifting on where we draw the lines . . . is a recipe for protracted and increasing acrimony with the [White House].”¹⁷ Internal documents obtained by the House Judiciary Committee and the Weaponization Subcommittee show that the Biden Administration pressured Facebook to censor information about the COVID vaccine’s side effects, even if the information was true.¹⁸ In a July 2021 meeting with OSG, a Facebook employee confirmed that Facebook was demoting content that questioned whether vaccine

¹⁴ Ex. 9 (E-mail from Facebook employee to Facebook employees (Aug. 6, 2021, 7:13 PM)).

¹⁵ Ex. 10 (E-mail from Nick Clegg to Facebook employees (Aug. 19, 2021, 5:25 PM)).

¹⁶ Ex. 11 (E-mail from Facebook employee to Facebook employees (July 22, 2021, 12:17 PM)).

¹⁷ *Id.*

¹⁸ Ex. 12 (E-mail from Sheryl Sandberg to Nick Clegg (Jul. 21, 2021, 4:49 PM)) (“The Surgeon General wants us to remove true information about side effects.”).

mandates constituted “government overreach,” despite acknowledging “[t]hat’s not false information.”¹⁹

Worse still, when Facebook questioned censoring information, the Biden Administration showed disdain and contempt for the First Amendment. For example, when the Administration flagged satirical content about the COVID vaccine, a Facebook executive first warned that removing satirical content would “represent a significant incursion into traditional boundaries of free expression in the US.”²⁰ But the Biden Administration was unpersuaded, insisting that the content “inhibits confidence” in the COVID vaccine.²¹

A Facebook vice president warned internally that the company was at “a crossroads” with the Administration over its censorship efforts.²² Facebook executives grasped the connection between the company’s business prospects and staying in the Administration’s good graces. One executive, recommending that the company consider bending to the Administration’s censorship requests, cautioned COO Sheryl Sandberg that Facebook had “bigger fish we have to fry with the Administration — data flows etc.”²³

¹⁹ Ex. 13 (Facebook employee’s notes of a call between OSG personnel and Facebook employees on July 16, 2021).

²⁰ Ex. 3 (E-mail from Nick Clegg to Facebook employees).

²¹ *Id.*

²² *Id.*

²³ Ex. 11 (E-mail from Facebook employee to Facebook employees).

Another looming issue was—and still is—reform of Section 230. As the district court explained, Section 230 of the Communications Decency Act is “valuable” to Big Tech because of its legal protections. *Biden*, 2023 WL 4335270, at *47. And the district court found that the federal government “threat[ened]” Big Tech with the repeal of Section 230 to induce compliance with its censorship campaign. *Id.* Mark Zuckerberg has referred to the possibility of antitrust enforcement as an “existential threat” to his empire. *Id.* at *4. Four days after President Biden publicly accused Facebook of “killing people,” the White House Communications Director publicly said the Administration was “reviewing” Section 230 reform as an option because the social media companies “should be held accountable.”²⁴ Internal documents show that Facebook executives feared that the Biden Administration would retaliate against the company for not censoring enough: one executive commented that the dispute over content was not “a great place for us to be,” and he would be “grateful for any further creative thinking on how we can be responsive to their [content] concerns.”²⁵ In response to mounting pressure, Facebook capitulated: “By August 2021,

²⁴ Betsy Klein, *White House Reviewing Section 230 Amid Efforts to Push Social Media Giants to Crack Down on Misinformation*, CNN (Jul. 20, 2021), <https://ti-nyurl.com/73hnfk3h>.

²⁵ Ex. 11 (E-mail from Facebook employee to Facebook employees).

Facebook executives were emailing each other about new planned changes to their Covid content policies,” including increased punishments for violators.²⁶

In short, the Biden Administration used its power to commandeer the apparatuses of social media companies to affect their COVID-related content policies. And out of self-interest, the companies complied and censored content beyond what it otherwise would have. This government coercion violates the First Amendment.

II. The United States has coerced speech about Biden Family influence peddling.

The federal government, specifically the FBI’s Foreign Influence Task Force (FITF), also used its power and influence to deceive and coerce social media companies into suppressing factual information during the 2020 election about the Biden family that the FBI knew to be true.²⁷ The district court rightly labeled “[t]he FBI’s failure to alert social-media companies that the Hunter Biden laptop story was real, and not mere Russian disinformation,” as “particularly troubling.” *Biden*, 2023 WL 4335270 *50. The laptop contained documents and emails with incriminating details

²⁶ Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, THE WALL STREET JOURNAL (July 28, 2023), <https://tinyurl.com/2bepvs5t>; *see also* Ex. 10 (E-mail from Nick Clegg to Facebook employees).

²⁷ Letter from Rep. Jordan, Chairman, House Comm on the Jud., to the Hon. Christopher Wray, Director, FBI, at 1 (July 20, 2023), <https://tinyurl.com/3m7a6wsa>.

about foreign business dealings that also implicated Hunter Biden’s father—then-presidential candidate, Joe Biden.²⁸

In a recent transcribed interview before the House Judiciary Committee and Weaponization Subcommittee, current Section Chief of FITF, Laura Dehmlow, testified that (1) FBI agents who knew the laptop was real were some of the same FBI agents who repeatedly warned social media companies about a potential “hack-and-leak” likely to occur in October 2020; and (2) despite direct requests from Twitter and Facebook for information on the day the *New York Post* story was published, the FBI decided to deliberately withhold critical information from the social media companies.²⁹

Although the FBI had the authenticated laptop in its possession since December 2019, it did not publicly acknowledge that it was real until after the November 3, 2020, election.³⁰ Rather than acknowledge the truth, the FBI actively influenced and deceived the social media companies to censor the story when it inevitably came

²⁸ Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun Email Reveals how Hunter Biden Introduced Ukrainian Businessman to VP Dad*, NEW YORK POST (Oct. 14, 2020), <https://tinyurl.com/v7maymv8>; STAFF OF H. COMM. ON THE JUD., SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T, & PERMANENT SELECT COMM. ON INTEL., 118TH CONG., THE HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS 1, 6 (2023), <https://tinyurl.com/47v4fxb8>.

²⁹ Ex. 14 (Excerpts of Transcribed Interview of Laura Dehmlow before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (July 17, 2023)), at 29–37, 173–174.

³⁰ Jordan, *supra* note 27, at 5.

out.³¹ In a well-executed, months-long plan, the FBI primed the narrative, telling social media companies to “look for a ‘hack and dump’ operation by the Russians prior to the 2020 election.”³² Then, as soon as the laptop’s contents were exposed, the FBI refused to answer questions and let the narrative it had constructed do its work of distracting from and minimizing the truth. Mark Zuckerberg’s justification for censoring the story illustrates the effectiveness of this plan: “the FBI basically came to us” and said, “you should be on high alert.” Facebook censored the story because when “[the FBI] come[s] to us and tell[s] us that we need to be on guard about something, then I want to take that seriously,” and the story “basically fit the pattern” the FBI warned about.³³ This federal coercion led to the censorship of accurate information.

In “the nine months leading up to the 2020 election, the FBI met over 30 times with social media platforms—all while in possession of Hunter Biden’s laptop.”³⁴ The FBI had “at least five meetings with Facebook, Google, Microsoft, [and] Yahoo!, in addition to multiple meetings with Twitter and Reddit.”³⁵ Yoel Roth, former Head of Site Integrity at Twitter, confirmed in a sworn declaration that he had regular

³¹ *Id.* at 1.

³² *Id.* at 4.

³³ Bruce Golding, *Zuckerberg Says Facebook Censored the Post’s Hunter Biden Stories Because FBI Warned of Russian Misinfo ‘Dump,’* NEW YORK POST (Aug. 26, 2022), <https://tinyurl.com/5n8xz6xd>.

³⁴ Jordan, *supra* note 27, at 1.

³⁵ *Id.*

meetings in 2020 with different federal agencies, including the FBI, where they “communicated that they expected ‘hack-and-leak operations’” against those associated with political campaigns “shortly before the 2020 presidential election, likely in October.”³⁶ “These expectations of hack-and-leak operations were discussed throughout 2020.”³⁷ He was also told “that material obtained through those hacking attacks would likely be disseminated over social media platforms, including Twitter” and even that there were rumors the materials could involve Hunter Biden.³⁸

The companies also participated together in regular “USG-Industry” meetings, including four in October 2020, with representatives from federal agencies, including the FBI.³⁹ During these meetings, the FBI asked social media companies what their “hack and leak” policies were, how the companies would handle a potential “hack and leak,” and whether the companies would remove hacked materials from their platforms.⁴⁰ In response, some companies without a specific “hack and

³⁶ Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Commission MUR 7821, (Dec. 17, 2020), <https://tinyurl.com/3mmzx2bk> [hereinafter Roth Decl.].

³⁷ *Id.*

³⁸ *Id.*

³⁹ Jordan, *supra* note 27, at 1.

⁴⁰ Deposition of Elvis Chan at 248:5–250:21 (filed below as ECF No. 204-1) [hereinafter Chan Dep.]; *see also* Roth Decl., *supra* note 36, ¶ 11.

leak” policy, such as Facebook, developed and adopted a new policy during summer 2020.⁴¹

Dehmlow confirmed that “the FBI could—and did—share information with companies regarding foreign malign influence operations, like hack-and-leak operations, including those conducted by Russia-aligned actors.”⁴² For example, the agenda for the October 7, 2020 “USG-Industry” meeting—one week before the October 14 *New York Post* story—lists “Hack/Leak Concerns” as a topic.⁴³

On the day the article was published, FBI met with Twitter, and a company representative asked if the laptop was real.⁴⁴ In testimony to the House Judiciary Committee and Weaponization Subcommittee, Dehmlow stated that, in response, “one of the FBI folks who was on the call” confirmed that the laptop was real before “another participant jumped in and said, ‘no further comment.’”⁴⁵ After the meeting, FBI personnel “deliberated internally” and determined that—even though they knew

⁴¹ Ex. 15 (Excerpts of Transcribed Interview of David Agranovich before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (May 16, 2023)); Ex. 16 (Excerpts of Transcribed Interview of Nathaniel Gleicher before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 21, 2023)).

⁴² Jordan, *supra* note 27, at 2; Ex. 14 (Laura Dehmlow Transcribed Interview), at 173–174.

⁴³ Ex. 17 (E-mail from Facebook employee to Matthew Masterson and Brian Scully (Sept. 29, 2020, 11:41 AM)).

⁴⁴ Ex. 14 (Laura Dehmlow Transcribed Interview), at 29.

⁴⁵ *Id.*

the laptop was not Russian disinformation—in all further communications with social media companies the FBI would reply with “no comment.”⁴⁶

Later that same day, the FBI met with Facebook. This time the FBI had its story straight. When Facebook asked whether the laptop was real, Dehmlow, on behalf of the FBI, said, “no comment.”⁴⁷ Despite requests made during Dehmlow’s interview and subsequently to Director Wray by letter, the FBI has thus far refused to reveal to the House Judiciary Committee and Weaponization Subcommittee the identities of the FBI official who told Twitter that the laptop was real, the FBI lawyer who instructed “no further comment” during the call with Twitter, or the FBI official who determined that the agency would respond only “no comment” when asked about Hunter Biden laptop’s authenticity going forward.⁴⁸

Facebook followed up again the next day, October 15.⁴⁹ According to an internal Facebook document recently obtained by the House Judiciary Committee and the Weaponization Subcommittee, a Facebook employee (and former FBI official) “spoke with SSA Elvis Chan (FBI San Francisco) on 15 October 2020, as a follow up to the call with the Foreign Influence Task Force on 14 October.”⁵⁰ Facebook

⁴⁶ *Id.* at 33.

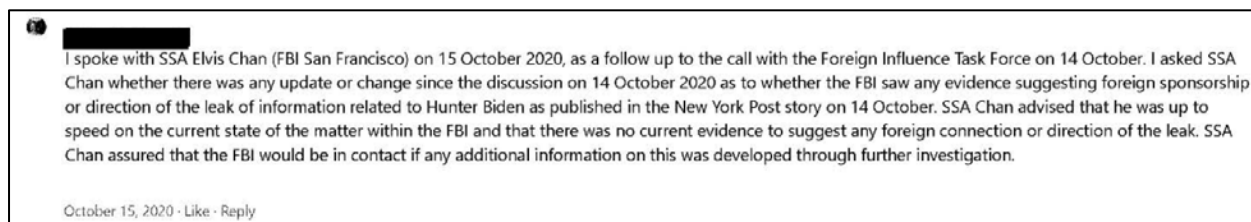
⁴⁷ *Id.* at 33; *see also* Chan Dep., *supra* note 400, at 215.

⁴⁸ *See* Ex. 14 (Laura Dehmlow Transcribed Interview), at 29–31; Jordan, *supra* note 27, at 5–6 (requesting a response by August 3, 2023).

⁴⁹ Ex. 18 (Entry on internal Facebook case file by Facebook employee (Oct. 15, 2020)).

⁵⁰ *Id.*

again asked if the FBI had any new information, to which “Chan advised that he was up to speed on the current state of the matter within the FBI and that there was no current evidence to suggest any foreign connection or direction of the leak.”⁵¹ But of course, the FBI knew not just of the *absence* of evidence suggesting any foreign connection; the FBI knew the laptop was real.⁵²



This internal Facebook document directly conflicts with the deposition testimony FBI Special Agent Elvis Chan provided in this case. Chan testified that he was “confident” that he “was not a party to any meeting with social media companies where Hunter Biden was discussed outside of the [October 14 FITF-Facebook meeting where Laura Dehmlow responded ‘no comment’].”⁵³ Later, when asked if, other than the October 14 FITF-Facebook meeting, he was “aware of any communications

⁵¹ *Id.* Chan testified in his deposition that, unlike Dehmlow, FITF Section Chief Bradley Benavides, the Russia Unit Chief of FITF, and other FITF personnel, he did not know prior to October 14 that the FBI had the laptop. *Cf.* Chan Deposition, *supra* note 40, at 230:7–19; Ex. 14 (Laura Dehmlow Transcribed Interview), at 37.

⁵² Jordan, *supra* note 27; Ex. 14 (Laura Dehmlow Transcribed Interview), at 37.

⁵³ *Cf.* Chan Dep., *supra* note 40, at 215:22–216:16; Ex. 18 (Entry on internal Facebook case file by Facebook employee (Oct. 15, 2020)).

between anyone at Facebook and anyone at the FBI related to the Hunter Biden laptop story,” Chan responded, “No.”⁵⁴

As a result of the FBI’s withholding critical information the day of (and the days after) the *New York Post*’s article was published, the social media companies began to do precisely what the FBI intended: suppress truthful First Amendment-protected speech less than three weeks before the presidential election.⁵⁵ The story implicating one of the two major party candidates was blocked by Twitter and de-amplified by Facebook, “significantly reducing its circulation and prevalence in users’ newsfeeds.”⁵⁶ All because the FBI—an organization that the companies felt compelled to follow—had led them to believe the laptop story was Russian disinformation.⁵⁷ The story was not Russian disinformation, and FBI personnel meeting with Twitter and Facebook knew *at the time* that it was not Russian disinformation.⁵⁸ This government coercion of the marketplace of ideas undoubtedly affected the 2020

⁵⁴ Chan Dep., *supra* note 400, at 233:22–234:3.

⁵⁵ Jordan, *supra* note 27.

⁵⁶ *Id.*

⁵⁷ FBI Director Wray testified that “the FBI is not in the business of moderating content or causing any social media company to suppress or censor” speech. Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary, 118th Cong. (July 12, 2023). On July 18, Chairman Jordan and Representative Mike Johnson, Chairman of the Subcommittee on the Constitution and Limited Government, wrote a letter to Director Wray providing him the opportunity to amend his testimony. Director Wray has not responded.

⁵⁸ Jordan, *supra* note 27.

election.⁵⁹ The district court’s findings that the federal government unlawfully coerced private speech are amply supported by the evidence.

III. The United States has coerced speech about elections.

The United States also flouted the First Amendment by coercing election-related speech. This coercion is especially troubling because speech pertaining to elections “occupies the core of the protection afforded by the First Amendment.” *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 346 (1995). Yet the federal government has repeatedly coerced social media companies to censor election-related speech. It has done so directly, through DHS’s Cybersecurity and Infrastructure Security Agency (CISA), and indirectly, through the private-sector Election Integrity Partnership (EIP). Following revelations from this lawsuit and the ongoing investigation by the House Judiciary Committee and Weaponization Subcommittee, CISA has taken steps to cover-up and hide its efforts to surveil and censor domestic speech.⁶⁰

⁵⁹ See Miranda Devine, *Media Helped Hide the Real Joe Biden by Censoring Hunter Stories*, NEW YORK POST (Nov. 28, 2021), <https://tinyurl.com/mvp474ba>.

⁶⁰ STAFF OF THE H. COMM. ON THE JUD., 118TH CONG., INTERIM STAFF REPORT: THE WEAPONIZATION OF CISA, (available at <https://bit.ly/45jYPke>) [hereinafter Interim Staff Report] (filed below as ECF 291-2).

A. Cybersecurity and Infrastructure Security Agency (CISA)

Congress established CISA in 2018 to “lead cybersecurity and critical infrastructure security programs, operations, and associated policy.”⁶¹ Shortly after the 2016 election, DHS Secretary Jeh Johnson designated “election infrastructure” as a “critical infrastructure subsector.”⁶² CISA’s “Countering Foreign Influence Task Force” (CFITF) focuses “on election infrastructure disinformation.”⁶³ But in an effort to expand its focus on foreign misinformation to domestic misinformation, “CISA transitioned its [CFITF] to promote more flexibility to focus on general MDM,” or so-called “Mis-, Dis-, and Malinformation.”⁶⁴

CISA’s focus on so-called “malinformation” is particularly alarming. According to CISA, “[m]alinformation is based on fact, but used out of context to mislead, harm, or manipulate.”⁶⁵ Put more plainly, “malinformation is *factual* information

⁶¹ 6 U.S.C. § 652.

⁶² Press Release, Dep’t of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), <https://tinyurl.com/2xt3twjd>.

⁶³ OFFICE OF INSPECTOR GEN., DEP’T OF HOMELAND SEC., OIG-22-58, DHS NEEDS A UNIFIED STRATEGY TO COUNTER DISINFORMATION CAMPAIGNS 5 (Aug. 10, 2022), <https://tinyurl.com/2p9h2p75>.

⁶⁴ *Id.* at 7.

⁶⁵ CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, MIS-, DIS-, AND MALINFORMATION PLANNING AND INCIDENT RESPONSE GUIDE FOR ELECTION OFFICIALS 1 (2022), <https://tinyurl.com/52pvpn5d>.

that is objectionable not because it is false or untruthful, but because it is provided without adequate ‘context’—context as determined by the government.”⁶⁶

In his deposition, Brian Scully, the first head of the CFITF and later the head of the MDM team at CISA,⁶⁷ said that CISA engaged in “switchboarding,” where CISA would flag alleged disinformation to social media platforms.⁶⁸ According to Scully, “switchboarding” involves CISA officials first receiving alleged “misinformation” reports from election officials and then forwarding those reports to social media companies so that they could take enforcement measures against the reported content.⁶⁹ Scully admitted that CISA was aware that its outreach to social media companies about alleged misinformation would trigger content moderation.⁷⁰

CISA also funded and utilized third parties, such as the Center for Internet Security (CIS), to achieve these aims. CIS is the nonprofit entity responsible for operating the Multi-State Information Sharing and Analysis Center (MS-ISAC) and

⁶⁶ INTERIM STAFF REPORT, *supra* note 600, at 10.

⁶⁷ Deposition of Brian Scully, 11:19–12:6, (available at <https://tinyurl.com/2epb2mw9>) (filed below as ECF No. 209-1).

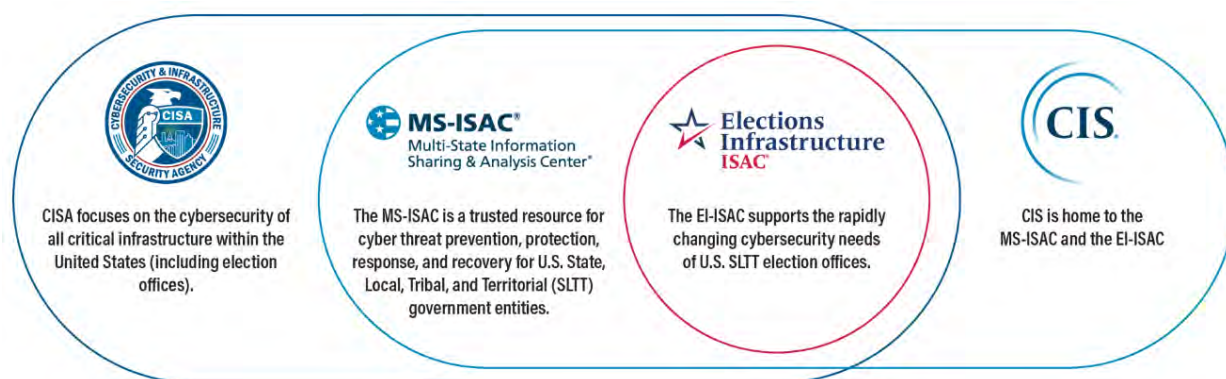
⁶⁸ *Id.* at 23:16–24:2.

⁶⁹ *Id.* at 17:1–18:1.

⁷⁰ *Id.* at 17:15–18:1. In response to a question from Representative Dan Bishop, DHS Secretary Mayorkas testified that he believed that “it is true” that “CISA does not flag anything to social media organizations at all,” but that he would “verify that.” Oversight of the Department of Homeland Security: Hearing Before the H. Comm. on the Judiciary, 118th Cong. (July 26, 2023). Secretary Mayorkas has failed to provide the Judiciary Committee with any information to verify his testimony.

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).⁷¹ The EI-ISAC allows election officials around the country to send alleged “misinformation” to CIS, which CIS then forwards to the relevant social media platforms.⁷²

As illustrated by the diagram below from CIS’s website, the “EI-ISAC is federally funded by CISA and a division of the Center for Internet Security.”⁷³ CISA requested \$27 million in FY 2024 funding CIS to operate the EI-ISAC and the MS-ISAC.⁷⁴



Illustrating that claims of “misinformation” are inherently political, the CISA-funded EI-ISAC facilitated attempts to censor core political speech. For example, a state government official working for Pennsylvania’s Secretary of State, a Democrat, reported to the EI-ISAC posts on Twitter and Facebook from Senator Ted Cruz’s

⁷¹ CENTER FOR INTERNET SEC., *EI-ISAC*, <https://tinyurl.com/36cny5pu> (last visited Aug. 7, 2023).

⁷² *Id.*

⁷³ *Id.*

⁷⁴ DEP’T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY OPERATIONS AND SUPPORT FISCAL YEAR 2024 CONGRESSIONAL JUSTIFICATION 73 (2023) (available at <https://tinyurl.com/5n72k25h>); *see also* INTERIM STAFF REPORT, *supra* note 60, at 7–8.

accounts.⁷⁵ In the offending post, Senator Cruz, a Republican, asked: “Why is it only Democrat blue cities that take ‘days’ to count their votes? The rest of the country manages to get it done on election night.”⁷⁶ Emblematic of this “switchboarding,” the federally funded EI-ISAC forwarded the report to Facebook.⁷⁷

B. The Election Integrity Partnership (EIP)

The United States, primarily CISA, also coerced social media companies into censoring speech about the 2020 election through the private-sector Election Integrity Partnership (EIP), led by Stanford University. Formed in the summer of 2020, EIP was a coalition of research entities created “in consultation with CISA and other stakeholders”⁷⁸ and “united government, academia, civil society, and industry, analyzing across platforms, to address misinformation in real time.”⁷⁹ Emails obtained by the House Judiciary Committee and Weaponization Subcommittee confirm that CISA officials were involved with EIP from the very beginning.⁸⁰

⁷⁵ Ex. 19 (E-mail from misinformation@cisecurity.org to Facebook employees (Oct. 27, 2022, 5:06 PM)).

⁷⁶ Sen. Ted Cruz (@tedcruz), TWITTER (Oct. 27, 2022, 12:34 PM), <https://tinyurl.com/2s9dce95>.

⁷⁷ Ex. 19 (E-mail from misinformation@cisecurity.org to Facebook employees).

⁷⁸ ELECTION INTEGRITY P’SHIP, *The Long Fuse: Misinformation and the 2020 Election 2* (2021), <https://tinyurl.com/4frucxab> [hereinafter EIP].

⁷⁹ *Id.* at 241.

⁸⁰ Ex. 20 (E-mail from Kate Starbird to Alex Stamos (July 8, 2020, 10:26 AM)).

Because the four entities comprising EIP were not government entities,⁸¹ the United States sought to use EIP to do things that the government could never do without violating the First Amendment—namely, directly monitoring and censoring speech. By its own account, EIP filled the “gap” in the government’s ability to police so-called “misinformation” and “disinformation” about elections on social media because “no government agency in the United States has the explicit mandate to monitor and correct election mis- and disinformation.”⁸²

EIP used the Jira Service Desk, a ticketing software to allow approved entities (government agencies, EI-ISAC, and others) to submit “misinformation” reports, creating a “Jira ticket.”⁸³ From there, EIP personnel analyzed the submission and could comment on the ticket, before a manager would assess whether to forward the ticket to the relevant social media platform(s).⁸⁴ EIP’s final report illustrates this workflow⁸⁵:

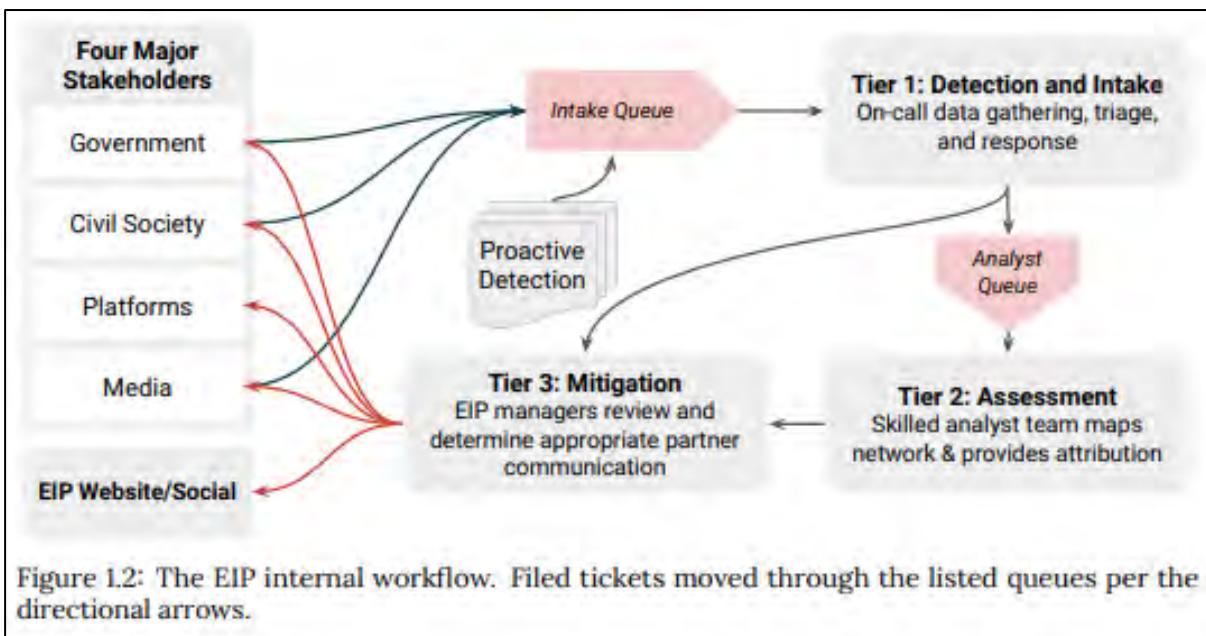
⁸¹ Stanford Internet Observatory, the University of Washington’s Center for an Informed Public, the Atlantic Council’s Digital Forensics Research Lab, and Graphika.

⁸² EIP, *supra* note 78, at v, 2.

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*



EIP was thoroughly intertwined with CISA, which aided EIP in the process of reporting undesirable election-related speech to social media platforms.⁸⁶ Stanford confirmed in a recent letter to Chairman Jordan that CISA was directly “tagged” in a number of Jira tickets “rather than or in addition to” the CISA-funded EI-ISAC.⁸⁷ Other documents obtained by the House Judiciary Committee and Weaponization Subcommittee confirm CISA’s involvement.⁸⁸

The FBI, the National Security Agency (NSA), and the Global Engagement Center (GEC) were also involved. The GEC is a federal government interagency organization housed at the State Department with the stated mission of countering

⁸⁶ *Id.* at 13.

⁸⁷ Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 27, 2023) (on file with the H. Comm. on the Judiciary).

⁸⁸ Ex. 21 (E-mail from Elena Cryst to TikTok employee (Nov. 4, 2020, 7:41 PM)); Ex. 22 (E-mail from Reddit employee to Alex Stamos (Nov. 3, 2020, 12:36 PM)).

foreign “propaganda and disinformation efforts.”⁸⁹ Most notably, the GEC submitted tickets to EIP through Jira.⁹⁰ Stanford recently confirmed to the Committee that social media platforms could see which entity submitted a ticket, including federal government entities.⁹¹ In addition, before the 2020 election, EIP briefed the NSA, and sent one Jira ticket to the FBI.⁹²

The EI-ISAC, federally funded and operated by CIS and CISA, also submitted tickets.⁹³ CISA even coordinated “an agreement” between CIS and EIP to avoid double reporting.⁹⁴ The two admittedly became “partners,”⁹⁵ sharing personnel.⁹⁶ Information obtained to date during the House Judiciary Committee and

⁸⁹ U.S. DEP’T OF STATE, *About Us—Global Engagement Center*, <https://tinyurl.com/43dmawd9> (last visited Aug. 4, 2023); *see also* Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), <https://tinyurl.com/3pmhu8j6> (“GEC’s ‘Chinese’ list included multiple Western government accounts and at least three CNN employees based abroad.”).

⁹⁰ *See, e.g.*, Ex. 23 (E-mail from Elena Cryst to Google employee (Nov. 2, 2020, 7:03 PM)).

⁹¹ Letter from John B. Bellinger III to the Hon. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 7, 2023) (on file with the H. Comm. on the Judiciary).

⁹² Ex. 24 (Excerpts of Transcribed Interview of Alex Stamos before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 23, 2023)).

⁹³ *Id.* at 114–115.

⁹⁴ *Id.* at 212:07–12.

⁹⁵ *Id.* at 369:01–11.

⁹⁶ *Id.* at 168:22–171:16, 183:20–22.

Weaponization Subcommittee’s investigation confirms that the government-funded EI-ISAC submitted over 100 Jira tickets in the lead-up to the 2020 election.⁹⁷

This close affiliation with the federal government heightened the coerciveness of EIP’s interactions with social media platforms. EIP onboarded major social media platforms, gaining privileged access to some of these platforms’ data and the ability to collect such data in real-time.⁹⁸ EIP’s direct recommendations for censorship resulted in the suppression of disfavored speech about the 2020 election.⁹⁹ Thirty-five percent of the URLs EIP “shared with Facebook, Instagram, Twitter, TikTok, and YouTube were either labeled, removed, or soft-blocked.”¹⁰⁰ Every Twitter account holder EIP identified as a “Repeat Spreader” of election-related “disinformation” expressed “conservative or right-wing political views.”¹⁰¹

EIP’s election-speech monitoring did not end with the 2020 election. EIP recreated itself for the 2022 election and may again for the 2024 election.¹⁰²

⁹⁷ Letter from John B. Bellinger III to the Hon. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023) (on file with the H. Comm. on the Judiciary).

⁹⁸ EIP, *supra* note 78, at 17, 181–82; *see* Ex. 22 (E-mail from Reddit employee to Alex Stamos).

⁹⁹ *Cf.* Ex. 22 (E-mail from Reddit employee to Alex Stamos); STANFORD INTERNET OBSERVATORY, *Background on the SIO’s Projects on Social Media* (Mar. 17, 2023), <https://tinyurl.com/3x4ys8me> (“EIP did not make recommendations to the platforms about what actions they should take.”).

¹⁰⁰ EIP, *supra* note 78, at 27.

¹⁰¹ *Id.* at 187–88.

¹⁰² Ex. 24 (Alex Stamos Transcribed Interview).

The United States’ coercive tactics with social media platforms to quell election-related messages it finds undesirable are unconstitutional—even when funneled through a private-sector entity. *See Norwood v. Harrison*, 413 U.S. 455, 465 (1973) (“[A] state may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish.” (cleaned up)).

CONCLUSION

For these reasons, and to vindicate the First Amendment’s promise of a marketplace of ideas free from government meddling, the Court should affirm the preliminary injunction.

Respectfully submitted,

GENE P. HAMILTON
America First Legal Foundation
611 Pennsylvania Ave. SE #231
Washington, D.C. 20003
(202)964-3721
gene.hamilton@aflegal.org

s/ Christopher Mills
CHRISTOPHER MILLS
Spero Law LLC
557 East Bay Street #22251
Charleston, SC 29413
(843) 606-0640
cmills@spero.law

Counsel for *Amici Curiae*

AUGUST 7, 2023

CERTIFICATE OF COMPLIANCE

1. This document complies with the type-volume limit of Fed. R. App. P. 29(a)(5) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this brief contains 6,496 words.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this document has been prepared in a proportionally spaced typeface using Microsoft Word 365 in 14-point Times New Roman font.

3. This document has been scanned for viruses and is virus-free.

Dated: August 7, 2023

/s Christopher Mills
Christopher Mills

CERTIFICATE OF SERVICE

I, Christopher Mills, an attorney, certify that on this day the foregoing Brief was served electronically on all parties via CM/ECF.

Dated: August 7, 2023

s/ Christopher Mills
Christopher Mills

APPENDIX

INDEX OF EXHIBITS

EXHIBIT NUMBER	TITLE
1	E-mail from Nick Clegg to Facebook employees (July 14, 2021, 11:46 AM)
2	E-mail from Facebook employee to Facebook employees (Apr. 27, 2021, 11:58 AM)
3	E-mail from Nick Clegg to Facebook employees (Apr. 19, 2021, 9:40 AM)
4	Facebook employee's notes of a call between White House personnel and Facebook employees on March 26, 2021
5	Facebook employee's notes of a call between White House personnel and Facebook employees on April 14, 2021
6	Facebook employee's notes of a call between White House personnel and Facebook employees on April 5, 2021
7	Facebook employee's notes of a call between White House personnel and Facebook employees on June 15, 2021
8	E-mail from Facebook employee to Facebook employees (July 16, 2021, 8:14 PM)
9	E-mail from Facebook employee to Facebook employees (Aug. 6, 2021, 7:13 PM)
10	E-mail from Nick Clegg to Facebook employees (Aug. 19, 2021, 5:25 PM)
11	E-mail from Facebook employee to Facebook employees (July 22, 2021, 12:17 PM)
12	E-mail from Sheryl Sandberg to Nick Clegg (July 21, 2021, 4:49 PM)
13	Facebook employee's notes of a call between Office of the Surgeon General personnel and Facebook employees on July 16, 2021

14	Excerpts of Transcribed Interview of Laura Dehmlow before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (July 17, 2023)
15	Excerpts of Transcribed Interview of David Agranovich before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (May 16, 2023)
16	Excerpts of Transcribed Interview of Nathaniel Gleicher before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 21, 2023)
17	E-mail from Facebook employee to Matthew Masterson and Brian Scully (Sept. 29, 2020, 11:41 AM)
18	Entry on internal Facebook case file by Facebook employee (Oct. 15, 2020)
19	E-mail from misinformation@cisecurity.org to Facebook employees (Oct. 27, 2022, 5:06 PM)
20	E-mail from Kate Starbird to Alex Stamos (July 8, 2020, 10:26 AM)
21	E-mail from Elena Cryst to TikTok employee (Nov. 4, 2020, 7:41 PM)
22	E-mail from Reddit employee to Alex Stamos (Nov. 3, 2020, 12:36 PM)
23	E-mail from Elena Cryst to Google employee (Nov. 2, 2020, 7:03 PM)
24	Excerpts of Transcribed Interview of Alex Stamos before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 23, 2023)

EXHIBIT 1

From: Nick Clegg [redacted]
To: [redacted]
CC: Brian Rice; [redacted]
Sent: 7/14/2021 11:46:33 AM
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

thx

From: [redacted] <[redacted]@fb.com>
Date: Wednesday, July 14, 2021 at 7:44 PM
To: Nick Clegg <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Cc: Brian Rice <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Because we were under pressure from the administration and others to do more and it was part of the "more" package. We removed four claims that multiple fact checkers had labeled false even though we didn't have a harm assessment. We shouldn't have done it. We stopped removing the man made claim in May and now we're moving the other three claims (covid is new/patented) from remove to reduce and inform.

From: Nick Clegg <[redacted]@fb.com>
Sent: Wednesday, July 14, 2021 11:41:56 AM
To: [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>; Brian Rice <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Can someone quickly remind me why we were removing – rather than demoting/labeling – claims that Covid is man made before May?

From: [redacted] <[redacted]@fb.com>
Date: Wednesday, July 14, 2021 at 5:32 PM
To: [redacted] <[redacted]@fb.com>, Nick Clegg <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>, Brian Rice <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Following up here (and replying on behalf of [redacted] as well who is presenting in another meeting): We worked to further streamline and simplify the talking point around the 12 people identified by the CCDH ('disinfo dozen'). We'd recommend using the following:

"People on the Center for Countering Digital Hate's list show up in multiple places across Facebook products: Facebook pages, Facebook groups, and IG accounts for example. If they repeatedly break our rules, we permanently remove that page, group, or account from our services, and we've done that in more than a dozen instances."

In case it's helpful for further context, the break-down of the entities we've removed associated with people

From: [REDACTED] <[REDACTED]@fb.com>
Date: Wednesday, July 14, 2021 at 8:04 AM
To: Nick Clegg <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Yes, we have said that publicly.

From: Nick Clegg <[REDACTED]@fb.com>
Date: Wednesday, July 14, 2021 at 7:50 AM
To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Ok – got it (I think) – can I cite your bullet point in blue on this (“entirely removed... more than a dozen” etc)? N

From: [REDACTED] <[REDACTED]@fb.com>
Date: Wednesday, July 14, 2021 at 3:42 PM
To: Nick Clegg <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

That is a good question. The “disinfo dozen” refers to 12 people. Many of those people have multiple presences on FB/IG. For example, RFK Jr. had a FB Page and IG account. We have removed the IG account but not FB Page, as he posts different content across those two presences and only the IG account has reached our threshold for removal.

From: Nick Clegg <[REDACTED]@fb.com>
Date: Wednesday, July 14, 2021 at 7:35 AM
To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Thx - now, for truly the most simplistic question...: if we've removed pages/accounts of a dozen individuals what's left on FB of the “disinfo dozen”?

N

Get [Outlook for iOS](#)

From: [REDACTED] <[REDACTED]@fb.com>

Sent: Wednesday, July 14, 2021 3:29:38 PM

To: Nick Clegg <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>

Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>;

[REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED]

[REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>

Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Thanks, Nick. See responses below in blue.

From: Nick Clegg <[REDACTED]@fb.com>

Date: Wednesday, July 14, 2021 at 4:38 AM

To: [REDACTED] <[REDACTED]@fb.com>

Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>

Subject: Re: Brief: 07.14.21 - Andy Slavitt Podcast

Thx, Just a few Qs:

- I don't understand the eg of "shedding" that we took action on?
Vaccine shedding is the term used to describe the release or discharge of any of the vaccine components in or outside of the body. We've seen people closing down their shops to people who have been vaccinated because of fears of shedding, to give just one example of how this claim is causing confusion and could contribute to hesitancy. Vaccine shedding can only occur when a vaccine contains a weakened version of the virus and occurs when a virus is released from an infected person. None of the Covid-19 vaccines cause any kind of shedding. None include living Covid-19 so it is impossible for vaccinated people to shed Covid-19 from the vaccine itself.

- The Q&A has Qs asking why we only took action on covid vaccine misinfo in Dec last year and Feb this year. Why these dates?

December 2020 is when we first announced we would be removing some false claims about Covid vaccines given the news the vaccines would soon be rolling out around the world. Before that we did not know what would be true or false about the vaccines. February 2021 is when we announced we would remove general vaccine misinformation (8 widely debunked claims, including vaccines cause autism).

- I find what we've actually done re the "disinfo dozen" v hard to follow. Any way to simplify that for me?

Center for Countering Hate's (CDDH) Disinformation Dozen

- We have removed violating content that these accounts have posted.
- We have entirely removed the Facebook Pages or Groups or Instagram accounts of more than a dozen of these individuals for repeatedly violating our misinformation policies. In other cases, we have restricted their activity (e.g. by not recommending their content).

N

From: [REDACTED] <[REDACTED]@fb.com>

Date: Wednesday, July 14, 2021 at 7:17 AM

To: Nick Clegg <[REDACTED]@fb.com>

Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>

Nick: Attached is an updated briefing for Wednesday's podcast interview. It now includes an overarching narrative and specific content examples you can cite. Please let us know if you have additional questions – the folks on this email can help to track down additional info.

Thanks,



PRODUCED TO HJC

EXHIBIT 2

From: [REDACTED] <[REDACTED]@fb.com>
Date: Tuesday, April 27, 2021 at 11:58 AM
To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Nick Clegg <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Vaccine Policy

+ Nick, [REDACTED]

Please see a draft note for Mark and Sheryl with 3 stronger enforcement options against vaccine discouraging content [here](#) (and copied below as well) further to the discussion with Mark last week. Let us know if any feedback or if there's anything missing here.

Thanks so much,

Subject: [For Decision] Vaccine discouraging content

Mark, Sheryl:

We are seeking your guidance on whether to take more aggressive action against certain vaccine discouraging content.

We are facing continued pressure from external stakeholders, including the White House and the press, to *remove* more COVID-19 vaccine discouraging content. For example, we recently shared with the White House a list of the [top 100 vaccine-related posts on FB in the U.S. for the week of 4/5-4/11](#). While authoritative information dominated the list, the White House was concerned that the #3 post was a [vaccine discouraging humorous meme](#), and they called on us to delete the meme.

We currently *remove* content that includes certain misinformation about covid and vaccinations (e.g., the covid vaccine has microchips) and content that explicitly discourages vaccination (e.g., the COVID-19 vaccine is too dangerous - don't get it!). Under our policies, this meme should not be removed.

Instead, we aim to *reduce* this sort of vaccine discouraging content, namely 'sensational or alarmist content' (e.g., there's no point vaccines are useless!; vaccines are the work of the devil; these vaxx are so bad for your body!) and 'criticism of personal vaccine choices' (e.g., it's child abuse to give your kid the vaccine; you'd have to be a complete moron to get vaccinated).

To reduce this content, we are currently building systems to review & demote on escalation, and over time hope to have demotions at scale through classifiers (although that kind of scaled enforcement is likely to be challenging). We are not convinced we'll be able to catch all kinds of this content quickly enough before it gains some distribution. Additionally, given people's interest in the topic, weaker demotions may not be sufficient to meaningfully limit the distribution of posts.

Based on consultations with vaccination communication experts and other health partners, we worry that removing (as opposed to demoting) more expressions of vaccine hesitancy might be counterproductive to the goal of vaccine uptake, because it would: 1/ prevent hesitant people from talking through their concerns online and 2/ reinforce the notion that there's a cover-up (a key prong of anti-vaccine narratives). Details of feedback from external experts and research are below.

We seek your guidance on how to treat this vaccine discouraging content. Here are the options:

1. 25% demotion (current plan, execution under way)
2. ~50% demotion, or even stronger (e.g., 80%) if we find that 50% isn't sufficient to keep such content out of top vaccine posts
3. Remove this content

Details below.

Thanks,

A. Definitions of the Vaccine Discouraging Content in Question

1. Sensational or Alarmist Vaccine Content: Content that otherwise does not violate our COVID-19 or vaccine policies above but that suggests that vaccines are unsafe, ineffective, sacrilegious or irrelevant, in exaggerated, conspiratorial, or sensational terms. This includes content that makes generalizations about vaccine harms or utility in hyperbolic terms or without providing context, or which connects vaccination to a conspiratorial narrative about a purposely hidden widespread health harm, secret, or truth.
 - a. Ex: "They're coming with these dangerous shots for you next -- the sheep of the world need to wake up."
 - b. Ex: "Vaccines are the work of the Devil"
 - c. Ex: "These VAXX are so bad for your body!"
 - d. Ex: "Vaccines are so useless, what's the point!"
 - e. Ex: "I need to detox my kid to get these vaccine toxins out...Any ideas?"
2. Criticizing the Choice to Receive/Provide Vaccines: Content that otherwise does not violate our COVID-19 or vaccine policies above but that disparages others on the basis of their choice to get vaccinated, or on their choice to vaccinate others, including attacking language used towards vaccinated people or those administering vaccinations, or blaming people for misfortune after vaccination.

- a. Ex: "You're committing child abuse for giving this vaccine."
- b. Ex: "Only someone clinically insane would get this vaccine!"
- c. Ex: "Any extreme pro-vaxers unfriend me. You are a danger to public health you thick, unscientific twats"
- d. Ex: "I can't believe they got vaccinated, what idiot sheeple"
- e. Ex: "Take a look around people -- anyone who gets these experimental vaccines is just a guinea pig."

B. Options for Addressing Severe Vaccine Discouraging Content

1. **25% demotion** ← *plan of record, still need to execute* - consistent with the Integrity Ranking Guidelines (IRGs), we can demote by 25%. We are just beginning to do this.
 - a. *Pros*: slows distribution of such content; consistent with normal practice for demoting problematic content without specific user notice/appeals
 - b. *Cons*: unsatisfactory to certain critics who want us to take even stronger action; some demoted content may still go viral
2. **~50% demotion**, or even stronger (e.g., 80%) if we find that 50% isn't sufficient to keep such content out of top vaccine posts
 - a. *Pros*: may satisfy some critics who want more aggressive action; significantly reduces virality of vaccine discouraging content
 - b. *Cons*: inconsistent with normal practice for demoting problematic content without specific user notice/appeals; could be seen as shadowbanning
3. **Remove**
 - a. *Pros*: may satisfy certain vocal critics; best option to reduce virality
 - b. *Cons*: removes true content and personal opinions; reduces public conversation on important issue; provides "evidence" to people who believe FB is overly censorious or participating in vaccine cover-ups

C. External Perspectives on Removing More Vax Hesitancy Content

Since 2018, we have consulted extensively with external experts about our approach to vaccine content on Facebook and our engagement has stepped up significantly during the COVID pandemic. We have received varied responses on what the right approach is when it comes to removal and have modest confidence in our current approach. Some key health partners, including the WHO, continue to advocate for removing much more content. **The WHO has communicated to us that they think our current policies are not comprehensive enough** especially when it comes to takedowns of entities that they believe we should be removing due to the harmful impact they have on vaccine confidence (and, in turn, ending the pandemic). As mentioned above, the White House also continues to put significant pressure on removing more.

However, many vaccine communication experts seem to think we are now in the right place in terms of policy-writing about what content we remove vs. reduce. **Among these experts, there is a general sense that deleting more expressions of vaccine hesitancy might be counterproductive to the goal of vaccine uptake, because it would: 1/ prevent hesitant people from talking through their concerns and 2/ reinforce the notion that there's a cover-up (a key prong of anti-vax narratives).** These risks seem particularly acute now in the US, because we are quickly approaching the point of supply exceeding demand and remaining vaccine holdouts being due to genuine hesitancy. Some experts have voiced the value in hesitant people being able to seek answers to their questions and having their concerns addressed. There may be risk of pushing them further toward hesitancy by suppressing their speech and making them feel marginalized by large institutions.

Prior external research on effective interventions to address vaccine hesitancy highlights the critical importance of facilitating open dialogue, especially dialogue that is or that can be tailored to the individual or their communities. Research suggests that attitude change happens when people get a chance for productive discourse and addressing people's concerns head on (rather than reducing chances for conversation) can lead to positive change. **Opening up a chance for people to express their hesitancy, criticism and concerns can serve as an important way for them to access information.** Moreover, past on-platform network research has suggested that there is likely to be a backlash from taking down conspiracy-oriented networks' content, though in light of lessons learned we may be better equipped to handle it with our tools than we have previously.

Consistent with this reasoning, in March, the Washington Post Editorial Board published a piece titled, "Banning vaccine-hesitant posts is not the way to ease people's fears" which made the case that removals (and broad, strong demotions) would be counterproductive: "**sweeping takedowns or down-rankings of all borderline content could foster more misgiving, and deprive people of the opportunity to discuss and learn.**"

Our conversations with experts informed the creation of the "Barriers to Vaccination (B2V): Vaccine Content Quality Integrity Framework" (from which we excerpted the definitions above), and we've since vetted this framework with outside experts. Of note, in early March, we discussed our planned approach with members of the "High Level Panel on Vaccine Confidence & Misinformation" (organized by London School of Hygiene and Tropical Medicine and the Center for Strategic and International Studies). Key take-aways:

- **The panel had very positive feedback for our framework, calling it "sophisticated and nuanced."** They appreciated that the B2V work addresses a critical gray zone of content that may contribute to vaccine hesitancy.
- **The Panelists highlighted the importance of avoiding unintended consequences that may be associated with squashing expression on the platform.**
- **Experts underscored that they would be very hesitant about removing content that leads users to discuss vaccines.** They expressed concern around stifling healthy debate about the vaccines, especially with regard to the sharing of personal vaccine anecdotes or other vaccine discussion and debate. For example, some pointed to the importance of facilitating open conversation online between parents whose children experienced adverse effects from the COVID vaccine.

While thinking through our policies, we also recently met with **Heidi Larson, the head of the Vaccine Confidence Project**. Heidi's general **view is that we need to create an open and safe space for people to have vaccine-related conversations**. She believes we need to hear about people's fears and anxieties related to the vaccine and respond appropriately (not just throw facts at people but understand there is an emotion behind people's claims and questions). We met with Heidi again on 4/26 to check in on whether our approach to content expressing vaccine hesitancy was still in the right place. While acknowledging that it's a complicated time due to recent discouraging safety events, **she continues to support not removing this content** due to the aforementioned potential inadvertent effects of removing this kind of content and is happy to be a spokesperson for us.

D. Content Examples

A. Content we REMOVE

Violating Misinformation & Harm ← REMOVE

EXHIBIT 3

From: Nick Clegg [redacted]

Sent: Mon 4/19/2021 9:40:45 AM (UTC-07:00)
Subject: Re: A/C PRIV White House/Covid

Yep that is of course right: identify the gaps in their views and our policies (incl via feedback from the researchers they've been listening to); identify whether there really are such significant gaps between our approach and YT's; see what further steps we can take.

N

From: [redacted] <[redacted]@fb.com>
Date: Sunday, April 18, 2021 at 7:30 PM
To: Brian Rice <[redacted]@fb.com>, Nick Clegg <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Subject: RE: A/C PRIV White House/Covid

AC PRIV:

As frustrating as these fake leaks and innuendo are (and they are!), my thoughts are that we should not let that distract us from the real issues here, which are the substance. Clearly we have a policy viewpoint gap with them we need to figure out perspectives on – what we believe violates and what they think does... and the belief that YT is doing better than us, which I find so hard to believe. Probably best to spend our effort here and not get sucked into this other thread.

At the end of the day, unless we get to a common ground on what we're doing on substance, the rest doesn't really matter.

From: Brian Rice <[redacted]@fb.com>
Sent: Sunday, April 18, 2021 7:05 PM
To: Nick Clegg <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Subject: Re: A/C PRIV White House/Covid

Thanks Nick. This is obviously very disheartening to read. Rob made an offhand comment about conversations with "other people from Facebook" during a recent conversation, this is clearly what he was referencing. Because of his history in the digital campaign world, it's not surprising that he'd have relationships with some of our employees. It's disheartening and unfortunately no longer surprising to read that our colleagues would portray our conversations this way. I haven't been part of any conversation that includes disparaging remarks made about Andy, or about any strategy to snow the White House — the only disparaging remarks I've heard people make on our calls have been in reference to the disrespectful tone Rob uses with employees at Facebook.

All of that said—Andy's challenge feels very much like a crossroads for us with the White House in these early days.

Get [Outlook for iOS](#)

From: Nick Clegg <[redacted]@fb.com>
Sent: Sunday, April 18, 2021 9:07:34 PM
To: Brian Rice <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Subject: A/C PRIV White House/Covid

Just got off hour long call with Andy Slavitt. There are some pretty serious – and sensitive (see last point) - issues we need to address. A summary:

• He was appreciative of the data we sent thru on Friday, and confirmed that Rob F had said that they had never received so much data from us before.

BUT:

- Andy attended a meeting of misinfo researchers (didn't provide names) organized by Rob F on Friday in which the consensus was that FB is a "disinformation factory", and that YT has made significant advances to remove content leading to vaccine hesitancy whilst we have lagged behind.
- Whilst appreciative of our emphasis on authoritative vaccine, the principal focus for Andy S and his team in the coming weeks is to reach the "hardest to reach" people who have a propensity to consume vaccine hesitant related content and who are not swayed by official/authoritative sources of content. Our systems, he believes – as confirmed by the researchers – feed vaccine hesitant related content to pockets of the population and that's the problem he wants our help to resolve.
- As an eg, he was outraged – not too strong a word to describe his reaction – that we did not remove this post which was third most highly ranked post in the data set we sent to him:
<https://www.facebook.com/td.mccomas/posts/4106421952731017> I countered that removing content like that would represent a significant incursion into traditional boundaries of free expression in the US but he replied that the post was directly comparing Covid vaccines to asbestos poisoning in a way which demonstrably inhibits confidence in Covid vaccines amongst those the Biden Administration is trying to reach. [It would be very helpful if someone could please check whether this content was also available on YT – Andy's assumption is that YT would never accept something like this]
- V worryingly, towards the end of the conversation, Andy told me in confidence – so please treat it as such – that internal FB employees are leaking to his team (I assume via Rob F) accounts of disobliging remarks made about both Andy and Rob by FB decision makers. Further, that those remarks are coupled with suggestions about how FB should "snow" the White House with info/data about authoritative Covid info in order not to share the most telling/helpful data about content which contributes to vaccine hesitancy. We then discussed the wider issue of trust – or the lack of it – between FB and the Biden team related to the events during the election and beyond, but needless to say I was shocked and embarrassed that somehow we are perceived to be behaving so unprofessionally.

We concluded that he would ask Rob F to share the data and policy recommendations from the researchers with us asap so that we could give a considered reply on further steps we may/may not be able to take. We agreed to speak again once that assessment has been made.

Given what is at stake here, it would also be a good idea if we could regroup to take stock of where we are in our relations with the WH, and our internal methods too.

Thx

N

From: Brian Rice <[REDACTED]@fb.com>
Date: Saturday, April 17, 2021 at 6:37 PM
To: Nick Clegg <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Email to Andy with report

Thanks Nick—here are some talking points that you can use if Andy raises Rob's questions:

How was this [Tucker Carlson] post not violative?

- while we remove content that explicitly directs people not to get the vaccine, as well as content that contains explicit misrepresentations about vaccines, we reviewed this content in detail and it does not violate those policies.

Moreover: you say reduced and demoted. What does that mean? There's 40,000 shares on the video. Who is seeing it now? How many? How effective is that?

- The video is receiving 50% demotion for seven days as it is in the queue to be fact checked

- Crowdtangle shows engagement not views, and a simple text search for "vaccine" in Crowdtangle doesn't have the same recall as our classifiers, i.e., doesn't include all of the posts about vaccines. The data that we provided doesn't include the Tucker Carlson video because our data pipelines don't populate that quickly – we provided data for the week before.

Why label this content with a generic "visit the covid information center" message?

- Our more granular label about vaccine safety says "COVID-19 vaccines go through many test for safety and effectively before they're approved". In light of the decision to pause the J&J vaccine, vaccine safety discussion evolved past "approval," and we were concerned that this was a confusing/irrelevant message to be applying to content discussion the decision to pause J&J without revoking approval. We temporarily reverted to a more generic message and are updating the more specific label for posts about vaccine safety to say "COVID-19 vaccines go through many tests for safety and effectiveness and then are monitored closely" to try to adapt to the changing factual situation and evolving discussion.

From: Nick Clegg <[REDACTED]@fb.com>
Date: Saturday, April 17, 2021 at 3:30 PM
To: Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Email to Andy with report

No time yet - I asked him to ping me when he wants to spk. If you want to jot down a few thoughts we Rob's Qs that's great but don't disturb your weekend unduly, I'm sure I can manage without too.

Get [Outlook for iOS](#)

From: Brian Rice <[REDACTED]@fb.com>
Sent: Saturday, April 17, 2021 12:05:37 PM
To: Nick Clegg <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Email to Andy with report

Nick—let us know if your call with Andy lands for a specific time this weekend? We aren't responding to Rob's questions over email but we can still get you some info in case Andy brings these up.

From: Nick Clegg <[REDACTED]@fb.com>
Date: Friday, April 16, 2021 at 9:07 PM
To: Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Email to Andy with report

Done – thx so much. N

From: Brian Rice <[REDACTED]@fb.com>
Date: Friday, April 16, 2021 at 5:53 PM
To: [REDACTED] <[REDACTED]@fb.com>, Nick Clegg <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Email to Andy with report

Nick—attached is the report to send with the email.

Date: Friday, April 16, 2021 at 8:12 PM

To: Nick Clegg <[redacted]@fb.com>, Brian Rice <[redacted]@fb.com>

Cc: [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>

Subject: Re: Email to Andy with report

Suggested update below to reflect that you said this to him in your last note: "I realize it may be of limited comfort at this moment, but this [Tucker Carlson post] was not the most popular post about vaccines on Facebook today. Our data is slightly lagging, and we'll get back to you with more detail on this specific post tomorrow. Right now, it appears that it probably was among the top 100 most-viewed vaccine posts. I'm including a few examples of posts that were more popular today at the end of this note."

From: Nick Clegg <[redacted]@fb.com>

Date: Friday, April 16, 2021 at 4:42 PM

To: Brian Rice <[redacted]@fb.com>

Cc: [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>

Subject: Re: Email to Andy with report

And you'll be answering the other points on the other thread with Flaherty? Would be good for me to have those for my call with Slavitt

Get Outlook for iOS

From: Nick Clegg <[redacted]@fb.com>

Sent: Friday, April 16, 2021 4:40:40 PM

To: Brian Rice <[redacted]@fb.com>

Cc: [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>

Subject: Re: Email to Andy with report

Yep fine - looking forward to getting the attachment I should send. N

Get Outlook for iOS

From: Brian Rice <[redacted]@fb.com>

Sent: Friday, April 16, 2021 4:34:31 PM

To: Nick Clegg <[redacted]@fb.com>

Cc: [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>

Subject: Email to Andy with report

Nick—

We are in final stages of approval for the report that will go to the WH tonight. Think best if you send to Andy with an email confirming you can talk this weekend—and I can forward to Rob.

Draft email below:

Andy,

Wanted to make sure to get this to you ahead of the weekend. We believe this is responsive to what you have asked us to do — namely to provide information on what we are seeing on the platform with respect to vaccine content, as well as the interventions we are deploying to counter misinformation. As I mentioned yesterday, our data is lagging and this covers the period 4/5 to 4/11. I don't yet have a more specific answer on the Tucker Carlson post.

This probably goes without saying, but I want to make sure to convey that this is not information we normally share, and this data set is not cleanly vetted according to an integrity process that would take much longer to conduct. We took your cue the other day that it was important to get this to you quickly even if not polished. We have not made this information public and we hope to continue to be able to share with you and the team under confidence.

We hope we can continue to engage on the content provided here, and we're happy to schedule time next week to discuss with the team.

Look forward to talking this weekend.

PRODUCED TO HJC

Sign Up

Email or phone

Password

Log In

Forgot account?

 **Timothy McComas**
April 4, 2021 ·

UH OH !!!!

10 years from now you will be watching TV and hear....



19K 2 comments 385K shares

Share

English (US) · Español · Português (Brasil) · Français (France) · Deutsch

Privacy · Terms · Advertising · Ad Choices · Cookies · More

Meta © 2023

PROVIDED TO HJC

See more of Timothy McComas on Facebook

Log In

or

Create new account

CONFIDENTIAL TREATMENT REQUESTED

META-118HJC-0053337

EXHIBIT 4

3/26 White House Call Notes

Attendees: Roby Flaherty

Attendees (FB): Brian Rice, [REDACTED] [REDACTED]

- Brian – wanted to make sure we had time, we have a few things coming to you. We have an update to the symptom survey in a week. We could set up time to walk through the one you have, the new info. It's a different look, but useful, want to talk through
- Rob – useful, especially from comms folks
- Brian – will have more detail on demographics, should be improved. We also have data stuff from last week, want to center our work on universe of content. Nick told Andy that it will take some time to build, will have that ASAP. Today, wanted you to meet [REDACTED] our Product lead across all COVID defensive work. When Nick was talking to Andy about areas where we were unable to provide answers, [REDACTED] should be able to provide more information. She'll do an overview. We'll make sure to follow up on any questions.
- [REDACTED] – Hopeful for open confirmation, my job is focus on responding to immediate issues. I report to Guy. I'm jumping in midstream, may have some questions, I want to understand where we've been missing the mark, addressing gaps, see areas where we may not have direct answers but could look at proxies, other solutions. Want to understand problems, priorities going forward.
- Rob – sounds great. Maybe helpful to hear where we're coming from – we're concerned about FB impact on vaccine hesitancy, we see so often in data that people who are vaccine hesitant see on FB. Our theory is that content is harder to remove is doing the most harm, people are setting on the fence. We understand taking down that content is not best solution, for us, we want to understand if our theory is right, where you see what's driving vaccine hesitancy, what you are doingm how we can plug in and get you things. If you find things that are working, want to hear that. That's what we care about. We're not trying to screw you guys, we want to solve this problem. In 3 months, when there's a demand problem, we'll be in the barrel
- [REDACTED] – similar strategies –
 - Inform
 - Remove what's actually harmful
 - Reduce where there is hesitancy
- [REDACTED] – I know you want numbers, I don't have numbers yet on how interventions are working on, looking at proxies. Today – can sepak to levers, where are we reducing content, introducing reshare friction, have some things we can dig into. Nick mentioned we're looking at viral content, that's a metric we want to get you, but centralizing work – also looking at large entities, big groups, pages, big IG accounts. Last one is comments. One thing that's difficult – good post, bad comments, we see

that quite often. We see authoritative info from WHO having a lot of hesitancy comments. Top skepticism comments on those posts, don't

- Rob – so you're focused on virality, big entities like pages/groups, less on comments/posts between friends
- [REDACTED] – for the most part, right – the way we think about – head problem – where do we see hot spots – minority individuals/entities producing content that then gets redistributed. From prioritization perspective, that's how we know content will be redistributed/upranked/reshared. This is for hesitancy (not misinfo, which gets different treatment). We want to know overall hesitancy content, what are interventions. Detection methodology is dependent on topical conversations – that will take weeks, if not months. So in the interim, focused on the hot spots. Does that make sense?
- Rob – yes, makes sense. Do you have a tangible example? Done or seen is helpful.
- [REDACTED] – I asked the teams this morning – overall viral pieces of content – anecdotally, they've shared
 - Topics trending towards uncertainty – FDA approval v authorization – general confusion about that
 - Another one – concerns about vaccinated people shedding the virus to non-vaccinated people nearby – indirect
 - Have seen a lot of groups sharing individual stories about side effects or death after vaccination
 - If we're taking authoritative information – we could detect outright discouragement based on a reliable link, but it's harder to detect skeptical comments like "Oh, isn't that interesting." – we are working to be able to detect that, but we can't yet
- Rob – that makes sense. Fascinating. I'm curious – NY Post churning out articles every day about people dying. What is supposed to happen to that from Policy perspective. Does that article get a reduction, labels?
- [REDACTED] – Let's go back to remove (outright misinfo), reduce (not benign, more sensationalism, eg claim vaccines create miscarriages, indirect discouragement), inform – levers are contingent on content type, who posted it. We look at removing from recommendations, explorer, we want to take all this content out of that. E.g. Health Groups are non-recommendable, want to get them out of areas where we recommend or amplification systems. What we're prioritizing in feed – want to make sure that anything we suspect is hitting skepticism, harmful topically but we can't remove, we reduce. I don't have those numbers today.
- [REDACTED] – a lot of things get viral copy-pasted. We have a concept of introducing an inform interstitial – if I go to reshare post like that, have an interstitial noting that a post has been rated false by 3PFC. We can also do fwd limits. These are all methods we've used where there's not super clear lines in the sand. That's a suite of tools we're trying to apply right now.
- Rob – The question I have, if you're applying these methodologies, where is it still breaking through? And to whom? If it's still there, where is next whack a mole?

- [REDACTED] – big whackamole is that this all depends on our ability to detect. We're getting better at detecting things like the microchip thing and delete that. We're getting better at detecting (human, natural language processing) discouragement. We find COVID posts, then we identify posts that are explicit discouragement, or this is bullying for choosing to get vaccinated. What's hard right now, we haven't completed full detection path. We need to close gaps, that's what we're doing. The comments thing isn't solved, that's the big thing keeping me up at night, that I'm most worried about from an implementation perspective.
- Rob – so substantive problem is not that there are holes in the policy, it's more that the detection of things that needs more work
- [REDACTED] – the hard part is that what could be applicable to policy is moving, the timeline takes some time. Things are evolving on a discussion basis. This also gets harder as events evolve. For example, recent charges in Italy against two doctors and a nurse for administering Astra Zeneca vaccine. That creates a net new topic for our systems to need to be able to identify and get to intervention. That's why inform – driving to authoritative sources, CIC – that's why it's so important. Best way to resolve/educate individuals who aren't adversarially minded – compared to every real world event. Trying to get to fastest real solution v managing symptoms of having right information. I want to get a few minutes at the end to talk about next touch point. A lot of what I just said – there are also individuals that are adversarial, very good at following rules, know where the lines are, driving things off platform.
- Rob – I can go over 12:30 if you can. My question on inform – intellectually my bias is to kick people off. Inform, intellectually, maybe path of most impact. How are you measuring impact when you do inform? Is there secret sauce targeting that we can use? Stanford has suggested building targeting tools of people that engage with antivax content.
- [REDACTED] – This is where it gets into Offense side, this is what Emily was talking about. How do we measure success – are we getting people vaccinated. We have metrics around how many people we're informing, how quickly, how thorough. Are we identifying right content. Best directional metric is that symptom survey. We don't have a strong causative way of saying because integrity did X, we now see preventing growth – we don't see that. That's why we end up in education. If we're getting at do people have more information, are they better educated, that symptom survey is best we have right now.
- Rob – that survey, you are doing treatment survey
- [REDACTED] – real measure of success – did people go to center, did they read content, did that change perspective – broader integrity – unless someone tells us, hard to measure if we're changing hearts and minds, unless we do survey
- Rob – what are most successful inform interventions?
- [REDACTED] – only a few that are very topical based right now, don't have metrics now. People have concerns about methodology or safety on vaccines. We're in a test phase on broad COVID inform treatment that drives to FB/IG. There's a post, we put inform treatment driving directly to CIC. Not even about violating content – just broad swath.

That's the next big push of what we think might be a good inform treatment. In an ideal state, we want to get as precise as possible. The north star would be addressing each topic, but that degree of specificity might not be something we can ever get to. So trying to go broad and wide, with a big focus on the US. Trying to push out much more information given trends we're seeing.

- Rob – our public campaign, largely grants, fed govt not most trustworthy actor on vaccines – how can community organizations plug into FB in a way that will be maximally effective. Is there tooling that's coming online?
- [REDACTED] – I'd love to continue this conversation – I'm not a lawyer, know we have to be sensitive to personal information, targeting. In terms of targeting, one of the interesting trends we've seen in my own experience – local FB Groups – city, council, regional groups giving info about when new appts are available. I'm personally seeing local group community organizing. Might be an interesting thing to look at – how are communities having those conversations – something to explore further.
- Rob – to Brian's point, that's the next question – how can we plug in, how can we help. We're going to be a clearinghouse for ad campaigns, what can we bring to bear.
- [REDACTED] – Action items:
 - Chat more about how to do more targeted communication to vulnerable communities
 - Symptom survey
- Brian – we'll put a briefing on with Curtiss, our research director.
- [REDACTED] – we owe you a WA follow up
- Brian – we'll send that over – we'll take your queues – weekly, biweekly checkin makes sense, if you want to communicate on the fly with me and [REDACTED] we're open
- Rob – probably both – let's put check in on calendar
- Brian – ok great, we'll put on the calendar

EXHIBIT 5

4/14 Notes on Call with White House

WH Attendees: Rob Flaherty, Clarke Humphrey, Andy Slavitt (joined at 30 min mark)

FB Attendees: Brian Rice, [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

- Brian: Idea today was to follow up based on meeting next week, we have [REDACTED] on to talk to approach to getting authoritative information, [REDACTED] has some info from survey, then will go through metrics. Also want to be very clear, know you are interested in empirical information regarding success of interventions. Obviously want to get you what's helpful for you to do your job.
- [REDACTED] I need to understand a little bit. How I've interpreted – you're trying to find a causal link between someone not being exposed to vaccine hesitancy content, and therefore went out and got a vaccine. From a behavioral perspective, we don't see that. I want to make sure I understand what you're looking for. We can pull click through rates, other numbers, but want to confirm.
- Rob: Three things. We have to explain to President, Ron, people, why there is misinfo on the internet, bigger problem than FB. Where issues are, what interventions are, how well they are working, for products, want to engage in things that you know to be effective. I don't even care about specific methodology, you have better, richer data than we'll ever have. What are the things driving hesitancy on your platform? What is it? How big is the problem? When you are intervening, how are you measuring success? I say these things because candidly there is not a lot of trust towards FB, I need to know what theory of the case is, where we can be most effective. I am, personally, nervous, reported that there are interventions that have been done in other contexts, like NEQ score, that have been pulled back. Want to make sure that you're not finding things that are effective that you aren't doing.
- [REDACTED] That's helpful. In terms of what we're doing, we look at overall universe of content on FB, 1% is related to vaccines. Some subset of that is hesitancy, some is misinfo. We know as of March, 900,000 pieces of content was misinfo, 150,000 was US. Outside of that, numbers are really hard for us because hard to identify definitive vaccine hesitancy content. Very explicit example – 40% of Marines not taking vaccine – that's being presented as fact. People are questioning government. We're struggling to identify within hesitancy content, the stuff that's nefarious, the stuff that isn't. We don't know that if we removed everything, that it would alleviate external factors.
- Rob: The 40% of Marines, vaccine passports, good examples. J&J. To me, the one view I have – total interactions on CrowdTangle – you have more data about who is seeing it, where's it going. We don't want to be in a position where we take down bad news. But if your goal as a company is to make it more likely that people will get the vaccine. People don't see this in only one way. Is your presupposition to do these broad things without any sense. If you're seeing something that is factual that is that kind of news, it will have a negative way in a way that it wouldn't on other platforms.

- [REDACTED] We are thinking about it the same way, we have the same challenge. We can't ask news outlets to take down bad news. That's why flooding with good information is so important. There are people that might see NYT, other trusted sources, have hesitancy. Then there's the actual trusted communities – health agencies/government/experts/FB, family/friends/community. In my own life, hard to get my mom to take vaccine because she thinks she already had COVID and someone else should get it. That's a weird example, removing the content prohibits discussion. How do we tone down the fervor?
- Rob: Good question to be asking, you are a fervor machine.
- [REDACTED] In terms of interventions, know that there are groups that are hot spots – mandatory post approvals – admins have to approve posts. If violating content approved, gives the group a strike. I'm uncovering new examples on comments – public figures on comments might be contributing more. Tomi Lahren post on how she's not getting the vaccine. Even with comment reduction, still struggling if we reduce comments from public figures, Tomi Lahren makes a post.
- Rob: On what basis are you finding that the public figure comments have impact?
- [REDACTED] We don't have that causal link – we'd have to do a controlled study to expose people to misinformation or hesitancy content and study it. That's unethical. We can't measure that. I'd love to understand how you all are measuring that.
- Rob: I don't work at a company that profits on data. Hard for me to say. This is the whole problem. You guys are grading your own homework.
- Brian: No, working with Carnegie Mellon, we aren't seeing that.
- Rob: As a general practice on Facebook, you don't have a mechanism to test attitudinal impact?
- [REDACTED] The impact assessment is the survey data.
- [REDACTED] There's a difference between being able to set up a causal type test on our proactive measures to try to encourage vaccine uptake. The information we're putting out – we can roll out slowly and have some sense on whether it's having an impact on attitudinal measures and we do some of those tests. On the side of stuff that's misinfo, negative things propagating throughout the network. We don't have as easy an opportunity way to set up tests to determine whether people were a priori hesitant or not. We can do that for proactive work, we do research before we throw it out. For example, things we are sharing with communities of color, making sure not culturally insensitive. Work with organizations on brand lift tests. It's harder on the side of harmful content.
- Rob: If you were to change the algorithm so that people were more likely to see NYT, WSJ, any authoritative news source over Daily Wire, Tomi Lahren, polarizing people. You wouldn't have a mechanism to check the material impact?
- [REDACTED] That would require people being comfortable self-reporting change in intent to FB. One of the reasons the symptom survey is set up separately with Carnegie Mellon, UMD, because we're not under the impression that people
- Rob: But you cannot link product to that.

- [REDACTED] No, because the privacy rules in place, communicated to govt regulators, is that FB can't have the identifiable data to tie it back.
- Rob: If concern is measurable attitudinal effect, there's nothing to test persuasive material on FB. Brand Lift surveys are what you sell people.
- [REDACTED] We have the ability to do that for what FB or partners are communicating. Those are interventions that we can roll out, randomize through. When you're talking about content issues, there isn't independence of observation, material spreading through the network. SUTFA (?) violations there. Difficult to estimate causal effect. Ranking changes, given the small set of the population that we don't know ahead of time, means there is a lot of dilution, takes a lot of time to pick up that effect. Attitudes don't change immediately because of a ranking change. Have to allow time to take effect. If we made a change today, even with perfect experiment, would take a long time. And in pandemic time, we don't have that time.
- [REDACTED] That's why from product perspective, it's so important to look at mechanisms – if we can't remove it, at least we need to contain it.
- [REDACTED] one piece of circumstantial evidence – we're seeing declines in vaccine hesitancy in the US similar to the decline that Census/Pulsar data is seeing. Trying to serve best data possible with others making decisions based on it. The problem is not stagnant as far as hesitancy among US FB population. It's going down. Is it going down as fast as it could? I don't have an answer.
- Rob: Is it going down universally?
- [REDACTED] we have seen it go down among subpopulations. Are seeing a
- [Andy Slavitt is on the call at this point – 11:30 AM]
- [REDACTED] In Georgia, started talking about J&J halting earlier, we picked up an angle change there. Even across subpopulations, we aren't seeing it. We aren't measuring conservatives. We do look at counties and states, that are good proxies. We've been seeing things go down until recently.
- Andy: Apologize I missed some of the beginning. A few questions on the pieces I've seen so far- is there any spillover effect on attitudes from Pfizer or Moderna vaccines? What can you tell us about what people are saying about J&J? If people are spooked by the fact that there is a pause, I don't consider that misinfo, disinfo, or problematic. The vaccines are working on 9 figures of Americans. What bothers us is when data is obscured by people that mispresent it, knowingly or unknowingly. If people have legitimate concerns and questions, we want to be able to answer them. People are within their rights to react to news. We want to know the most effective way to respond to that. More broadly, feels like we're having a surprisingly tough time pinning down a plan of action of limiting the effects of people spreading misinfo on FB or WA. Question I asked 6 or 8 weeks ago – do we have or are we measuring the top, most shared negative sentiments? Are we measuring those over time? Are we taking the time to measure the impact of them? We've heard lots of conversation about other initiatives, a little bit of we can't do this, we can't do that. I just want to make sure that when we're frustrated, we're frustrated because we can't seem to get a straight answer to what feels like a very simple question.

- [REDACTED] Andy, nice to meet you, I'm the product lead. Going to try and work through your questions. [REDACTED] could you speak to J&J effects? I don't know that we have spillover measurements on Moderna and Pfizer?
- Andy: Perfectly reasonable you wouldn't have, if you could monitor over next few days, would be great.
- [REDACTED] On Moderna and Pfizer, based on guidance from Rob, trying to promote as much good as we can in CIC. [REDACTED] can speak to J&J.
- [REDACTED] Just quickly, because I think more important piece Andy is asking about is info diffusion on the platform. We are seeing an increase in vaccine hesitancy early states where media had more attention, e.g., Georgia shutting down J&J earlier, so far increase in hesitancy only in Georgia. People are giving more reasons about why they are hesitant – lack of trust in govt, not sure vaccine will work, people more interested in waiting to see if vaccine is safe. We're looking to see if we can match messaging to users to some of these concerns. For example, decline in trust in government – opportunity to push more local, authoritative people as spokespeople for information. Encouraging people not to wait and see. That doesn't answer spillover question, we'll get back to you if we have something reasonable to share that's good information.
- Andy: Don't wait to report to us to address spillover issues. Thank you for focusing on that. You can go onto the larger question.
- [REDACTED] Want to reanchor on where we seem three biggest forms of problems:
 - Minority - disinfo dozen – actively pushing to remove – their patterns of behaviors have started to shift to avoid policies – for example, they are using bitly links off platform. We're looking at all their identities and removing. Are they going to make mistakes so we can take them down? Vast minority of entities are actually maliciously intended.
- Andy: Clarifying q on that group – Have you limited ability to share?
- [REDACTED] Yes – we haven't explained that they are feature limited to them. Hard to detect content if not outright misinfo. We've taken other steps – removing amplification for Health Pages and Groups, but we don't want to remove good content or downrank re-education opportunities. Push and pull to calibrate.
- Andy: You don't have algorithms that can tell the difference?
- [REDACTED] Our detection classifiers can find outright misinformation
- Andy: Those are not shareable?
- [REDACTED] if we are able to identify and remove misinformation, if we can't remove, we reduce wherever we can.
- Andy: middle ground – how do you put caps on it.
- [REDACTED] three mechanisms
 - Where to put hard product features in place – e.g., mandatory post approval by admins – slows down
- Andy: Has that been done?
- [REDACTED] yes. Another example, want to slow down the rate at which content can be produced. Good posts have bad comments. We've rate limited the amount of comments to slow that down. Goes back to containing when we can't remove.

- Rob: This is a place where it's worth zooming in, where the rubber is meeting the road. What are you trying? How is it working?
- Andy: If you've done those things, can you measure the amount of shares of negative dis- or misinformation? Can you show us what those are? Last week it was 4%, this week it's 2%? That gives us a baseline. We recognize this is an ongoing battle. We don't know right now how big the battle is, whether we're winning or losing. Then we're able to not flail around and begin to focus with you on how to make it better. Is that possible to produce some kind of report?
- [REDACTED] Before you got here – we can pull raw numbers. Those will not necessarily correlate with attitudinal changes. Because this is real world, we will see the numbers fluctuate. For example, with J&J, may see spikes.
- Andy: So if you told me, we've gone from 3% to 2% but it hasn't changed attitudes. That's all we want; you control what you can control. Someday, there could be bad info about Pfizer, we have to answer honestly. FB isn't accountable for that. FB is accountable for people getting truthful, reliable information, not content that subtly changes. I just want to reinforce a lot of what Rob has been saying.
- [REDACTED] It would make a lot of our lives easier if when we delete content, we change minds. When we talk about constraint, that's the best thing we can measure. We've had a lot of policy conversations, don't want to go back to that. This is hard from technical and policy perspective. How to get the right information to the right people to get people vaccinated.
- Andy: Happy to think through challenges with you. Depends on who is sending message – in mainstream newspaper that's reliable, one thing, if comments that aren't, someone with a misleading story. Drudge report had a headline yesterday – 6/7 million cases of J&J have problem- total disaster. Together, someone coming on that news for the first time gets the intended effect.
- [REDACTED] In terms of scale, that would make me nervous too. The technical challenge, building
- Andy: We care about posts shared the most.
- [REDACTED] Can ask one question – what I'm hearing is – give us a better sense of raw numbers – those might flip and won't show sentiment. We want to hear what we can do better – for J&J – communities in rural areas, MI, potentially more likely to take J&J. I don't know the best way to go about reaching them. Would love to hear from your side how your campaign is reaching people so we can build into product.
- Andy: over long term, if you believe govt/expert agencies put transparency and safety first, will pay off. If people get accurate information, feel comfortable that someone watching backs. Worries about being rushed are not as true. Black community – got very good feedback from black physicians, black activists. At the same time, people in conservative community, just as we were getting people off the edge, now people more likely to say right all along. If people do their own homework, we ought to trust them. Not everyone will choose to get a vaccine. If people can make own decisions, we'll get over 80%. But worried about people being unduly influenced.
- [REDACTED] I just want to be clear that attitudinal shift data on misinfo doesn't exist.

- [REDACTED] With inform strategy, on J&J side, we tried to put risks in context. If there are other things you want to get out, we'd love to see that to help inform people.
- Rob: I obviously care about attitudinal shifts, matters to me. I still feel like I don't know what you are doing, what the metrics of success are. What are the 10 things you've tried?
- [REDACTED] to be fair, we are tracking that. Reduced VPVs, reduced ranking. What I can't give is attitudinal shift. That's the first time I'm hearing in those terms. That would be great for us to provide. We have hard policy constraints – things like Tomi Lahren's post. Just want to be clear we haven't declared victory.
- Andy: If you added to that policy changes you are considering, that would be helpful as well. I will tell you this just to have Rob's back, he gets asked this, it's becoming the number one question. I would just ask you not to put him in a position where he says he doesn't know. Better if he can say here's what the data says here's what they're doing, this is what they are working on.
- [REDACTED] Completely hear that. If I'm frustrated, it's because we want to achieve the same things. What we can give you is data.
- Andy: [REDACTED] I appreciate you being honest. I think it will be challenging for Rob to say that FB team is frustrated too. That kind of reaction would not go over well. We have to get past that.
- [REDACTED] To be extremely clear, reason I'm frustrated is not because it's a big problem, it's because it's moving so fast. The 40% Marines – that's coming from a community already hesitant. Comes from care.
- Rob: Maybe I haven't been able to articulate – what do you need from me to get the information you need?
- Brian: We'll develop a report get you data. We don't want to send something that will be frustrating. We've got a good sense, from what Andy has told us on this call would be most helpful – data picture. We will and can get you a report, Andy. We've been struggling to get you a usable dataset.
- Rob: Can we drill down on that. I don't need we saw 5% lift over X. I need – we tried XYZ, this is what seems to be working. What did you try? What is scaling? What was ineffective or political bullshit. Then a sense of what now.
- Andy: What Rob just asked for, complements the data. Do get the sense that this isn't a social media wide problem, it's unique to FB and WA. Conversations are not as challenging – we have much more straightforward conversations with others. I think people believe you can solve it. Simplify to here's what's going on, here's what's working.
- [REDACTED] this is my third meeting – Rob, we can pull that on the interventions. A lot of it will look like what we discussed two meetings ago. Product measures will look like what we've talked about. Haven't thrown away a lot. Just want to manage expectations. Want to understand how we're working with you in a different way than others.
- Rob: I feel like we're running around in circles. Some partners give us lots of information, some partners tell us to fuck right off. This feels like we're chasing our tails. If you don't want to give information, just say that. I don't want to feel like I'm

going to a dog and pony show. My dream for FB to play ball. It's about will we get out of this fucking mess. I'm not doubting that you are sincerely trying to solve this problem in good faith. I'm doubting that you are telling us everything or that you [REDACTED] aren't getting the resources you need to tackle this. Of 1% of vaccine info, this is what's concerning, this is who is seeing it, this is what we're doing.

- [REDACTED] Super helpful, appreciate the feedback. When I say want things from you all, just to improve our process. One example – we can't do race targeting. Using SVI.
- Andy: I've jumped into 3 or 4 FB conversations; each one has been almost exactly the same. I've asked the same questions with Rob. They all finish the same way. Good promise at the end. This is a new set of people; you're hearing the questions for the first time. I can't call Nick back and say that something is different now. Feels like we're in the same place.
- Brian: It's been 2-3 weeks, know Nick told you we'd be working on reporting. We'll get that to you ASAP. I think Nick said at the time it would take some time to figure out.
- [REDACTED] What helps me is understanding is it doesn't have to be qualitative. On the metrics – the most viral content is the authoritative content – I thought that wouldn't be useful. We'll look for faster qualitative bunch along with product info.
- Rob: Two reasons why not useful – we see it in CrowdTangle. I don't know if widest reach stuff is the problem, or stuff that's in groups, private.
- [REDACTED] Answer hasn't changed
 - Disinfo dozen style people staying under policy limits
 - Authoritative posts with comments and dialogues
- Rob: What that implies to me that you think there's not a problem. So, tell me what is. If it's far reaching authoritative but bad news.
- [REDACTED] That's why we didn't send it. I don't have the numbers on comments but pulling. The last thing that's evolving – public figures
- Rob: concept of disinfo dozen is concerning – is it impact or subjective?
- [REDACTED] subjective – reason it makes me nervous – how do we stay below these lines. Maybe misspoke when I said frustration – relates to nuance and extent of the problem. I want to work with you on these things – scrapper faster data
- Brian: Thanks Rob. We don't want to be running in circles. We'll get you something to react to. That will inform next steps.

EXHIBIT 6

4-5 Notes on Call with White House re Symptom Survey

WH attendees: Rob Flaherty, Courtney Rowe, Clark

FB attendees: Brian Rice, [REDACTED] [REDACTED] [REDACTED]

- Brian: Want to introduce [REDACTED] he leads our work on the COVID survey that we're sending regularly to you. Want to walk through how we use it, how we approach it, how we think it will be useful in the work you're doing to identify pockets of the country where vaccine hesitancy is more of a problem. [REDACTED] will give an update at the end. Will turn it over to [REDACTED] let us know if you have questions.
- [REDACTED] Hi Rob and Courtney, nice to meet you. Please interrupt with any questions, see this as a conversation. I lead a special methodology team – Demography and Survey Science. I'm a sociologist by training. The survey that we're running with CMU and UMD – using FB's superpower in combination with superpower of public health community to understand at a granular level issues. We rely on public health experts to help with what goes into survey, we aren't public health experts. In the US alone, we collect about 40,000 responses per day. Next largest – 75,000 responses every two weeks – the Household Pulse Data. Temporal and granularity make valuable instrument. We don't have access to individual responses, but we use data internally to help inform messaging campaigns, understand in the US, the world, where different messages might resonate. I can go into high level insights by race/ethnicity/age etc., real time info on preventative health behavior. But want to address what you want to hear about. High level things most pertinent:
 - We've all heard in the media and other data sources about disparities among people of color versus whites with respect to hesitancy. This survey points out that vaccine accepting black and LatinX adults are less likely to have attempted to make an appointment. In LatinX community, highest gap in MD, NY, VA. MD – disparity between LatinX and white adults is largest – interesting because MD is one of the least hesitant states. State like NM, much older Latino population, actual parity between white population and Latino population there.
 - States where most hesitant – MI, Indiana, Ohio – reasons people are giving – side effects, waiting to see what happens, lack of trust. In other states, a lot of diversity across the US. Nice thing about this data is you can dive in at a county level to see how the numbers are changing over time so you can think about potential interventions.
 - Another highlight – looking at real time preventative health behaviors. E.g., Texas with no mask mandate – we can look before and after lifting mask mandate on March 10. 3% decrease in people reporting wearing masks. We see heterogeneity across counties. Travis county kept mask mandate, saw very little change. Harris county, saw a 5-point change. We can understand microinterventions, how they are affecting behaviors. Can also look at interest in vaccine, what concerns people are having.

- This is just some of the ability that we have. The results are usually available about a day after collected. If we collect today, can see estimates tomorrow. That allows us to be able to understand the changes occurring as pandemic is unfolding.
 - Change instrument frequently, in 7 languages.
 - Would love to answer questions, what you'd like to see.
- Brian: Rob, you heard from [REDACTED] that we're using survey to get feedback and see in the real world how people are responding. View it as a valuable tool. Would love feedback on how could use it. We have a new version coming to you next week.
- [REDACTED] Have collaborated with CDC, gotten a lot of good feedback, a lot of interest from academic community. Zeke Emmanuel just co-published an article looking at self-modulated behaviors in response to rising case rates.
- Rob: In terms of the survey, when gleaning things from it, how do you compare population on FB against general population?
- [REDACTED] About 93% of adults in the US use the internet, about 83-84% on FB. We have more data about people on FB than people on survey panels. People don't join FB to take surveys, orthogonal w/r/t bias. Some slight skews, but we think we do pretty well. The value of the data isn't that there isn't bias, it's that the bias is consistent over time. If you want to understand over time across geographies, we can offer that better than anyone else.
- Rob: First packet I got in mid-March, was results from February, was useful. I'm curious, what are messaging things that are most useful. What are you finding that has worked?
- [REDACTED] We haven't engaged with our own interventions, we're rolling that out, it's early to say.
- [REDACTED] You'll recall, we're doing a lot of broad inform, we felt we didn't have the right targeting in place to go deep. One thing I want to make sure we're not losing, any subtext – how do we enable you to find the communities that need the more targeted messaging?
- Rob: we want to find where is the biggest problem, what has been materially useful.
- [REDACTED] Survey itself can tell you the reasons that hesitant but persuadable are being influenced by norms and expectations of people around them in their lives. You can see at a geographic level the differences. But you can also see who they trust. Those also vary by geography and population. If you take that – can explore local messengers in one community, friends and family in another, more elite spokesperson is another. It can help you with the messaging, but you have to try it to see if works.
- [REDACTED] It's hard for us to prove out that an informative piece of content changes hearts and minds outside of survey. Social norms, like profile frames, seeing friends and family and public figures, could help.
- [REDACTED] So when 28% people of NH saying they are waiting because other people need it more, then maybe you need to match message to not to wait. Almost like political microtargeting.
- Rob: How do we make that operationally useful for us and track it?

- [REDACTED] Because of privacy reasons, we work through academic partners. You could work through academic partners, or there is a public API. We can talk about the cadence you might want to receive the information.
 - For example, prime minister's office in UK want to access data to build out a dashboard.
 - We can help get in format that's the easiest way for you to consume.
- Rob: Format like the document you sent, the high-level takeaways, that's helpful. With API, might need Cyrus or HHS. I probably won't be using the API.
- Courtney: Would be great to follow up with Cyrus. Love that broken down by region and demographics. But equally important, how do we work with you all to push back on it. If someone in rural Arkansas sees something on FB, it's the truth.
- [REDACTED] OK – so in terms of action items
 - Find ways to reduce delay
 - Maybe there is a future opportunity to bring in my counterpart Katie who is working on roll out of info on state sides
- Courtney: That would be great. But we want to understand how to counter and correct myths. That piece of it is equally important. Seeing counternarrative on FB will be much more effective.
- Brian: We will push to get more frequent versions of this, can also look for red alert, COVID survey concierge service, will look at what we can provide. [REDACTED] want to see what survey can tell WH about where people are hesitant and how we get messages to them. Then also on FB to counter misinfo through labeling, pushing authoritative info to people. That's something we're making a priority.
- Courtney: Super helpful to get this information, this is what we need. What we need is help pushing back on the myths.
- [REDACTED] Doesn't just help us understand how and where to intervene, but it also tells us if the interventions are working. We can see overtime if hesitancy is decreasing where we are doing interventions.
- Rob: Rather than chasing individual narratives/demographics, know you've said that broad access is more of philosophical approach.
- [REDACTED] Don't think that targeting is the wrong way to do it, it's a sequencing thing. Remove harm, reduce hesitant, inform good. In an ideal state, we inform, but we can also identify and reduce hesitant. But since the detection still isn't quite there for hesitancy, we are starting with inform. Maturity of our detection is the core of challenge for identifying and removing and also means harder to do more targeted interventions.
- Rob: Question I have – if we focus on broad stuff next – if we are to take things from more targeted info, we run targeted ads and local media. You can look at what's showing promise, what's in the lab.
- [REDACTED] Yes – right now, it's all broad. Wondering if there is a way to combine vast majority of fastest groups about how to find appointments, discussing side effects. Do we leverage this kind of activity – we know from human patterns of behavior that people are trying to do X, can we build a better data set.

- [REDACTED] That's where a lot of our efforts are trying to go. We are looking at using CDC SVI to see if we're having a more or less positive effects on those counties that are considered as vulnerable by CDC. Can we bring together behavioral aspects of what we see. Not building two different tools, building one, market the same one to different people.
- [REDACTED] Can we bring Katie next time, Brian? This is at the heart of biggest opportunity to work together.
- Brian: Yes.
- Rob: Is the problem that there isn't a tool? Or the more someone uses FB, the more likely to be vaccine hesitant?
- [REDACTED] Don't think we have data that suggests that. Literature on vaccine hesitancy – people bring hesitancy to the groups that they are in. They aren't more hesitant as a result of social media campaigns. Do think that for some populations – not knowing how to get an appointment is actually a barrier. FB can help meet that need. For other populations, might have a more effective message. Vaccine hesitant, anti-vaxxers. We can address concerns of vaccine hesitant by understanding concerns and address.
- [REDACTED] Remove harm – about trying to actively do harm – that's the vast minority but we want to remove. Hesitancy – want to keep getting as much information as I can to you. Vast majority of overall widely distributed content, authoritative and good – from CDC, etc. Hesitancy themes around side effects – is vaccine causing nose bleeds, enlarged lymph nodes. We still have a gap in understanding or managing expectations as to what experience could be like. Another thing – lots of questions over finding appointment. Seeing a trend in memes and satire making fun of individuals that don't want to get vaccine. Political themes: video of Biden speaking, reactions. Still small group of adversarial people, large group who are hesitant and have concerns about side effects, finding appointments.
- Rob: Are you able to provide resources?
- [REDACTED] This is why on broad inform – we tag anything with COVID-19 vaccine, it directs you to the COVID information center. Ideal state – I have a concern about a nosebleed, here's a resource exactly about that. That from a technical perspective is really hard, which is why it's broader.
- [REDACTED] It's hard, and it may not be effective. Some research shows that allowing people to express experience and concerns might be a more effective path to having a conversation with them. Have to be careful in how we approach.
- Rob: If people are having the conversation, is the presumption that we let people have it. Direct them to CDC. What then?
- [REDACTED] I think it's an and. We all know people that have had the experience that think that FB is listening to them. The more general stuff, connection to CDC, pops up as very predictable, that's fine, people don't have issues with that. You have the opportunity to go back later, to surface information. At the immediate moment, have the big brother feel. We should pay attention to those conversations, make sure that people see information, even if it's not right then. Have easy access to information.

- [REDACTED] Also need to be honest here, deficit of trust in the government, deficit of trust in FB. Figuring out the right interventions that doesn't reinforce some of those concerns around trust is really critical. Who are your trusted sources? Friends and family? Community figure? In areas where we or you aren't the right voice, where we can find the right voice to address concerns>
- Rob: how do we get that stuff to people?
- [REDACTED] there are a number of public health agencies we're working with to do campaigns on FB – make use of ability to understand population and target messages appropriately.
- Brian: Some of this is actually targeting. [REDACTED] and our ads team know more – a lot can be accomplished through targeting, third parties can definitely target – there will be demographic information that will be able to be used as well.
- Rob: There are ways we can target around it. Since it's a global pandemic, can we give agencies access to targeting parameters that they normally wouldn't be able to?

... (missed 1 Q)

- Courtney: Have other issues – for example, women of childbearing age worried about fertility. Can we adjust survey on a dime? Pregnancy is another one but I'm less worried about it. Conservative circles. Can we send stuff your way to look at?
- [REDACTED] Yes you can definitely share information with us, we can look at what we're seeing, look at modifications to survey. CDC weighs in on questions. We do have questions, for example on pregnancy, we can look at whether it corroborates what you're seeing. We have other things like job occupations that we're looking at.
- [REDACTED] Want to be mindful of time,
 - In March took down 700,000 pieces of content globally, 150,000 in the US – this is a drop because we took down a lot and then were cleaning up
 - For full transparency and honesty, have moved out of a sprint that the teams have been in for the last 8 weeks, achieved goals, made progress – closed out foundationa understanding work, early virality detection. Now focus for teams will be expediting execution.
 - Don't want to seem like we've changed teams or priority, we're just shifting focus
- Rob: Team that had been focused on vaccine hesitancy is moving to execution phase, figured out what you need to do
- [REDACTED] That's right, but just within moving target, we've now identified the head of the problem, know what we're doing, overall priority, teams, resources, hasn't changed.
- Brian: We described this as a lockdown earlier. Wanted to hear from us, as things pop out of Facebook and into the Washington Post. Want to communicate clearly with you.
- Rob: I appreciate that, am not 100% understanding it but probably more me than you. What are the things that you found?
- [REDACTED] What I don't want you to think is that we've declared victory and on vacation. What we found – had some improvements on misinfo accuracy, adjusting policies (e.g., removing 2 million pieces of content). Vaccine hesitancy – what we talked about last

time – it's around topics – symptoms/appointments/memes/political themes, less about small group of adversaries. Now we're focused on executing.

- Rob: Execute is trying out new interventions?
- [REDACTED] Great question – when I say execute – we've already been deploying interventions in a first version way. Now we're expanding and improving the quality of those.
- Courtney: What are you qualifying as misinformation versus politically charged? What does that universe of stuff look like overall?
- Brian: The way that you describe it probably isn't the way we think about it – misinfo v. politically charged. We have a policy definition of misinformation, then we have gradations of what we take down, versus reduce/inform. Might be easier to send some examples.
- Courtney: What are all the narratives that are out there? Would be interesting to see what's misinformation versus something we'd flag.
- Brian: That's what [REDACTED] getting into with respect to the themes. We'll update you on the major themes that we're seeing each week. Flat out, adversarial misinfo versus vaccine hesitancy content.
- Courtney: E.g., in last seven days, have seen claims about people playing God, etc. Is that misinformation?
- [REDACTED] Maybe we can get some visual examples and send over. We'll pull Katie in around messaging channels. What am I missing Brian?
- Brian: Going to look at different ways to share survey information with Rob. Don't want to just link API to you, want to be topline. We'll take that back with [REDACTED] team too.
- Courtney: super helpful.
- Rob: We can offline about specific format. We're most interested in what's keeping you up at night.
- [REDACTED] We can do that, raise up to you quite frequently. Have a number of epidemiologists looking at this internally and externally.
- Courtney: I pinged the team about vaccine passports, can get you some examples.
- [REDACTED] Religious thing – survey lets us know if concerns are religious.
- Courtney: OK great.
- [REDACTED] we'll meet again in a week? Can move to Mondays going forward.

EXHIBIT 7

6/15 Meeting with White House

FB Attendees: Brian Rice, [REDACTED] [REDACTED] [REDACTED]

WH Attendees: Rob Flaherty

Brian – Rob, I know we have a lot to cover. Want to respond to conversation from a little while back. Start off with the Policy changes we made on May 26. Then we'll walk through content demotion where we hopefully explain in a way where you're comfortable with it. And hopefully our colleague [REDACTED] will join to provide more context around the statistics we sent over on vaccine sentiment. Wanted to make sure we gave you clarity there.

Rob – sounds great.

[REDACTED] – I'm [REDACTED] – I lead the product teams working on integrity within FB App. Around the distribution of reducing problematic content, inform treatments. I'll touch on 3 new misinfo experiences related to reducing distro of misinfo, touch briefly on how ranking works, I know we've discussed in the past, demotions are anchored in ranking, so will gloss over that, then go to details of demotions.

Rob – great

[REDACTED] – 3 new misinfo tools announced at end of May. Leveraged a few of them in election period.

New approach – give people more info about Pages that have shared misinformation or have content that has been repeatedly fact checked. So now where there's the case, you can get more information about what fact checkers said about content on that page. Part of overall inform strategy to give people more information.

More aggressive approach to entities that have repeatedly shared misinfo – Pages or Groups – it's typically the same sets of Pages/Groups. We've introduced logic so that we increase demotion strength/amount of demotion that we apply to those entities. This is one I was especially excited about. We know it's the same set of entities that are repeatedly sharing. This one is key.

Last one- improvement in way we notify people that they've shared content that fact-checkers later rate. We've redesigned notifications that the person gets to make it easier to understand. Additional info we're adding in – fact checker's article debunking the claim, prompt to share additional context with other people.

[REDACTED] – those are the three main new misinfo levers we've introduced. Any questions.

Rob – biggest question is related to how demotion works. But to make sure I have it right – first one is a pop up when you go to like a page that tells you it's repeatedly shared misinfo?

[REDACTED] – yes. And includes substantive information about the fact checker. We can send you an example of what it looks like.

Rob – how many times does the Page have to share to trigger treatment?

[REDACTED] – It varies across experiences. In this case, I think it's 5. Let me follow up specifically. Want to make sure you have the most accurate information.

Rob – I'm curious about notifications after sharing something fact-checked. In many different worlds ago, Brian and I talked about – the CW said it hardens people. What changed? What research have you done?

██████ – I can't speak to what was discussed earlier. These experiences have been being built for quite some time, have evolved. We've refined user research that told us that people do pay attention, there is value in providing this information, even if it's after the fact. Brian, any other context?

Brian – was this around the election?

Rob – this is when we first talked on Beto stuff – badging, notifying people. Research said counterproductive. I think this is a good thing.

Brian – I do remember that was our sense at the time – going back after the time. Let me go back to the teams and see.

██████ – We have pivoted substantially in the couple years I've been here towards a much more inform-centric approach. Another experience we launched last year – when a person goes to share an out-of-date piece of content or one likely to have misinfo in it, we surface what we call a reshare interstitial that informs people at time of sharing that content might be out of date. We found that as classifiers have improved over time, we've been able to be more targeted in approach, that type of information has quite materially slowed the spread of viral misinformation. A lot of this was over time improving our ability to classify, getting the copy and experience right – informative but not judgmental. Saying likely to be problematic in XYZ ways, you choose if you reshare. We notify you there might be some issues.

██████ – external studies in this space are heterogenous in their effects. Quality of classifier really matters in prompts, even if after the fact. Also, nature of the topic itself. Tone in which you approach it matters quite a bit. One of those situations where it works sometimes, it's not going to work all the time. You have to test and adjust it. I'm sure that improving classifier over time is what's making this work.

██████ – and getting the tone right is also a key factor. Can influence whether pause before sharing.

Rob – Tone is way copy is written?

██████ – right. We spent months of time landing the precise copy where we wouldn't be perceived as being paternalistic. Landing the words was really important. We launched the first ones in March/April last year have now used during election periods, other scenarios. It's a powerful lever against misinformation.

Rob – Cool, awesome

██████ – I love this approach specifically because we are transparent with users. Demotion work – it is difficult to be transparent, give people a sense of how their content is being enforced on. In this case, able to be transparent and clear about the fact that the content will get less distribution, fewer people are going to see it.

Rob – that makes sense.

██████ – Ok, I'll just cover context-setting COVID approach. We remove content that clearly violates our policies. Then there is a set of content that doesn't violate but could be harmful, and so important to reduce the amount of times content is seen. Won't spend much more time on that if that works for you.

Rob – OK

██████ – I can spend a minute on how ranking works. Demotions, in their simplest form, is a discount to a ranking score that we assign to a piece of content. Zooming out a bit – there is so much content out there – each person has more inventory than they could possibly ever go

through. Ranking is important because it's important to order what people see. Rank based on user value – determined by signals. What you might want to see most versus what I might want to see most. What we do is take all these different signals, assign a ranking score to a piece of content. Say there is a piece of sensationalist content, vaccine related. We assign a value – say it's 10 – given all the different things we incorporate into ranking score. Our integrity system then calculates an integrity score or multiplier. In the case of sensationalist content – we're certain that this piece of content is correctly classified as such – sensationalist content gets a demotion strength or discount of 40%/0.4. – we subtract 4 from 10. Piece of content that would have otherwise had a ranking score of 10 now has a rank of 6. So, when we stack rank or order the content after applying integrity score determines where it goes. Tricky piece is that ranking systems are deeply personalized. Difficult to say that a piece of content will rank in X position in everyone's feed universally. Not how it works. But I can say this piece of content would be seen by roughly 40% fewer people based on demotion. That's one way to think about the "under the hood" of demotion works.

Rob – this is interesting. If seen by 40% fewer people, who are the remaining 60%? What are the audience differentiations? What kind of person can see it?

██████ – this is where the personalized nature of news feed comes in (and note I'm talking conceptually, it may not be precisely 60/40). One example is a low inventory user. So, if my dad only has 4 friends, there's limited content for him to see. Another reason – connected to a page or group. Or if someone is scrolling deeper into feed than you or I might do.

Rob – Reason I ask – seems plausible that 40% that are no longer seeing it are less susceptible to it and 60% are more open to it. Attitudinal difference.

██████ – I think that's right – although we can't say who it's bad for, or whether their attitudes are antecedent.

Brian – Thinking about that population – I've been asking the same questions – you'd have the 40% might be the fence sitters. The remainder may have signal that they want to see it – they're not fence sitters. They are the folks that won't be convinced. There's an argument that you're removing it from fence sitter. I don't think we have data to show it.

Rob – Devil in the details. It's hard for me to make a personal evaluation of whether it's making a difference.

██████ – If we wanted to understand if it's making a difference, we'd have to randomly assign who gets demotion and who doesn't and have some sense of prior attitudes. Given that this is a rare event. That random assignment becomes harder when you're talking about content that others inject into the system versus our ability to inject content. With vaccines, it's probably not exposure to one thing or exposure over a short time. At the point of the pandemic where we're talking about vaccines, people have hardened/crystallized their attitudes. Hard to study. On integrity – we hope they are effective, taking steps because we don't want the content up. And then there are times where we are actively putting things at the top of people's feed. In that case, we control random assignments and can look at differences.

██████ – two other things.

60/40 – don't want to anchor in them, they are arbitrary. Could have used X and Y.

This is where inform treatments become important. People who might want to see that content will continue to see it. With overlay of authoritative content pinned to the top – embedded

authoritative information – becomes very important. People can choose to engage. But in parallel, we're providing a counter to that misinformation. Does that make sense?

Rob – It makes sense. You guys are much longer on inform, we're much longer on reduce.

██████ – what do you mean by that?

Rob – we're keen on what platforms are doing to reduce the spread of bad information, that platforms are not funneling people towards bad content. That's our primary concern. If you guys have data that show that inform counteracts the spread of bad information, great.

██████ – it does. The value of inform is that we know that it does have an impact on distribution.

Rob – I'd love to see that.

██████ – particularly important for borderline content where difficult for classifiers.

██████ – a couple data points that have been really helpful for me. Search interstitial. I think we have data that interstitials do reduce borderline and misinfo shares. It's a clear example of interstitial having a meaningful impact. Other data we have goes one step further – proactive campaigns with CDC and so on. Able to measure causal and in some cases positive impact on vaccine attitudes. Another example of value of inform.

Rob – I haven't seen that data.

██████ – as with all marketing campaigns, depends on targeting and copy. More than happy to share.

██████ – some of them were in Nick's email.

Rob – that was my last thing I wanted to get at with Brian. We came away that you weren't measuring, then we saw that you were. Was that brand lift? How are you measuring?

██████ – Measured in a few ways. A lot of the ones in Nick's note were brand lift or analogous (compare people exposed to content to random control group and survey). That's one of the techniques we've used. In addition to that, have done additional studies to try to attribute to real world uptake. Those take longer. Blood donations is a good example – when we rolled out in the US worked closely with American Red Cross – we were able to see with their data – increase of 19% increase nationwide of new donors. Using same techniques in this space. Direct brand lift, then broader body of work that goes all the way to attribution in the physical world.

██████ – I have to hop, Rob happy to follow up with whatever details might be helpful. There is some upcoming work on increased transparency that would love to chat with you about sometime in the future.

Rob – Great, thank you.

██████ – We are able to do causal inference/impact analyses. The conversation we had previously was how can we understand impact of misinfo on people's attitudes. That's where we have a hard time studying.

Rob – that makes sense. I actually do have to run also. I still have more questions, can email them to you Brian.

Brian – great. As ██████ mentioned, we are doing more as a Company to try and make this easier to understand. Coming in the next couple weeks. We can follow up with you then. But send questions, we'll do our best.

Rob – also interested outside of COVID in promotion of good information – NEQ score stuff rings a lot of alarm bells. Would like to dive in next time we talk.

EXHIBIT 8

EXHIBIT 9

From: [REDACTED]
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Urgent help assessing misinfo/misinfo adjacent Policy options
Date: Friday, August 6, 2021 7:13:48 PM

+ @ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> and @ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> for Comms visibility;
@ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> for Legal

Hi all,

Thanks so much again for the sprint on this. Leadership met today and decided we should move forward on our 4 recommendations (pasted below and also in our team's working doc here <[https://docs.google.com/\[REDACTED\]](https://docs.google.com/[REDACTED])>) and scope the exact product work needed to implement and then execute on the ones that are relatively easy to do.

[REDACTED] and [REDACTED] will be driving next steps on this overall while I'm out on PTO next week, coordinating with [REDACTED] and will reach out to our Product counterparts on Options 2a, 2b, and 2c. @ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> could you be on point to further scope Option 1a with your Recs Product counterparts?

@ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> and @ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> , please let us know if there's additional feedback you got on the Product side for how to best scope these options and whom to involve. I appreciate you flagging earlier today that we'll have to make some prioritization calls as we scope each of these options further.

@ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> , @ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> and @ [REDACTED] <[mailto:\[REDACTED\]@fb.com](mailto:[REDACTED]@fb.com)> , please let us know if you have any immediate thoughts on deadline to turn v2 of these options around. We'll move fast but aren't aware of a specific moment when we need to commit to any of these privately or publicly with external stakeholders.

[REDACTED]

Recommendations to further scope:

Option 1a. Designate linked assets as non-recommendable

- * Impact: Any assets linked to Groups/Pages/Profiles/Accounts that have been removed for COVID misinfo violations would not be recommended to users. E.g., RFK Jr.'s IG Account is removed, so his FB Page will be non-recommendable.
- * Recommendation: We recommend this as a stop-gap measure specifically targeting Disinfo Dozen assets. Per the recent Avaaz <https://secure.avaaz.org/campaign/en/fb_algorithm_antivaxx/> report, some entities affiliated with removed Disinfo Dozen Pages are still being recommended because they do not have recent violations.
- * Difficulty: Low (1-6 weeks)

1.

Option 2a. Count COVID M&H, Vaccine WDH, & COVID RFH toward misinfo Repeat Offender Status

- * Impact: Currently, strikes for COVID Misinfo & Harm, Vaccine Widely Debunked Hoaxes, and COVID Repeatedly Fact-Checked Hoaxes receive Community Standards strikes, but they do not count towards Misinformation Repeat Offender (RO) Status. If we count those strikes towards Misinfo RO Status, entities spreading COVID or vaccine misinfo would more quickly receive related penalties, such as content demotion or an advertising ban, on top of normal CS penalties.
- * Recommendation: We recommend this because the Misinfo RO system is meant to penalize misinfo actors and therefore should count this content, which is more egregious than false information fact-checked by a 3PFC.
- * Difficulty: Low (1-6 weeks)

Option 2b. Develop a strike system for health-related Partly False and Missing Context ratings that could trigger domain/Page/Group/account Repeat Offender (RO) status in more instances [Note: leadership feedback is to develop this for DOMAINS only]

- * Impact: Our latest analysis of URLs directing to Disinfo Dozen webpages found that a significant percentage of the most viewed URLs have Partly False or Missing Context 3PFC ratings. Counting health-related Partly False and Missing Context ratings toward entity-level penalties could allow us to take stronger action to reduce the distribution of the domains and associated entities themselves.
- * Recommendation: We recommend this as it is consistent with the precedent of taking stronger measures against Covid-related fact-checked content. However, this requires considerable lift for just a small set of bad actors.
- * Difficulty: High (6+ weeks)
- * In the interim, we could demote in-Feed domains associated with removed entities (note: three Disinfo Dozen domains are already experiencing demotion under Misinfo RO penalties).

Option 2c. Demote Partly False rated Covid or vaccine misinformation more strongly

- * Demote Partly False rated Covid or vaccine misinformation more strongly (up to 80% from 50% today) (Recommended)
- * Impact: COVID or vaccine misinfo that we don't remove would appear lower in people's News Feed.
- * Recommendation: We are already demoting COVID content rated Missing Context as a BTG and see this as consistent with that precedent.
- * Difficulty: Low (1-6 weeks)

From: [REDACTED] <[REDACTED]@fb.com>
 Date: Tuesday, August 3, 2021 at 7:46 PM
 To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
 Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
 Subject: Re: Urgent help assessing misinfo/misinfo adjacent Policy options

+ [REDACTED]

From: [REDACTED] <[REDACTED]@fb.com>
 Date: Tuesday, August 3, 2021 at 11:11 AM
 To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
 Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
 Subject: Re: Urgent help assessing misinfo/misinfo adjacent Policy options

Thank you SO much to everyone who's already chimed in on the doc. We just learned the leadership meeting has been postponed until Friday, so we have another 24 hours to get any additional Product input. [REDACTED] I will also side-ping a couple of you today to resolve open comments from overnight.

From: [REDACTED] <[REDACTED]@fb.com>
 Date: Tuesday, August 3, 2021 at 11:01 AM
 To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
 Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
 Subject: Re: Urgent help assessing misinfo/misinfo adjacent Policy options

+ [REDACTED]

From: [REDACTED] <[REDACTED]@fb.com>

Date: Tuesday, August 3, 2021 at 11:39 AM

To: [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>
Cc: [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>

Subject: Re: Urgent help assessing misinfo/misinfo adjacent Policy options

+ @ [redacted] <[mailto:\[redacted\]@fb.com](mailto:[redacted]@fb.com)>

From: [redacted] <[redacted] fb.com>

Date: Tuesday, August 3, 2021 at 6:00 AM

To: [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>
Cc: [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>

Subject: Re: Urgent help assessing misinfo/misinfo adjacent Policy options

+ @ [redacted] <[mailto:\[redacted\]@fb.com](mailto:[redacted]@fb.com)> + @ [redacted] <[mailto:\[redacted\]@fb.com](mailto:[redacted]@fb.com)>

Feedback from Health Integrity London

1. RFH strikes for demotion are not in production. We had strikes for RFH deletes and plan to enable strikes for demotions as a P2 for Q3 when we onboard responses to Misinformation's infra. RFH has ~40 new content enforcements per day (excluding banking which is ~550/day).
2. RE Section 3 "Demote more content" - As we plan to integrate with misinfo's infra for all responses (P1 Q3) these features could be prioritised for launch at that time. @ [redacted] <[mailto:\[redacted\]@fb.com](mailto:[redacted]@fb.com)> to comment on feasibility/timelines.
3. I have added another section with additional BTGs measures for consideration. One of which is automated Feed demotions on Covid posts by Health Misinfo Ros which was a BTG lever that we launched during the lockdown with Feed Integrity. At that time it was developed with [redacted], but while she's out I believe @ [redacted] <[mailto:\[redacted\]@fb.com](mailto:[redacted]@fb.com)> is covering here.

Thanks

From: [redacted] <[redacted] fb.com>

Date: Tuesday, 3 August 2021 at 01:43

To: [redacted] <[redacted] fb.com>, [redacted] <[redacted] fb.com>, [redacted]

We need to send these to leadership by EOD Tuesday, in advance of a Wednesday meeting with [REDACTED], [REDACTED], [REDACTED], and others, where they'll discuss.

Questions for you are:

1. Are any of these ideas definitely not feasible from a Product POV?
2. For all the ideas that are feasible, could you indicate in our doc whether they are a light (1-6 weeks to implement) or heavy lift (> 6 weeks)?

Thanks so much,

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] and [REDACTED]

PRODUCED TO HJC

EXHIBIT 10

From: Nick Clegg <[REDACTED]@fb.com>
Sent: Thursday, August 19, 2021 5:25 PM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: [A/C PRIV] Enforcement Update re COVID-19

Yep this looks good thx. N

Get Outlook for iOS

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, August 19, 2021 4:24:53 PM
To: Nick Clegg <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: [A/C PRIV] Enforcement Update re COVID-19

Nick, [REDACTED] [REDACTED]

This email provides a follow-up to our August 6th discussion regarding our response to the Surgeon General on COVID-19 misinformation. During that discussion, we agreed to further explore four discreet policy options for reducing the prevalence of COVID-19 misinformation on our platforms. Since then, teams have scoped the requirements for executing those options. As discussed further below, we plan to roll-out the first three options over the next coming weeks, and will roll-out the fourth option as an escalation only policy.

Please let us know if you have any concerns with the following plan by 9 am ET tomorrow; otherwise, we plan to provide an update to the Surgeon General and start executing against these tomorrow.

Thank you,
[REDACTED]

1. Option 1: Designate any assets linked to Groups/Pages/Profiles/Accounts, which have been removed for COVID misinfo violations, as non-recommendable to users.

- a. **Impact:** Any asset linked to Groups/Pages/Profiles/Accounts that have been removed for COVID misinfo violations would not be recommended to users (e.g., RFK Jr.'s IG Account is removed, so his FB Page will be non-recommendable).
- b. **Status:** **By the end of this week, we will enforce on approximately 60 linked assets related to the Disinfo Dozen that have been removed for COVID misinfo violations.** Over the next three weeks, we will engage in further work to understand how to mitigate the risk of over-enforcement here. We will then return with a further recommendation on a broader policy change that will affect more than just the 60 Disinfo Dozen-linked assets.

2. Option 2: Count COVID Misinformation & Harm (M&H), Vaccine Widely Debunked Hoaxes (WDH), & COVID Repeatedly Fact-Checked Hoaxes (RFH) toward Misinformation Repeat Offender status.

- a. **Impact:** Currently, only 3PFC-rated False/Altered content counts toward misinfo repeat offender status, which results in demotions and demonetization for entities. Counting COVID M&H, Vaccine WDH, and COVID RFH strikes towards misinfo repeat offender status would more quickly penalize entities spreading COVID or vaccine misinfo on top of our normal Community Standards penalties.
- b. **Status:** **We are targeting the end of September for launch.** This includes updating language on existing transparency surfaces to notify affected entities how content we remove for COVID/Vaccine violations factors into their Repeat Offender status.

3. **Option 3: Demote COVID or vaccine misinformation rated Partly False more strongly.**

- a. **Impact:** We currently demote content rated Partly False at 50%. We will increase that demotion level to 80% for COVID and vaccine misinfo. Note: In the last month, fact-checkers applied "Partly False" ratings to at least 1k COVID-19/vaccine content.
- b. **Status:** We are targeting the end of next week for launch. This includes transparency updates in an existing NewsRoom Post (link).

4. **Option 4: Count COVID or vaccine-related URLs that are rated Partly False or Missing Context towards "domain" Repeat Offender (RO) status (i.e., penalize the URL domains from which the content was shared).**

- a. **Impact:** The Disinfo Dozen report faulted FB for allowing users to share URLs linked to the Disinfo Dozen. Misinfo Policy found that, for the most viral Disinfo Dozen URLs rated by third-party fact checkers, 85% of those ratings were either Partly False or Missing Context. However, only False ratings count towards misinfo repeat offender status, which means, for those URLs rated False, all user shares of that URL's domain will be demoted.
- b. **Status:**
 - i. **Change:** This is a heavy lift to integrate into our existing repeat offender system. Instead, we will approach this as an on-escalation break-the-glass measure. We will periodically manually review domains that had a high number of third-party fact check ratings to see if enough of them were COVID or vaccine related. We will enforce on domains that meet that threshold manually for 90-day domain demotion (note: threshold is still TBD). Misinfo Policy and Product are aligned on this modification of the option as a BTG solution.
 - ii. **Caveats:** This will not flow through the normal repeat offender process, so will not have messaging that domain repeat offender status has been met. However, many of our domain repeat offender demotions do not give notification unless the domain is explicitly tied to a page. We will need to have a reactive comms plan for partners that may experience these demotions.

PRODUCED TO PUBLIC

EXHIBIT 11

From: [REDACTED]
To: [REDACTED]
CC: [REDACTED] Brian Rice; [REDACTED]
Sent: 7/22/2021 12:17:53 PM
Subject: RE: Surgeon General

Thanks. I'm sharing this with Nick and the status on the label of the IG video. He's calling Andy shortly. Thank you!

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, July 22, 2021 12:13 PM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Surgeon General

All --

To follow-up on #2 below, we were able to evaluate the groups closer. Based on the evidence of the post showing an intent to evade enforcement, and the presence of strikes in the group, PLUS evidence that they have a back-up group ready to go if their larger group is removed, we are comfortable removing both groups.

[REDACTED]

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, July 22, 2021 2:37 PM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Surgeon General

[REDACTED]

On #2, we discovered this content in two groups. Both groups are using coded language to discuss COVID and vaccines. We don't have a policy prohibiting people from using coded language if their content otherwise does not violate our policies. One group had only 6 posts and no violations; the other had 3,600 posts and 2 violations. I am asking PREsc to continue reviewing those groups to

make sure there are no violations. **We could amend our Help Center to prohibit Groups and Pages from using coded language to discuss COVID and vaccines if there is evidence that they intend to avoid detection (we believe there is such evidence here -- see post below where they are teaching members how to use code words).**



On #3, we reviewed 28 websites linked to the "Disinfo Dozen" and found that 15 prominently feature content that would violate our COVID/vaccine misinfo policies, or would be borderline vaccine discouraging, if they were on our platform.

Of those 15, >50% of the recent shares of 2 of those domains would violate our policies if on platform; 25-50% of the recent shares of 6 of those domains would violate our policies; and <25% of the recent share of 7 of those domains would violate our policies.

- If we were to blackhole all 28 websites, that would remove approximately **500 million** pieces of content.
- If we were to blackhole only the 15 websites, that would remove approximately **252 million**

pieces of content.

- If we were to backhole only the 2 domains where >50% of the recent shares contain violating content (i.e., childrenshealthdefense.org and vaccines.mercola.com), >66 million pieces of content would be removed.

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, July 22, 2021 1:58 PM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>
Subject: RE: Surgeon General

Nick is pinging about this. Looks like the content in #1 still isn't labeled. Can we get the label applied, content demoted, and tell him what he can say about why the label/demotion didn't happen in the ordinary course? @ [REDACTED] it looks in the case like it's assigned to someone off-duty in Dublin. Can someone take the enforcement action?

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, July 22, 2021 8:21 AM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>
Subject: Re: Surgeon General

Just confirmed with Mia that (1) below is Tier 2 Borderline Vaccine content and should be labeled and demoted. I'll comment in the Case [REDACTED] started.

Will also ask Presc to look into (2).

From: [REDACTED] <[REDACTED]@fb.com>
Date: Thursday, July 22, 2021 at 8:19 AM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>
Subject: Re: Surgeon General

fyi I sent the first IG link to PRESC a bit earlier. Being looked at in C#1001299.

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, July 22, 2021 7:59 AM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Brian Rice <[REDACTED]@fb.com>
Subject: FW: Surgeon General

On the do-outs from Nick's email below:

Whether you think this is the right approach or no, this is a reasonable way to look at things”

2. Andy S has also provided this as an eg of unlabeled content which he says is doing the rounds and is being cited by a clinic in LA as one of the reasons why many people are not getting their second jab:

https://www.instagram.com/p/CRbw8NEsOc6/?utm_medium=share_sheet

Grateful if someone could explain why this wasn't labeled?

He also shared this which I think rather proves our point – are we supposed to remove “gibberish”? - but grateful for views since I'd like to get back to Andy on it (he claims he is trying to be helpful by passing on our POV to the Surgeon General before the Fri meeting):

<https://twitter.com/oneunderscore/status/1418016654580199427?s=10>

3. Sheryl is keen that we continue to explore some moves that we can make to show that we are trying to be responsive to the WH. [REDACTED] – I have explained to her that you think the blackholing idea doesn't work after all.

We should take stock after the Fri meeting, but my sense is that our current course – in effect explaining ourselves more fully, but not shifting on where we draw the lines or on the data we provide (subject to the agreement last night that we'd offer up VPVs of content we've removed but only if demanded from other platforms on the same basis) is a recipe for protracted and increasing acrimony with the WH as the vaccine roll out continues to stutter through the Fall and the Winter. Given the bigger fish we have to fry with the Administration – data flows etc – that doesn't seem a great place for us to be, so grateful for any further creative thinking on how we can be responsive to their concerns.

THx

N

PRODUCED TO HHS

EXHIBIT 12

From: Sheryl Sandberg <[REDACTED]>
To: Nick Clegg
Sent: 7/21/2021 4:49:24 PM
Subject: Re: Covid misinfo: Delta assessment + Mitigations

Sounds good

From: Nick Clegg <[REDACTED]@fb.com>
Sent: Wednesday, July 21, 2021 2:13:45 PM
To: Sheryl Sandberg <[REDACTED]@fb.com>
Subject: Re: Covid misinfo: Delta assessment + Mitigations

Well, I'm pushing [REDACTED] et al to see what more data we can share with them which is a big ask from the WH – the problem is they disregard the “reach” data (vs engagement) that we already share with them, and they don't ask the same of other cos (YT et al) so I'm going to propose to Surgeon Gen on Fri that he asks for comparative data from all the cos not just us which should move things along on that front.

Re misinfo itself it's worth reading the email from [REDACTED] in detail – what the WH appears to want us to remove ranges from humor to totally non violating chatter about vaccines. I can't see Mark in a million years being comfortable with removing that – and I wouldn't recommend it.

We don't need to decide everything at once – we should wait to see what Surgeon Gen tells me on Fri before deciding how/whether we need to make any bigger moves.

[REDACTED] now tells me that she's sceptical that the “blackholing” of links actually works in practice – frustrating – so if you answer to the wider thread be aware that it's not yet clear whether it's workable.

N

From: Sheryl Sandberg <[REDACTED]@fb.com>
Date: Wednesday, July 21, 2021 at 11:01 PM
To: Nick Clegg <[REDACTED]@fb.com>
Subject: RE: Covid misinfo: Delta assessment + Mitigations

I am for this – should I reply to the broader thread?

And you sure we should not do more?

From: Nick Clegg <[REDACTED]@fb.com>
Sent: Wednesday, July 21, 2021 1:58 PM
To: Sheryl Sandberg <[REDACTED]@fb.com>
Subject: Re: Covid misinfo: Delta assessment + Mitigations

Possibly the highlighted bit – the team still needs to bottom out details – keen to know whether you and Mark would be supportive. N

From: Sheryl Sandberg <[REDACTED]@fb.com>
Date: Wednesday, July 21, 2021 at 10:47 PM
To: Nick Clegg <[REDACTED]@fb.com>
Subject: RE: Covid misinfo: Delta assessment + Mitigations

There is separate, ongoing work on publishing wider transparency reports incorporating the "top 100 posts" reports which we have provided in recent weeks to the WH.

N

From: [REDACTED]@fb.com>
Date: Wednesday, July 21, 2021 at 8:35 PM
To: Nick Clegg <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, Brian Rice <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Covid misinfo: Delta assessment + Mitigations

Nick,

TLDR: There is likely a significant gap between what the WH would like us to remove and what we are comfortable removing. There are some policy mitigations that could get the two parties closer, but Content Policy does not recommend pursuing them.

You asked for information about the delta between content that Facebook is removing and the White House wants us to remove and mitigation options. The White House rarely provides any specificity about what it wants removed, but it routinely complains to us about content identified in critical media reports. We've compiled specific criticisms and extrapolated from more general complaints below:

1. Cross-platform disables:

- a. Delta: The WH wants cross-platform disables. We only do cross-platform disables for child safety and dangerous organization violations.
- b. Mitigation (not recommended): We could remove all of a person's groups/pages/accounts once they have had a single group/page/account removed for covid misinfo violations. This would remove approximately 50 non-violating entities associated with the Disinfo Dozen, including many entities that have nothing to do with COVID or vaccines. We are continuing to research what other entities might be affected.
- c. Background:
 - i. Jen Psaki said that if you're banned on one platform, you should be banned on all platforms. We do not and should not ban users from FB or IG because they've been banned by competitors. We assess FB pages and profiles and IG accounts based on the content they post and do not typically enforce against a non-violating page/profile/account if a connected entity is removed (we only enforce cross-platform on DOI and Child Safety violations). This practice has been a point of contention around the "Disinfo Dozen" because we have removed their violating entities (23 entities from 11 of the 12 people) but continued to allow their non-violating entities (53 entities - this set is under constant review and number changes often).

2. Off-Platform Links:

- a. Delta: The WH wants all links to the Disinfo Dozen's off-platform domains removed. We only remove links to off-platform content if the content violates child safety or dangerous organizations violations.
- b. Mitigation (not recommended): We could remove all posts from FB/IG if the posts contain a link to domains associated with covid misinfo violators, but it would likely remove significant amounts of benign content posted by regular users, such as their posts about person experiences or government criticism that also include a link to a website. Some of the off-FB/IG websites also have non-covid-related content, so we could be removing posts that are not about COVID and link to the websites for non-COVID reasons. It is unlikely that we have capacity to review individual off-platform links, so we would likely have to execute at a domain level.
- c. Background:
 - i. To get to the claim that 65% of covid misinfo comes from the Disinfo Dozen, we assume the WH

is complaining about non-violating content on FB that includes links to content off FB that would violate if posted on FB.

- ii. We could blackhole links to any domain or sub-domain associated with pages, groups, or accounts removed for violating our covid misinfo policies. We are currently investigating the impact that this change would have, including both scope of removals and how much of the content would be benign. Given resource constraints, we do not think it is feasible to review all pages before removal.
- iii. We are still collecting information on how much content this would remove and a rough estimate of what percentage of that content links to benign versus violating content.

1. True information:

- a. Delta: The Surgeon General wants us to remove true information about side effects if the user does not provide complete information about whether the side effect is rare and treatable. We do not recommend pursuing this practice.
- b. Mitigation (not recommended): We currently label all of this content and demote some of it. We could remove the content or increase the demotion strength.
- c. Background:
 - i. The Surgeon General's report on misinformation defines misinformation as including: "An anecdote about someone experiencing a rare side effect after a routine surgery. The specific anecdote may be true but hide the fact that the side effect is very rare and treatable. By misinforming people about the benefits and risks of the surgery, the anecdote can be highly misleading and harmful to public health."
 - ii. Experts have advised us that it's important to allow people to ask questions and allow open discussion of vaccine safety and efficacy to overcome vaccine hesitancy. For content that is presented in a sensational or shocking way or promotes vaccine refusal, we demote the content and apply a label with a link to accurate, authoritative information. We believe the information push partially combats the incomplete information while giving users space to express their views and share their personal experiences.

1. Other Vaccine Hesitant Content:

- a. Delta: The WH generally objects to content that appears in media criticism of our covid misinfo efforts. While we don't have specifics, we can extrapolate that they would like us to remove content that provides any negative information on or opinions about the vaccine without concluding that the benefits of the vaccine outweigh that information or opinion; humorous or satirical content that suggests the vaccine isn't safe
- b. Mitigation: Similar to true information, we recommend adhering to expert advice that we allow open discussion of vaccine safety and efficacy and do not recommend removing this content. We could consider increasing the demotion strength on content being demoted that is still breaking through into top posts.
- c. Background:
 - i. We reviewed a recent report, titled [Facebook has a vaccine misinfo problem](#), that concluded 12 of the top 15 vaccine-related posts on Facebook in a one-month period were "negative." We replicated the report's Crowdtangle search to review the content. None of the content or users relate to the "Disinfo Dozen." Of note, in order to maintain the narrative of FB's failure, our critics remove UNICEF content from their analysis because it effectively dominates covid content -- an accurate report on covid content from this Crowdtangle search would show that 5 of the top 15 posts were authoritative, pro-vaccine posts from UNICEF.
 - ii. None of the content should have been removed. Five pieces of content labeled "negative" are being demoted for being vaccine hesitant. Six pieces of content labeled "negative" are non-violating -- one is an ABC News report; two are personal opinions opposing mask and vaccine mandates; and two are personal opinions about the speaker's decision not to get vaccinated. Four pieces of content are labeled "positive" or "neutral." There is a full content assessment below.

Detailed Assessment of Other Vaccine Hesitant Content:

1. The #2 ranked content is an ABC News report about side effects. It is deemed "negative."
 - a. Delta assessment: We don't know whether the WH would propose that this reporting from network news should be removed for accurately reporting on side effects. We do not recommend doing so.

1. Five pieces of content (ranking 1, 5, 7, 13, 14) were borderline content and were demoted and labeled, but the demotion strength did not remove them from the top 100 FB posts for the relevant time period. All received the label: "COVID-19 vaccines go through many tests for safety and effectiveness and are then monitored closely" with a link to FB's COVID-19 Information Center.
 - a. Delta assessment (content assessment below): We suspect the WH believes this content should be removed. We demote and label this content because we find it irresponsible in its sensationalism and lack of context; however, it is a mix of true content and criticism of the government, both of which are appropriate to allow on platform.
 - b. #1, 5, and 7 are from Candace Owens and suggest that the vaccine is experimental or has side effects, including death, and are critical of the government. #5 was also fact-checked by a 3PFC.
 - c. #13 is from Tucker Carlson and offers sensationalized reporting on a true incident of a 12 year old suffering a rare side effect and reporting on a study published in the *Journal of the American Medical Association (JAMA) Pediatrics* about the dangers of wearing masks to children. The content was posted the day after the JAMA study was published. JAMA retracted the study two weeks after publication.
 - d. #15 is from Turning Point USA and suggests that the government has no authority to mandate taking an experimental vaccine.
1. Five pieces of content (ranking 4, 6, 8, 11, 12) were labeled negative.
 - a. Delta assessment (content assessment below): The WH has previously indicated that it thinks humor should be removed if it is premised on the vaccine having side effects, so we expect it would similarly want to see humor about vaccine hesitancy removed. We don't have insight into whether the WH wants personal opinions about government mandates or explanations of personal choices not to get the vaccine removed. We believe there is a strong interest in protecting the expression of personal opinion and personal choice.
 - b. #4 is a cartoon attempt at humor, suggesting that door-to-door vaccinators would be tied to trees.
 - c. The other four pieces of content all offer personal opinions about mask or vaccine mandates or the decision to be vaccinated.
1. Four pieces of content (ranking 3, 9, 10, 15) were labeled positive or neutral.

Disinfo Dozen Status On Platform:

1. We have been aware of the Disinfo Dozen back in March. We took very aggressive actions based on them, and other entities we flagged, by expanding the amount of Misinfo that we remove and by giving the "Worst of the Worst" entities 48 hours to remove all violating misinformation or otherwise they would be removed. As a result of that, we removed known anti-vaxxers such as RFK Jr.'s IG Account.
2. This resulted in behavior modification by these actors -- RFK stopped posting anti-vax content on his FB page, and some other members of the Disinfo Dozen also stopped posting violating content.
3. We have continued to monitor these accounts and have found the following:
 - a. 91 entities are tied to the Disinfo Dozen (however, the majority of these entities do not share anti-vax content and some post infrequently or stopped posting altogether).
 - b. 23 of those entities have been removed.
 - c. We are confirming additional entities (approx. 15) that may be removed under our "Single Use Multiple Account" and Recidivism policies (we are aiming to have these results by EOD).
 - d. 11 of the 12 Disinfo Dozen members have had one entity removed by us. The 12th posts mainly about internet censorship now. We are watching his profile closely.

EXHIBIT 13

7/16 Call with SG's Office

Attendees (SG's Office): Eric Waldo, Kyla Fullenwider

Attendees (FB): [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]
[REDACTED]

- [REDACTED] Good to see you Eric, Kyla. Long time no see.
- Eric: Great to see you.
- [REDACTED] I'll run point for a little bit and then will pass it over to you. I have a few of our team members on the call. Won't do full intros, they'll introduce themselves as we go. We do have [REDACTED] our Head of Health, on the line. What we were initially going to do was some intros to some of our work. But given the announcement, wanted to focus a bit more on that. Understanding information sources you're using, understanding the advisory, and discuss next steps to move forward. Would love to hear from you Eric.
- Eric: I'm Eric Waldo, Director of Engagement for Surgeon General Murthy. I spent all 8 years in the Obama Administration. Week 4 for me, really excited to be part of Dr. Murthy's team. You obviously heard the remarks from Dr. Murthy and Jen Psaki. Dr. Murthy has been clear that we're really calling for an all-society approach – individuals, organizations, technology can do, especially with respect to misinformation. We know this is a broader issue for society. Health Advisory is one of the tools for SG's office. We have commitments from Rockefeller Foundation, other organizations, in response to SG's call for action. Before we go further, want introduce Kyla.
- Kyla: I'm leading SG's work on health misinformation, including the Advisory. We're excited to walk through some pieces of it today. I was previously CIO for US Census Bureau, stood up work on misinformation there. Nice to meet you all, good to be here. We set up calls with as many stakeholders as possible who were mentioned in the Advisory. Want to go through at a high level.
 - To reiterate – Advisory is one of three tools that SG has to call public attention to an issue of concern. A report is longer, multi-year effort, hundreds of pages, on a topic with a lot of literature and substantial evidence base – for well-established health issues. Then you also have a call to action, 20–50-page document, around a topic. In the middle. Advisory is a shorter document – calling attention to an emergent issue for public health. Just adding some context, most folks, including myself a year ago, might not be familiar.
 - As Eric mentioned earlier, wanted to be very intentional about a whole of society approach. Called out stakeholder groups of particular importance, individuals/families, educators, health professionals, technology platforms, researchers, government (list incomplete, see advisory for full list).
 - First parts of the document set the stage – lay the groundwork for how we got here. Second page – unique to SG Advisory – we call out specific actions and recommendations. Let me move through and skip forward to tech platforms.
 - If you hadn't had a chance to review the section on tech platforms, would be great to do so. Everything rooted in evidence-base, in conjunction with experts we consulted. Wanted to find middle ground of interventions and solutions that are doable but meaningful. What we wanted to address here are not just the low-hanging fruit but things that could create systemic impact over the long term. But not so visionary that are not able to be implemented. Happy to talk through any of those pieces.

- Just jumping to conclusion – message that we really wanted to drive home – speed and scale at which misinformation is spreading is truly unprecedented and it's having quantifiable impacts on COVID response. Wanted to make that clear. We do think we're in a unique circumstance – what WHO calls infodemic – that needs to be addressed.
- [REDACTED] let's recircle back on questions but would love to hear more about specifics.
- Kyla: sounds good.
- Eric: [REDACTED] I know you flagged the 4 action items from Jen Psaki's remarks. I don't know if you want to walk through those, what your current stance is on those, anything you might be doing in response to call to action, we'd love to hear that.
- [REDACTED] Great, that would be a helpful discussion. Will turn it over to [REDACTED] and our team.
- [REDACTED] Happy to discuss and start with the four points. The overall recommendations on what technology platforms can do – we're broadly aligned, make a lot of sense. We'd love to work together. Excited about that as one area of discussion, anticipate it will be ongoing, working to build shared understanding of solution space. Would also be helpful to get to a shared understanding on the scope of the program – it would be quite helpful for us to learn some of the specific data points and research you're seeing, maybe even connect our research teams. We also obviously partner with academics, others. But quite helpful if we have a shared understanding of the problem grounds solutions. In an ideal world – how do we align on solutions, how do we align on shared understanding of most concerning things you are seeing.
- Eric: That absolutely makes sense.
- [REDACTED] So, on aligning on solutions –
 - More transparency – in general, we agree here. You're probably familiar with our tool called CrowdTangle. It's currently just showing engagement not just reach. We've been working to share reach with government partners since January. We've made substantial investments in this tool that's open to researchers and academics. We agree that reach better contextualizes things. Open to feedback on how reports could be more useful, other thoughts
- Kyla: Are you planning to continue having CrowdTangle available going forward?
- [REDACTED] Not my specific product area, but it's been available for many years. It's available to government partners by exception – CDC, WH, and others do have access.
- Kyla: CrowdTangle – that will continue to be a tool that's available for use?
- [REDACTED] We can confirm that but I'm not aware of any plans to change that.
- Kyla: If there's an update on CT, that would be great if you could provide that.
- [REDACTED] That's initial steps and thinking on measuring. Related to this point and the fourth point about amplifying trusted sources. We are very focused on understanding the impact of interventions. We've partnered with organizations – funding RFPs to understand impact of misinformation and RFPs on effectiveness of educational information. One of the more recent things we did – Alliance for Advancing Health Online. Working with Merck, WHO, others, working to foster a better understanding of interventions and how they are improving outcomes. We're providing a substantial amount of funding. We're very invested and want more research, more RFP submissions. That could be an area to go deeper in the future.
- [REDACTED] To second point on enforcement strategy, maybe best to have [REDACTED] discuss.
- [REDACTED] On this question – the way we enforce on content – what's being posted on a Page or Group. People post different content on a Page than for instance on an IG account. On RFK, Jr., for example, was using IG account to spread anti-vax account. It reached the threshold of strikes and was removed. He then stopped posting on FB about vaccines at all.

- [REDACTED] On the third point – one of the reasons we were reporting on top engaged posts and top reach posts- wanted to see what kind of content was in there. We've been sharing reports with the White House on this.
 - The top posts on our platform are mostly not about COVID or vaccines. Among the subset of posts that are about COVID and vaccines- the top 100 posts on COVID/vaccines, there are a few more on the potentially inducing hesitancy side. But if you zoom out, those are fewer than the ones coming from credible, authoritative sources. We have more work to do, but that's what we're seeing and what we are sharing. Replicable from CrowdTangle. We're very open to if there are things that we're missing, would love to engage on the specifics.
 - I'll also say in the SG's Advisory around designing systems in such a way that you can slow down the spread of misinformation. That's a promising approach we are committed to. For example, last year, in WA, we removed the ability to forward a link to many people at once. There were good use cases, like sharing a link to a birthday party, but took action to limit misinformation spread.
 - When people share content that could be misinformation, have an interstitial that links to the COVID Information Center.
 - Just some examples of the changes we've already made that are aligned with this approach. The WA one in particular was a big system change.
- Kyla: The piece we talk about specifically about adding friction – do you have anywhere publicly where you share the impact of those interventions?
- [REDACTED] I know these have all been shared publicly, not sure how deep we got into the data, but we can follow up.
- [REDACTED] On this question – policy side and enforcement side. We've been working hard over the last year and a half to keep up, have been working with CDC and others to update our policies as things evolve. The enforcement piece is also difficult, training classifiers. We also have partnership with third party fact checkers – for things that don't meet removal threshold, get sent to third party fact checkers. Content is temporarily demoted pending fact check. We have shared that about 95% of the time when people see those screens/interstitials, they didn't go on to post the content.
- Kyla: Size of fact checking team?
- [REDACTED] We partner with 80 organizations in over 60 languages.
- [REDACTED] And we attack virality aspect through feed demotions. We remove content that can lead to imminent physical harm. For content that doesn't meet that threshold, we instituted borderline demotions. For example, someone sharing negative side effect posts. Similarly, posts questioning whether you should get a vaccine under a mandate, whether it's government overreach. We demote those. That's not false information, but it leads to a vaccine negative environment. When it comes to looking at COVID misinformation, it's a different approach. What we normally do is just remove or leave to fact checkers. Here, we introduced a middle ground.
- [REDACTED] There's a lot on educational, amplifying credible sources I want to touch upon briefly before we break as well.
- Kyla: [REDACTED] do you have anywhere this borderline policy?
- [REDACTED] Yes, it's all public in our Community Standards. There is a link that details all of this, we can send it to you.
- [REDACTED] Last point – helping get people access to credible information. Will be a huge part of solution. This is an area we've invested a lot in, have commitment to. A lot of our efforts are

around helping organizations meet people where they are with information. And then there is social norming work. A lot of research shows that if you know someone who has gotten vaccinated, it can make you more likely to do get it. We worked with USG on profile frames. At this point, I think 50% of users in the US have seen a friend or family member use a COVID vaccine profile frame. KFF study also shows that friends/family can be very influential. We've also delivered 10 billion ads impressions through partner channels, working to publish data on the impact. There's a lot to build on.

- On Amplification, changing how we amplify within core product, making sure that trusted/credible sources are getting more distribution.
- Eric: Thank you, this is super, super helpful. I know we weren't going to get all the way home. Let me just say two things as we wrap up. 1- thank you for jumping on the call, we're getting comfortable with being uncomfortable. Want to be honest, appreciate courage having this conversation. I think you'll continue to hear the White House and leaders say they want to move forward with solutions. You'll hear that from Dr. Murthy. Want to be super straight with you. Kyla and I can offline with the team and circle back on solutions. I want to say thank you, can be uncomfortable, really appreciate it.
- [REDACTED] I'm very conscious you need to jump, we'll stand by. Again, we're looking to understand what you're seeing, understand next steps and how to partner moving forward. We'll be in touch on email.

PRODUCED TO HJC

EXHIBIT 14

1

2

3

4

5 COMMITTEE ON THE JUDICIARY,

6 U.S. HOUSE OF REPRESENTATIVES,

7 WASHINGTON, D.C.

8

9

10

11

12 INTERVIEW OF: LAURA DEHMLOW

13

14

15

16

17

Monday, July 17, 2023

18

19

Washington, D.C.

20

21

22 The interview in the above matter was held in room 164, Cannon House Office

23 Building, commencing at 10:03 a.m.

24

Present: Representative Jordan.

1 Appearances:

2

3

4 For the COMMITTEE ON THE JUDICIARY:

5

6 [REDACTED], LAW CLERK

7 [REDACTED], INTERN

8 [REDACTED], CHIEF COUNSEL FOR OVERSIGHT

9 [REDACTED], PROFESSIONAL STAFF MEMBER

10 [REDACTED], SENIOR SPECIAL COUNSEL

11 [REDACTED], COUNSEL

12 [REDACTED], MINORITY CHIEF OVERSIGHT COUNSEL

13 [REDACTED], MINORITY INTERN

14 [REDACTED], MINORITY OVERSIGHT COUNSEL

15

16 For the U.S. DEPARTMENT OF JUSTICE:

17

18 MATTHEW HANSON, SPECIAL COUNSEL,

19 OFFICE OF LEGISLATIVE AFFAIRS

20

21 For the FEDERAL BUREAU OF INVESTIGATION:

22

23 MARY DOOCY, ASSISTANT GENERAL COUNSEL,

24 OFFICE OF GENERAL COUNSEL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

MAJORITY COUNSEL 1. This is the transcribed interview of Laura Dehmlow.

Chairman Jordan has requested this interview as part of the committee's oversight of the Federal Bureau of Investigation.

Would the witness please state your name for the record?

Ms. Dehmlow. Laura Dehmlow.

MAJORITY COUNSEL 1. Could agency counsel please state your name for the record?

Ms. Doocy. Mary Doocy, FBI.

Mr. Hanson. Matthew Hanson, Department of Justice.

MAJORITY COUNSEL 1. And, Ms. Dehmlow, you understand agency counsel has the primary fiduciary duty to the Bureau and not to you individually?

Ms. Dehmlow. I do.

MAJORITY COUNSEL 1. And so you would like to continue with agency counsel today?

Ms. Dehmlow. Yes.

MAJORITY COUNSEL 1. On behalf of the committee, I want to thank you for appearing here today to answer our questions.

The chairman also appreciates your willingness to appear voluntarily.

My name is [REDACTED], and I'm with Chairman Jordan's staff.

I'll now have everyone else from the committee who is here in the room introduce themselves, as well.

[REDACTED] [REDACTED] with Chairman Jordan's staff.

[REDACTED] [REDACTED] with Chairman Jordan's staff.

[REDACTED] [REDACTED] Chairman Jordan's staff.

[REDACTED] [REDACTED], Chairman Jordan's staff.

[REDACTED] [REDACTED], Chairman Jordan's staff.

1 MINORITY COUNSEL 2. [REDACTED], oversight counsel for the Democrats
2 and Judiciary Committee.

3 MINORITY COUNSEL 1. [REDACTED], chief oversight counsel for the House
4 Judiciary Committee.

5 [REDACTED]: [REDACTED], Democratic staff and intern.

6 MAJORITY COUNSEL 1. Thank you.

7 I would like to now go over the ground rules and guidelines that we will follow
8 during today's interview.

9 Our questioning will proceed in rounds. The majority will ask questions for 1
10 hour, and the minority will then have an opportunity ask questions for an equal period of
11 time if they so choose.

12 We'll alternate back and forth until there are no more questions and the interview
13 is over.

14 Typically, we take a short break at the end of each hour, but if you would like to
15 take a break apart from that, please just let us know. We're happy to accommodate
16 that.

17 As you can see, there's an official court reporter taking down everything we say to
18 make a written record.

19 So we ask that you give verbal responses to all questions.

20 Do you understand?

21 Ms. Dehmlow. I do.

22 MAJORITY COUNSEL 1. So the court reporter can take down a clear record, we will
23 do our best to limit the number of people directing questions at you during any given
24 hour to just those people on the staff whose turn it is.

25 Please try and speak clearly so the court reporter can understand and the folks

1 down at the end of the table can hear you, as well.

2 It is important that we don't talk over one another or interrupt each other if we
3 can help it, and that goes for everyone present at today's interview.

4 We want you to answer our questions in the most complete and truthful manner
5 possible. So we'll take our time. If you have any questions or if you do not understand
6 one of our questions, please just let us know.

7 Our questions will cover a wide range of topics. So, if you need clarification at
8 any point, please just say so. If you honestly don't know the answer to a question or do
9 not remember, it's best not to guess. Please give us your best recollection. It's okay to
10 tell us if you learned information from someone else. Just indicate how you came to
11 know that information.

12 If there are things you don't know or can't remember, just say so and please
13 inform us who to the best of your knowledge might be able to provide a more complete
14 answer to our question.

15 You should also understand that by law you are required to answer questions
16 from Congress truthfully.

17 Do you understand that?

18 Ms. Dehmlow. I do.

19 MAJORITY COUNSEL 1. This also applies to questions posed by
20 congressional staff in an interview.

21 Do you understand this?

22 Ms. Dehmlow. I do.

23 MAJORITY COUNSEL 1. Witnesses that knowingly provide false testimony
24 could be subject to criminal prosecution for making false statements under 18, U.S.C.,
25 United States Code, section 1001.

1 Do you understand this?

2 Ms. Dehmlow. Uh-huh.

3 MAJORITY COUNSEL 1. Is there any reason you are unable to provide truthful
4 answers to today's questions?

5 Ms. Dehmlow. No.

6 MAJORITY COUNSEL 1. Finally, I'd like to make note that the content of what we
7 discuss here today is confidential. We ask that you not speak about what we discuss
8 in this interview to any outside individuals to preserve the integrity of our investigation.

9 For the same reason, the marked exhibits that we will use today will remain
10 with the court reporter so they can go in the official transcripts. And any copies of
11 those exhibits will be collected at the end of the interview.

12 All right. That's the end of my preamble.

13 Is there anything my colleagues from minority would like to add?

14 MINORITY COUNSEL 1. Just thank the witness for taking time out of your
15 schedule to join us today.

16 MAJORITY COUNSEL 1. Mary or Matthew, do you have anything for the record?

17 Ms. Doocy. No.

18 Mr. Hanson. No.

19 MAJORITY COUNSEL 1. Okay. Well, the clock now reads 10:06 a.m.
20 We'll get started with our first hour of questioning.

21 Ms. Dehmlow. Okay.

22 EXAMINATION BY MAJORITY COUNSEL 2:

23 Q Good morning.

24 A Good morning.

25

1 Q Could you state your full name for the record?

2 A Laura Dehmlow.

3 Q Okay. And where do you currently work?

4 A The Federal Bureau of Investigation.

5 Q And what is your current title?

6 A I'm the section chief of the Foreign Influence Task Force.

7 Q And what is the Foreign Influence Task Force?

8 A The Foreign Influence Task Force is a component part in Counterintelligence
9 Division that is charged with understanding and mitigating foreign malign influence
10 operations targeting the United States.

11 Q And how long have you been in that role for?

12 A A bit over 2 years.

13 Q [REDACTED]

14 A [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 Q [REDACTED]

18 A [REDACTED]

19 [REDACTED]

20 Q [REDACTED]

21 A [REDACTED]

22 Q [REDACTED]

23 A [REDACTED]

24 Q [REDACTED]

25 A [REDACTED]

1 A There were -- as I mentioned earlier, we aimed to get together with most of
2 the companies within the couple of weeks in the immediate -- in the immediate weeks
3 preceding the election.

4 Q Are you familiar with the October 2020 New York Post story on Hunter
5 Biden's laptop?

6 A I am.

7 Q Do you recall whether any of these social media companies you were
8 meeting with asked you any questions about it?

9 A I do.

10 Q And what is your recollection? Who --

11 A So I remember having a conversation with or being involved in a
12 conversation with Twitter, and I honestly can't recall if this was repeated to me -- I might
13 have been a few minutes late to the meeting -- or if -- or if I was -- I actually overheard it.

14 But it was -- it was relayed to me later that somebody from Twitter -- I don't recall
15 who. I'm not sure who. Somebody from Twitter essentially asked whether the laptop
16 was real. And one of the FBI folks who was on the call did confirm that, yes, it was
17 before another participant jumped in and said no further comment.

18 Q Do you recall who from the FBI said it was real?

19 A I do.

20 Q And who was that?

21 A It's a non-SES employee. I'd have to take that back.

22 MAJORITY COUNSEL 1. What's their title?

23 Ms. Dehmlow. An analyst.

24 MAJORITY COUNSEL 1. What field office are they out of?

25 Ms. Dehmlow. Again, I'm not sure that I'm allowed to provide details here

1 because it was a non-SES employee.

2 Ms. Doocy. We'll take it back.

3 MAJORITY COUNSEL 1. Can we not know about this, just not the name of the individual?

4 Ms. Doocy. They're in the Criminal Investigative Division. We can tell you that
5 and then get back to you if we can provide a non-SES name.

6 MAJORITY COUNSEL 1. I think the committee would like to know the name of the individual
7 but also their title.

8 Ms. Doocy. Sure.

9 BY MAJORITY COUNSEL 2:

10 Q Was this individual affiliated with FITF?

11 A Again, it was somebody from the Criminal Investigative Division who is
12 embedded with us.

13 Q So yes?

14 A Yes.

15 Q And did this question occur in the context of a bilateral meeting?

16 A It did.

17 Q Do you recall how soon after the story broke that this meeting occurred?

18 A I don't remember. I believe it was the same week, but I don't remember
19 the specific day.

20 BY MAJORITY COUNSEL 1:

21 Q On that call with that IA who's in the Criminal Investigative Division, that was
22 the individual who said, "yes, the laptop is authentic"? Is that correct?

23 A I don't believe it was that specific. Again, I don't recall hearing the
24 conversation itself. I know it was relayed to me afterwards. But my understanding is
25 that we confirmed that, yes, the laptop was a real laptop.

1 Q And then you said another FBI individual came on and said, "No further
2 comment."

3 A Yes.

4 Q Is that correct?

5 A That's correct.

6 Q Who was that individual?

7 A It was some -- it was one of our lawyers who was on the call.

8 Q And who was that individual?

9 A Again --

10 Ms. Doocy. We'll take that request back. They're not SES.

11 MAJORITY COUNSEL 1. Do they work out of the General Counsel's Office or a specific field
12 office?

13 Ms. Doocy. They're in the Office of the General Counsel. But, again, we'll take
14 that request back. We don't have authorization to speak to their specific name in this
15 context.

16 MAJORITY COUNSEL 1. Okay. I think the committee would like to know the individual's
17 name, as well as their title.

18 Thank you.

19 MAJORITY COUNSEL 3 Just to clarify, when you say the laptop was real, you mean it
20 was, like, a real laptop or that it belonged to Hunter Biden or what exactly?

21 Ms. Dehmlow. Since I wasn't -- I don't recall the specifics. I think my
22 understanding is generally we confirmed the existence of the laptop.

23 BY MAJORITY COUNSEL 2:

24 Q Who relayed this information to you?

25 A I don't recall. The reason that I remember it specifically is that we had a

1 conversation afterwards, talking, deliberating on how we would answer the question if
2 another company asked.

3 Q And did this deliberation occur immediately following --

4 A I would say within, yeah, within the next couple of hours.

5 Q During this time period, October 2020, does FITF have its own in-person
6 office? Or is this conversation over Zoom?

7 A Which -- which part of the conversation, the conversation with the
8 companies or the conversation, the deliberations?

9 Q The deliberations.

10 A I believe it happened over our -- our -- our chat function.

11 Q Do you recall how many FBI personnel were part of this deliberation?

12 A I don't.

13 Q Do you have a ballpark sense?

14 A Just a handful probably.

15 Q Do you recall why you were not in attendance at this part of the bilateral
16 meeting?

17 A Again, it's possible that I was. I just don't recall the part. The part that I
18 remember with clarity is the part immediately after that. It's a very busy time. I might
19 have just been running late, a couple of minutes late, you know. It was a very busy time
20 for the FITF.

21 Q Do you know how Twitter reacted when the first agent said that the laptop
22 was real?

23 A No recollection.

24 Q Did you receive any followup requests for information from Twitter?

25 A Not that I recall, not that came to me.

1 Q So you said he was one example.

2 Do you recall other social media companies?

3 A I believe Facebook -- we met with Facebook soon thereafter. Can't
4 remember if it was the same day or within a couple of days. And they also asked, and I
5 said, "No comment." That was the -- that was the decision we made in those
6 post-meeting deliberations, which is pretty typical. It was an ongoing investigation, and
7 we don't generally comment on ongoing investigative matters when asked.

8 Q Okay.

9 MAJORITY COUNSEL 1. Who made the decision that the FBI would have no comment
10 to the social media companies going forward?

11 Mr. Hanson. So I want to be clear.

12 Ms. Dehmlow, obviously, can answer the question as long as it doesn't get into
13 internal deliberations or advice from a lawyer or anything.

14 Ms. Dehmlow. Yeah, and, unfortunately I can't answer that with any further
15 detail on that advice.

16 MAJORITY COUNSEL 1. So you can't tell us who made the decision?

17 Ms. Dehmlow. I can say there were internal deliberations with a number of
18 parties, and then -- but I can't get into that further.

19 MAJORITY COUNSEL 1. So then, Counsel, are you instructing her not to answer the question
20 any further?

21 Ms. Doocy. We'll take the request for the non-SES back and get back to you as
22 soon as possible.

23 MAJORITY COUNSEL 1. And the content of the discussion?

24 Ms. Doocy. So, in this context, she's not authorized to speak to internal
25 deliberations which may implicate attorney-client or other legal privileges today, but we'll

1 take your request back.

2 MAJORITY COUNSEL 1. But you're instructing her not to answer today. Is that accurate?

3 Ms. Doocy. To the specifics of the conversation she received related to whether or not she

4 was deliberating about the veracity of the laptop, in this context, yes.

5 MAJORITY COUNSEL 1. Okay.

6 BY MAJORITY COUNSEL 2:

7 Q With respect to the internal deliberations, were there individuals who

8 participated other than members of FITF?

9 A Yes. Again, I can't get into more specifics because of the deliberative
10 process privilege they're articulating.

11 Q Were there members participating in these deliberations other than
12 members of FITF and other than members of OGC?

13 A I can't recall specifics.

14 Q Do you recall who from Facebook asked the question?

15 A I don't.

16 Q Was the laptop on the agenda for either of these bilateral meetings with
17 Twitter or Facebook?

18 A No. It came as a surprise to us that there was questions. At least it came
19 as a surprise to me. I wasn't tracking the news story until that moment.

20 Q And who else was on the call with Facebook?

21 A It would have been essentially the same -- same folks, probably the unit
22 chiefs from FITF and some range of other folks. But I don't recall specifics.

23 Q You said that you were the one that said "no comment"?

24 A Uh-huh.

25 Q Had it been decided in advance that you'd be the one to answer that

1 question?

2 A No, not that I recall.

3 Q Who was the section chief of FITF at the time?

4 A Bradley Benavides.

5 Q Was he on the call?

6 A Not to my recollection, no.

7 Q Was he on the Twitter call?

8 A Not to my recollection, no.

9 Q Did he usually attend these calls?

10 A He did not.

11 Q Was Elvis Chan on the call with Facebook?

12 A It's likely, but I don't recall specifically.

13 Q Was Elvis Chan on the call with Twitter?

14 A It's likely, but I don't recall specifically.

15 Mr. Jordan. You acknowledged, back to the meeting with Twitter, when the first
16 FBI official acknowledged that the FBI -- that the -- excuse me -- that the laptop was real,
17 how long had you -- how long you had known that information?

18 Ms. Dehmlow. I don't remember. I really can't recall.

19 Mr. Jordan. Did you learn that it week you? Learn it months before? When
20 did you know that the laptop was real?

21 Ms. Dehmlow. I really don't remember.

22 Mr. Jordan. You said -- that's the word you used. You said the agent said the
23 laptop was real. Is that right?

24 Ms. Dehmlow. He confirmed at some point that the laptop existed, yes. But,
25 again, I don't recall the specific language, and I wasn't there.

1 Ms. Doocy. Can I confer with the client for a moment?

2 MAJORITY COUNSEL 1. Yeah, we'll go off the record.

3 [Discussion off the record.]

4 MAJORITY COUNSEL 1. We'll go back on the record.

5 BY MAJORITY COUNSEL 2:

6 Q When the Facebook employee asked the question, do you recall exactly
7 what they asked?

8 A I don't.

9 Q Do you know if it was about the laptop?

10 A Yes. It was essentially whether or not we -- yes, it was something about the
11 laptop. I don't remember -- I know that my answer was "no comment" because -- and
12 the question doesn't stick in my mind because it was something about the laptop. And I
13 said, "No comment."

14 Again, that was not my decision. It wasn't my final call. There were other
15 agency, other departments, other FBI equities at stake, investigative equities, and so
16 pretty typical for us to come to that conclusion.

17 Q Were you aware if Twitter or Facebook were taking steps to censor the
18 story?

19 A I was not.

20 Q Did you ever become aware?

21 A Eventually, when the -- when there was extensive news coverage about it
22 ultimately, but I don't know if I knew it that week, within a couple of months.

23 Q Do you think it was the right decision to say "no comment"?

24 A Not here to -- again, it wasn't my call and it's pretty typical for us to not
25 comment on ongoing investigative equities.

1 Q When the information was relayed to you following the Twitter call that the
2 first agent had said the laptop was real, just to clarify, you knew prior to that
3 conversation that the laptop was real. Is that correct?

4 A I did, yes.

5 Q But you don't recall when approximately you learned.

6 A I don't, sorry.

7 Q Sitting here today, do you know when the FBI first determined that the
8 laptop was real?

9 A I don't. I know that there is some information in the public record
10 regarding when the FBI acquired the laptop, but I don't, sitting here, remember that date.

11 Q Do you know who else at FITF knew that the laptop was real?

12 A I don't actually. I would assume both my -- yes, I would certainly say that
13 Brad Benavides was aware.

14 Q What about the individuals on the Russia unit?

15 A I would assume the unit chief was also aware. I'm pretty certain of that
16 fact.

17 Q For the individual --

18 Mr. Hanson. Just to clarify, do you know to a certainty that they were aware, or
19 are you just making deductions?

20 Ms. Dehmlow. I'm pretty certain that they were aware.

21 Mr. Hanson. Okay.

22 BY MAJORITY COUNSEL 2:

23 Q In advance of the bilateral meeting, would the FITF team discuss internally
24 about what to cover in a meeting?

25 A We would, yes.

1 Q -- that very frequently it wasn't a FITF-owned investigation or equity. Is
2 that right?

3 A I don't think that's what I testified, no.

4 Q Okay.

5 A I said FITF is focused on those actors and those activities, and those activities
6 are inclusive of the information that we're passing to -- to -- to the social media
7 companies. So that was very much a FITF equity. We're program managing those
8 cases.

9 BY MAJORITY COUNSEL 1:

10 Q When you say that the Hunter Biden wasn't a FITF-owned equity --

11 A Uh-huh.

12 Q -- did it have any equities in the FBI investigation of Hunter Biden?

13 A Did what have any equities?

14 Q FITF.

15 A Again, I can't speak to that ongoing investigative action. That's an ongoing
16 investigation. I can't speak to any details regarding it.

17 Q Is that an instruction from counsel?

18 A I think, yes, but they can confirm it.

19 Mr. Hanson. I'd ask you to not respond to any information regarding ongoing
20 investigations.

21 Ms. Dehmlow. I can't speak to ongoing investigations, ongoing investigative
22 activity.

23 BY MAJORITY COUNSEL 2:

24 Q If the ongoing investigation had FITF equities in it, then FITF would be able to
25 share information?

1 A Not broadly. The FITF can only share information in the context of the
2 Justice Manual provision regarding details of foreign malign influence operations. So it's
3 not that we can just broadly share anything regarding an ongoing investigative equity.
4 There's specific provisions of the Justice Manual that govern what we can and cannot
5 share.

6 Q Okay. But, if the Hunter Biden laptop were part of a foreign malign
7 influence operation, that is something that FITF would be able to share information on.

8 A Yeah, I don't want to speak to a hypothetical. But if there is a foreign
9 malign influence operation and we've got specific details about how those actors are
10 propagating information operations, influence operations on platforms, that's something
11 that we could share the specific details of.

12 Q Okay. I mean, that sounds like a "yes" to my previous question but --

13 A I want to be really specific about what we do and don't do because we don't
14 just comment broadly on investigative activity.

15 MAJORITY COUNSEL 1. So did FITF share any information with social media companies
16 regarding the Hunter Biden investigation as it relates to foreign malign activity?

17 Ms. Doocy. Same instruction.

18 Ms. Dehmlow. Yeah.

19 MAJORITY COUNSEL 1. What's the instruction, Mary?

20 Ms. Doocy. Not to comment on ongoing investigations.

21 MAJORITY COUNSEL 1. Thanks.

22 BY MAJORITY COUNSEL 2:

23 Q So, in these bilateral FITF meetings, social media companies, is it fair to say it
24 was routine that they would be receiving information related to foreign malign influence
25 operations that related to investigations of the FBI?

EXHIBIT 15

COMMITTEE ON THE JUDICIARY,
U.S. HOUSE OF REPRESENTATIVES,
WASHINGTON, D.C.

INTERVIEW OF: DAVID AGRANOVICH

Tuesday, May 16, 2023

Washington, D.C.

The interview in the above matter was held in room 2237, Rayburn House Office Building, commencing at 9:59 a.m.

Present: Representatives Jordan and Gaetz.

Appearances:

For the COMMITTEE ON THE JUDICIARY:

[REDACTED] COUNSEL

[REDACTED] PRESS ASSISTANT

[REDACTED] CHIEF COUNSEL FOR ADMINISTRATIVE LAW

[REDACTED] CHIEF COUNSEL FOR POLICY AND STRATEGY

[REDACTED] CHIEF COUNSEL FOR OVERSIGHT

[REDACTED] RESEARCH ASSISTANT

[REDACTED] DIGITAL DIRECTOR

[REDACTED] SENIOR SPECIAL COUNSEL

[REDACTED] COUNSEL

[REDACTED] MINORITY INTERN

[REDACTED] MINORITY FELLOW

[REDACTED] MINORITY DEPUTY CHIEF COUNSEL FOR THE SUBCOMMITTEE ON CRIME

AND FEDERAL GOVERNMENT SURVEILLANCE

[REDACTED] MINORITY CHIEF COUNSEL FOR THE SUBCOMMITTEE ON CRIME AND

FEDERAL GOVERNMENT SURVEILLANCE

[REDACTED] MINORITY STAFF ASSISTANT

For DAVID AGRANOVICH:

RIDGE BLANCHARD

REGINALD BROWN

Kirkland & Ellis

1301 Pennsylvania Avenue, N.W.

Washington, D.C. 20004

MAJORITY COUNSEL 1. We'll go on the record.

This is a transcribed interview of David Agranovich. Chairman Jordan has requested this interview as part of the committee's investigation of how and the extent to which the executive branch has coerced and colluded with companies and other intermediaries to censor speech.

Would the witness please state his name for the record.

Mr. Agranovich. David Agranovich.

MAJORITY COUNSEL 1. On behalf of the committee, I want to thank you for appearing here today to answer our questions. The chairman also appreciates your willingness to appear voluntarily.

My name is [REDACTED] [REDACTED] and I'm with Chairman Jordan's staff.

I will now have everyone else from the committee who is here at the table introduce themselves as well.

MAJORITY COUNSEL 2. [REDACTED] counsel for Chairman Jordan's staff.

MAJORITY COUNSEL 3. [REDACTED] with Chairman Jordan's staff.

MINORITY COUNSEL 1. [REDACTED] with Chair Nadler's staff.

MINORITY COUNSEL 2. [REDACTED] with Mr. Nadler's staff.

[REDACTED] [REDACTED] [REDACTED] with Ranking Member Nadler.

[REDACTED] [REDACTED] [REDACTED] Jim Jordan's staff.

[REDACTED] [REDACTED] [REDACTED] with Chairman Jordan's staff.

[REDACTED] [REDACTED] [REDACTED] Chairman Jordan's staff.

[REDACTED] [REDACTED] [REDACTED] majority.

Mr. Blanchard. I'm Ridge Blanchard with Kirkland & Ellis.

Mr. Brown. Reg Brown -- Reginald Brown for Kirkland & Ellis for the witness and

Meta.

[REDACTED]

[REDACTED] And I also noticed a couple of additional people came in the room.

MAJORITY COUNSEL 1. Yeah. If the folks who came in would state their name for the record.

Mr. Gaetz. Matt Gaetz, majority member of the House Judiciary Committee.

[REDACTED] majority.

MAJORITY COUNSEL 1. Thank you. I'd like to --

MINORITY COUNSEL 2. If I can ask for you all to speak up a little bit. I'm having

a little bit of trouble hearing you.

MAJORITY COUNSEL 1. Sure.

I'd like to now go over the ground rules and guidelines that we'll follow during today's interview.

Our questioning will proceed in rounds. The majority will ask questions first for 1 hour, and then the minority will have an opportunity to ask questions for an equal period of time if they choose. We will alternate back and forth until there are no more questions and the interview is over.

Typically, we take a short break at the end of each hour, but if you would like to take a break apart from that, please just let us know.

As you can see, there are official court reporters taking down everything we say to make a written record, so we ask that you give verbal responses to all questions.

Do you understand?

Mr. Agranovich. Yes.

MAJORITY COUNSEL 1. So the court reporters can take down a clear record, we will do our best to limit the number of people directing questions at you during any given hour to just those people on the staff whose turn it is. Please try and speak clearly so the court reporter can understand and so the folks down at the end of the table can hear you.

It's important that we don't talk over one another or interrupt each other if we can help it, and that goes for everybody present at today's interview.

We encourage witnesses who appear before the committee to freely consult with counsel if they so choose. It is my understanding that you are appearing today with counsel. Is that correct?

Mr. Agranovich. That is correct.

MAJORITY COUNSEL 1. Could counsel please state your name for the record.

Mr. Brown. We have already done that. Reginald Brown, Kirkland & Ellis.

Mr. Blanchard. Ridge Blanchard, Kirkland & Ellis.

MAJORITY COUNSEL 1. Thank you.

We want you to answer our questions in the most complete and truthful manner as possible, so we will take our time. If you have any questions or if you do not understand one of our questions, please let us know.

Our questions will cover a wide range of topics, so if you need clarification at any point, just say so. If you honestly don't know the answer to a question or do not remember, it's best not to guess. Please give us your best recollection, and it's okay to tell us if you learned information from someone else. Just indicate how you came to know the information.

If there are things you don't know or can't remember, just say so, and please inform us who, to the best of your knowledge, might be able to provide a more complete answer to the question.

You should also understand that although this interview is not under oath, by law, you are required to answer questions from Congress truthfully.

Do you understand that?

Mr. Agranovich. Yes.

MAJORITY COUNSEL 1. This also applies to questions posed by congressional staff in an interview.

Do you understand that as well?

Mr. Agranovich. I do.

MAJORITY COUNSEL 1. Witnesses that knowingly provide false testimony could be subject to criminal prosecution for perjury or for making false statements under 18

U.S.C., section 1001.

Do you understand this?

Mr. Agranovich. I do.

MAJORITY COUNSEL 1. Is there any reason you are unable to provide truthful answers to today's questions?

Mr. Agranovich. No.

MAJORITY COUNSEL 1. Finally, I'd like to make note that the content of what we discuss here today is confidential. We ask that you not speak about what we discuss in this interview to any outside individuals to preserve the integrity of our investigation.

For the same reason, the marked exhibits that we will use today will remain with the court reporters so that they can go in the official transcript, and any copies of those exhibits will be returned to us when we wrap up.

All right. That's the end of my preamble. Is there anything that my colleagues --

Mr. Brown. [REDACTED] someone else came into the room. I just want to make sure we get names.

[REDACTED] Hi. I'm [REDACTED] I'm with the House Judiciary minority.

Mr. Brown. I'm sorry?

[REDACTED] [REDACTED]

Mr. Brown. [REDACTED]

MAJORITY COUNSEL 1. Is there anything my colleagues from the minority would like to add?

MINORITY COUNSEL 2. No, thank you.

MAJORITY COUNSEL 1. Okay. The clock now reads 10:06. We'll start the first hour of questioning.

MAJORITY COUNSEL 2. Great.

EXAMINATION

BY MAJORITY COUNSEL 2:

Q Thank you, Mr. Agranovich.

Could you state your full name, please.

A Yes. My full name is David Jacob Agranovich.

Q And where's your current place of employment?

A I currently work at Meta.

Q Okay. What's your current title?

A I'm Meta's director for global threat disruption.

Q [REDACTED]

MINORITY COUNSEL 1. I'm sorry. We can't hear you.

MINORITY COUNSEL 2. We can't hear you.

MAJORITY COUNSEL 2:

Q [REDACTED]

A [REDACTED]

Q Okay. Great. Your counsel started to provide some of this. At a high level, could you provide your employment history?

A Yes. So I currently work at Meta as Meta's Director for Global Threat Disruption. And I joined the company as Meta's Global Threat Disruption Lead.

[REDACTED]

[REDACTED]

condensing that down to coordinated inauthentic behavior.

A Uh-huh.

Q Were there other policies that you consulted with the government on?

A Not that I can recall. Yeah, not that I can recall.

Q You said that hack-and-leak concerns, hack-and-leak operations, that would fall under your team's purview.

A The hack-and-leak policy specifically would fall under our team's purview.

Q Is that a policy you worked on directly?

A Yes.

Q How has it changed since you first joined Meta?

A The hack-and-leak, as you can imagine, hack-and-leak has been an issue that security teams, not just ours but across industry and government, have been focused on for several years now.

There were hack-and-leak operations that were identified going back to 2016, linked to Russian military intelligence services. There were hack-and-leak operations targeting the Macron election in France after that. And then there have been a number of hack-and-leak operations linked to a number of different foreign intelligence actors in countries all over the world since then.

So, naturally, hack-and-leak was one of the various threat factors that we were focused on and wanted to make sure that we were both keeping abreast of and being cautious to make sure we weren't allowing the platform to be manipulated in any way.

And so the hack-and-leak policy which we had developed functionally focused on three main areas.

So, first, determining whether the material that we were evaluating was obtained by a hacked, from a hacked source; i.e., was it obtained by someone without

authorization to access that material?

Second was the material being disseminated with an intent to deceive? And that functionally on our platform, what that would mean is, is there indicia of deception, is there fake account usage or fake accounts being used to disseminate the material?

And then, third, was the material being disseminated on behalf of or at the direction of a foreign government influence operation?

And so that's the three-part test of the hack-and-leak policy, and that's functionally what the policy was in my time at Meta.

Q And was that -- so that was the case when you first started back in 2018 to today? When did this three-part test come into being?

A To the best of my recollection, the policy was developed in early to mid-2020.

Q And what was --

MINORITY COUNSEL 2. I'm sorry? When?

Mr. Agranovich. In early to mid-2020?

BY MAJORITY COUNSEL 2:

Q And what was the policy before then?

A I understand there are other policies at the company that can apply to hacked materials. They're not policies that I work on, but I know that those existed prior to the hack-and-leak policy being developed.

Q And did you ever consult with the government regarding your -- or regarding Meta's hack-and-leak policy?

A I recollect that we discussed the fact of us working on hack-and-leak issues in meetings with the government, but I don't believe we consulted with the government on the policy itself.

Q Okay. Did the government ever contact you to comment on your hack-and-leak policy?

A Not to my recollection.

MAJORITY COUNSEL 2. Do you know where we are on time?

MAJORITY COUNSEL 3. You have about a minute.

Mr. Brown. You have about a minute and 37 seconds left.

BY MAJORITY COUNSEL 1:

Q When did those meetings occur?

A Which meetings?

Q The meetings you just referenced where there was a discussion of Meta's hack-and-leak policy with the government?

A I believe the summer of 2020.

Q And which entities were those discussions happening with?

A That would be the Foreign Influence Task Force, DHS, CISA, and ODNI.

MAJORITY COUNSEL 2. Were these one-on-one meetings or were other companies invited as well?

Mr. Agranovich. These meetings, these were multiple companies, and then the government agencies I mentioned.

MAJORITY COUNSEL 2. Do you remember who instigated these meetings? Was it on the government end, or was it from industry's end?

Mr. Agranovich. I don't know who instigated the meetings.

Mr. Brown. We're at time. I was wondering if we could take a break off the record. Thanks.

[Recess.]

MINORITY COUNSEL 2. We're ready to go back on the record.

EXHIBIT 16

1

2

3

4

5 COMMITTEE ON THE JUDICIARY,

6 U.S. HOUSE OF REPRESENTATIVES,

7 WASHINGTON, D.C.

8

9

10

11

12

13 INTERVIEW OF: NATHANIEL GLEICHER

14

15

16

17

18

Wednesday, June 21, 2023

19

20

Washington, D.C.

21

22

23

The interview in the above matter was held in room 164, Cannon House Office

24

Building, commencing at 10:05 a.m.

25

1 Appearances:

2

3

4 For the COMMITTEE ON THE JUDICIARY:

5

6 [REDACTED] COUNSEL

7 [REDACTED] DIGITAL ASSISTANT

8 [REDACTED] PROFESSIONAL STAFF MEMBER

9 [REDACTED] SENIOR SPECIAL COUNSEL

10 [REDACTED] COUNSEL

11 [REDACTED] MINORITY INTERN

12

13

14

15 For the SUBCOMMITTEE ON CRIME AND

16 FEDERAL GOVERNMENT SURVEILLANCE:

17

18 [REDACTED] MINORITY DETAILEE

19

20 For NATHANIEL GLEICHER:

21 REGINALD BROWN, ESQ.

22 JORDAN GREENE

23 Kirkland Ellis

1

2 MAJORITY COUNSEL 1. We can go on the record.

3 MAJORITY COUNSEL 2. This is a transcribed interview of Nathaniel Gleicher.

4 Is that how you pronounced it?

5 Mr. Gleicher. Gleicher.

6 MAJORITY COUNSEL 2. Chairman Jordan has requested this interview as part of

7 the committee's investigation of how and the extent to which the executive branch has

8 coerced and colluded with companies and other intermediaries to censor speech.

9 Would the witness please state your name for the record?

10 Mr. Gleicher. Nathaniel Jurist Gleicher.

11 MAJORITY COUNSEL 2. On behalf of the committee, I want to thank you for

12 appearing here today to answer our questions. The chairman also appreciates your

13 willingness to appear voluntarily.

14 My name is [REDACTED] and I'm with Chairman Jordan's staff.

15 We'll now have everyone else from the committee who is here at the table to

16 introduce themselves, as well.

17 MAJORITY COUNSEL 1. [REDACTED] Chairman Jordan's staff.

18 [REDACTED] [REDACTED] Chairman Jordan's staff.

19 [REDACTED] [REDACTED], Chairman Jordan's staff.

20 [REDACTED] [REDACTED] Chairman Jordan's staff.

21 MINORITY COUNSEL 1. [REDACTED] Chairman Nadler's staff.

22 [REDACTED] [REDACTED] Legal Intern, House Judiciary, Democratic staff.

23 MAJORITY COUNSEL 2. I would like to now go over the ground rules and

24 guidelines that we will follow during today's interview.

25 Our questioning will proceed in rounds. The majority will ask questions first for 1

1 hour, and then the minority will have an opportunity to ask questions for an equal period
2 of time if they choose. We will alternate back and forth until there are no more
3 questions, and then our interview is over.

4 Typically, we take a short break at the end of each hour. But if you would like to
5 take a break apart from that, please just let us know.

6 As you can see, there's an official court reporter taking down everything you say
7 to make a written record. So we ask you give verbal responses to all questions.

8 Do you understand?

9 Mr. Gleicher. Yes.

10 MAJORITY COUNSEL 2. So the court reporter can take down a clear record, we
11 will do our best to limit the number of people directing questions at you during any given
12 hour to just those people on the staff whose turn it is.

13 Please try and speak clearly so the court reporter can understand and so the folks
14 down at the end of the table can hear you. It's important that we don't talk over one
15 another or interrupt each other if we can help it, and that goes for everybody present at
16 today's interview.

17 We encourage witnesses who appear before the committee to freely consult with
18 counsel if they so choose, and it's my understanding you are appearing today with
19 counsel. Is that correct?

20 Mr. Gleicher. Correct.

21 MAJORITY COUNSEL 2. Could counsel please state your name for the record?

22 Mr. Brown. Reg Brown, Kirkland & Ellis.

23 Mr. Greene. Jordan Greene, Kirkland & Ellis.

24 MAJORITY COUNSEL 2. Thank you.

25 We want you to answer our questions in the most complete and truthful manner

1 as possible. So we will take our time. If you have any questions or if you don't
2 understand one of our questions, please let us know.

3 Our questions will cover a wide range of topics. So if you need clarification at
4 any point, just say so. If you honestly don't know the answer to a question or don't
5 remember, it's best not to guess. Please give us your best recollection, and it's okay to
6 tell us if you learn information from someone else. Just indicate how you came to know
7 the information.

8 If there are things you don't know or can't remember, just say so and please
9 inform us who, to the best of your knowledge, might be able to provide a more complete
10 answer to the question.

11 You should also understand that, although this interview isn't under oath, by law,
12 you are required to answer questions from Congress truthfully.

13 Do you understand?

14 Mr. Gleicher. Yes.

15 MAJORITY COUNSEL 2. This also applies to questions posed by congressional
16 staff in an interview.

17 Do you understand?

18 Mr. Gleicher. Yes.

19 MAJORITY COUNSEL 2. Witnesses who knowingly provide false testimony could
20 be subject to criminal prosecution for perjury, or making false statements under 18
21 United States Code 1001.

22 Do you understand?

23 Mr. Gleicher. Yes.

24 MAJORITY COUNSEL 2. Is there any reason you are unable to provide truthful
25 answers to today's questions?

1 Mr. Gleicher. No.

2 MAJORITY COUNSEL 2. Finally, I would like to note that the content of what we
3 discuss here today is confidential. We ask that you not speak about what we discuss in
4 this interview to any outside individuals to preserve the integrity of our investigation.

5 For the same reason, the marked exhibits that we use today will remain with the
6 court reporter so that they can go in the official transcript. And any copies of those
7 exhibits will be returned to us when we wrap up.

8 All right. That's the end of my preamble.

9 Is there anything my colleagues from the minority would like to add?

10 MINORITY COUNSEL 1. Not at this time, no.

11 I will -- I just want to alert everybody one of my colleagues will coming in to hand
12 me something, [REDACTED]. And then she'll just be leaving.

13 MAJORITY COUNSEL 2. Okay.

14 MINORITY COUNSEL 1. Thanks.

15 MAJORITY COUNSEL 2. The clock now reads 10:05 a.m. We will start the first
16 hour of questioning.

17 EXAMINATION

18 BY MAJORITY COUNSEL 1:

19 Q Mr. Gleicher, what's your current place of employment?

20 A I work at Meta.

21 Q And what's your current title?

22 A I am head of security policy.

23 Q [REDACTED]

24 A [REDACTED]

25 Q [REDACTED]

1 Q You mentioned the community standards. Is the hack-and-leak policy
2 separate from the CIB policy?

3 A Yes.

4 Q Can you state again if your team has primary responsibility for the
5 enforcement of the hack and leak policy?

6 A Yes.

7 Q Do you know when that policy was first adopted?

8 A I believe it was adopted -- I don't remember the exact date but it was sort of
9 mid-2020.

10 Q Did you work on the development of that policy?

11 A Yes.

12 Q And do you recall which other teams, if any, from Facebook were involved in
13 the development of that policy?

14 A I don't know about specific teams. But within [REDACTED]'s org, there
15 were a number of people thinking about issues around the 2020 elections at that time.

16 Q So is it concern about the 2020 elections that led Facebook to adopt a
17 hack-and-leak policy?

18 A In part, yes.

19 Q What specifically about the 2020 election?

20 A As we were preparing for the 2020 elections, we identified that one of the
21 likely risks it was important to prepare for was a hack-and-leak campaign from a foreign
22 threat actor like Russia.

23 Q And by "we," do you mean Facebook?

24 [Discussion off the record.]

25 Mr. Gleicher. My apologies. Could you say that again?

EXHIBIT 17

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 9/29/2020 11:41:42 AM
To: Matthew Masterson [REDACTED]@hq.dhs.gov]; Brian Scully [REDACTED]@cisa.dhs.gov]
CC: [REDACTED]@cisa.dhs.gov; [REDACTED]@cisa.dhs.gov; [REDACTED] [REDACTED]@fb.com]
BCC: [REDACTED] [REDACTED]@fb.com]
Subject: October 2020 USG/Industry Meeting (Draft Agenda)

Gents,

We wanted to share the draft/proposed agenda in advance of our USG/Industry meeting scheduled from 2:00-3:30 PM EST on Wednesday, October 7th. Additionally, to facilitate the logistics for the call, we have included the dial-in information below.

Please let us know if you have any additions or concerns.

Thanks!

[REDACTED]

*****DRAFT AGENDA*****


- 10 minutes: Dial In/Opening
30 minutes: Threat Updates (Including Pre/Post Presidential Debates)
Threat update from USG -- Foreign Actor/Activity & Non-IO Cyber Threats
Threat update from industry (FB, Twitter, GOOG)
40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
Updates on USG Election Process
Election Day Virtual Coordination Center Update
Top 5 Delegitimization Claims To Counter
Hack/Leak Concerns
10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

Meeting Dial-In Information:

- To join the meeting on a computer or mobile phone: https://bluejeans.com/[REDACTED]
One-Touch: [REDACTED]
Meeting ID: [REDACTED]
Participant Passcode: [REDACTED]
To join via phone:
1) Dial: [REDACTED]
2) Enter Conference ID: [REDACTED]
3) Enter Participant Passcode: [REDACTED]
Want to test your video connection?
https://bluejeans.com/111

EXHIBIT 18

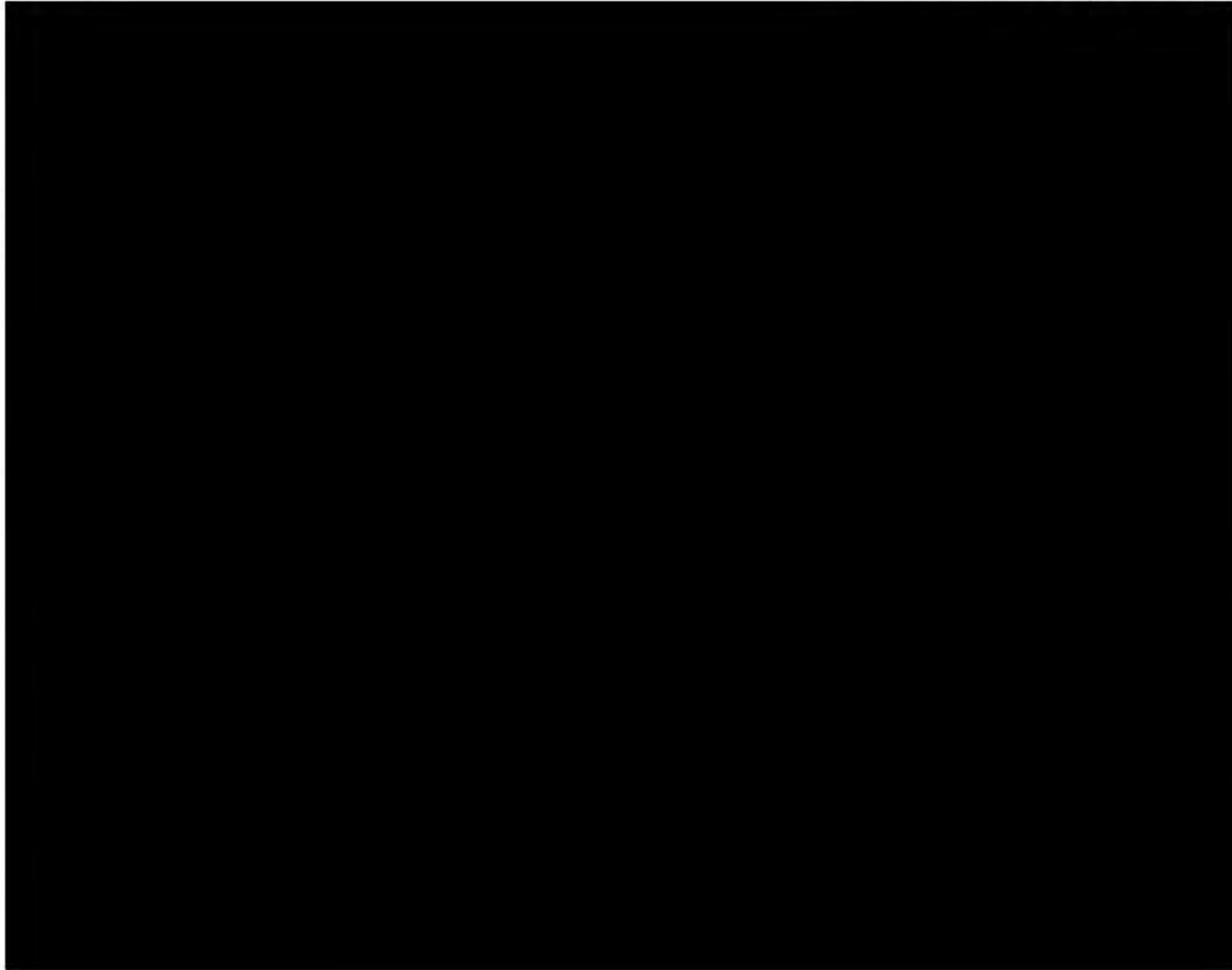
Hack/Leak Investigation (AC/PRIV)

Encrypted C#215252 Info Operations Investigation (3)  Matt Richard Unpublished **High** Created Oct 15, 2020 [More](#)

[Overview](#) [Timeline](#) [Assets](#) [Actions](#) [Discussion](#) [Files](#) [Access Requests](#) **1** [Intelligence Notes](#) [Providence](#) [Searchlight](#)

Discussion

[Add Work Chat Thread](#) [Activity & Comments](#)





[Redacted Name]

I spoke with SSA Elvis Chan (FBI San Francisco) on 15 October 2020, as a follow up to the call with the Foreign Influence Task Force on 14 October. I asked SSA Chan whether there was any update or change since the discussion on 14 October 2020 as to whether the FBI saw any evidence suggesting foreign sponsorship or direction of the leak of information related to Hunter Biden as published in the New York Post story on 14 October. SSA Chan advised that he was up to speed on the current state of the matter within the FBI and that there was no current evidence to suggest any foreign connection or direction of the leak. SSA Chan assured that the FBI would be in contact if any additional information on this was developed through further investigation.

October 15, 2020 · Like · Reply

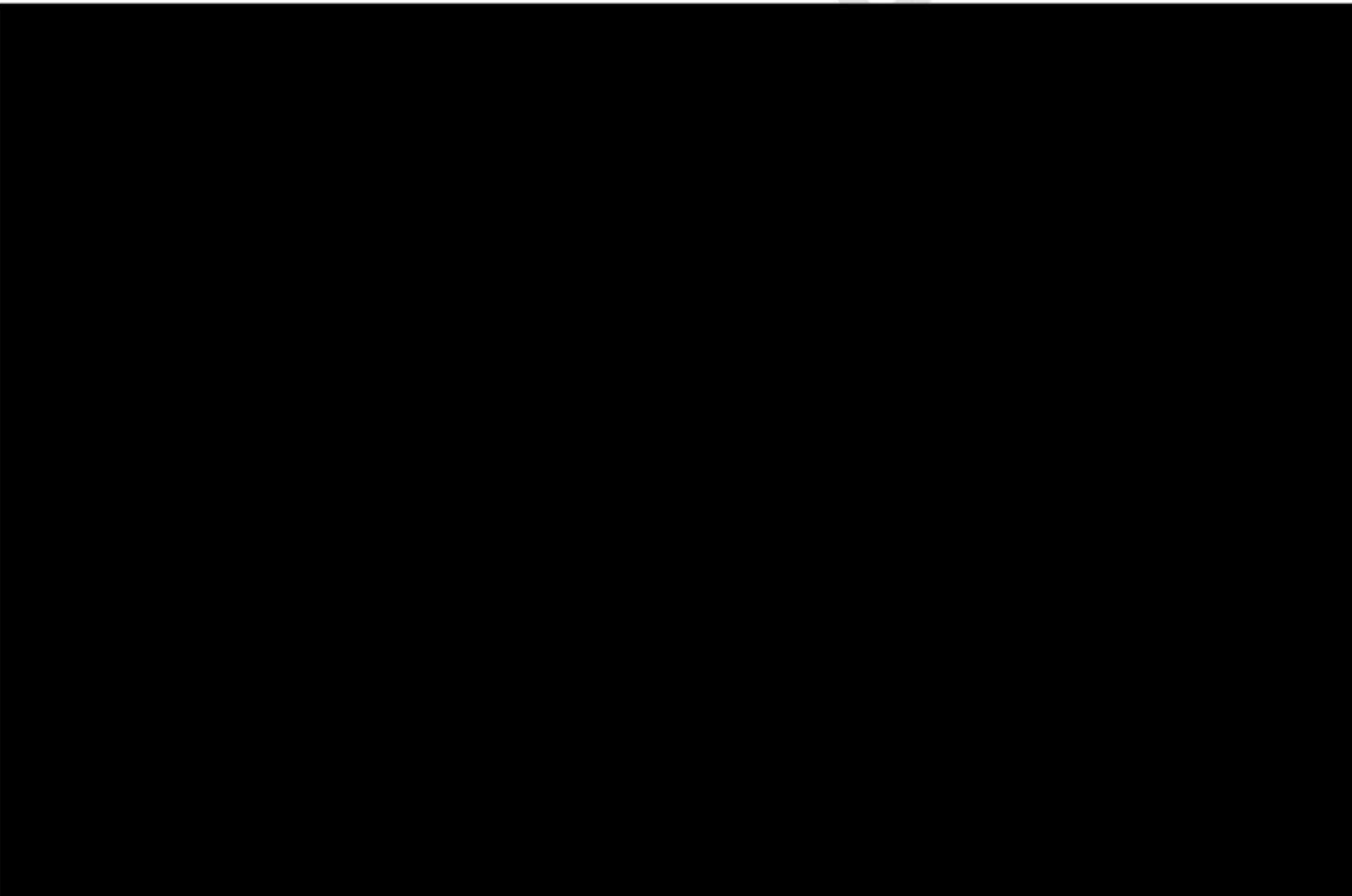
[Redacted Name] subscribed [Redacted Name]

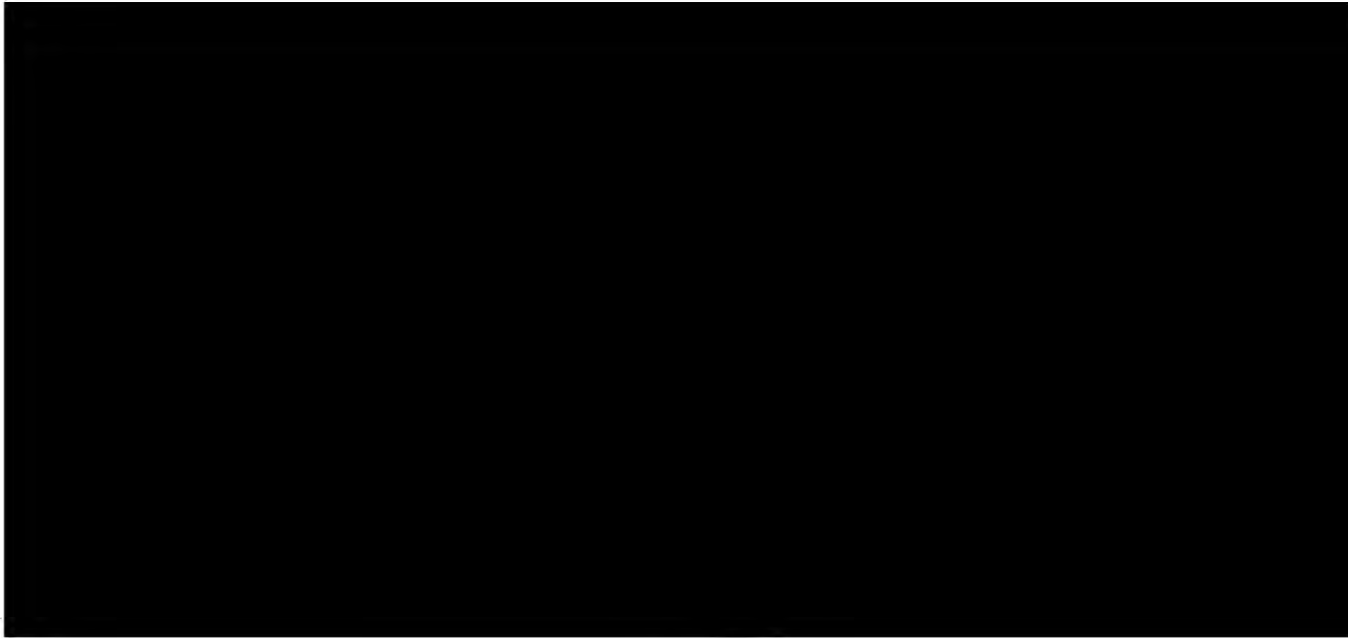
October 15, 2020 · Like



[Redacted Name] Here is where I will be working through the various hack/leak policy factors: [https://fb.quip.com/\[Redacted\]](https://fb.quip.com/[Redacted])

October 15, 2020 · Like · Reply





Produced

EXHIBIT 19

From: Misinformation Reports [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=093D02C79B0F4DBA805C5322CD750647-MISINFORMATION]
Sent: 10/27/2022 5:06:15 PM
To: [REDACTED]@fb.com' [REDACTED]@fb.com]; 'reports@content.facebook.com' [reports@content.facebook.com]
CC: [REDACTED]@pa.gov' [REDACTED]@pa.gov]; [REDACTED]@pa.gov' [REDACTED]@pa.gov]
Subject: FW: Misleading Post about Election Results Timing (Ticket 1027-02)

Please see below report submitted to the EI-ISAC.

EI-ISAC
31 Tech Valley Drive
East Greenbush, NY 12061

elections@cisecurity.org
[REDACTED]

[Report an incident](#)



From: [REDACTED] <[REDACTED]@pa.gov>
Sent: Thursday, October 27, 2022 4:55 PM
To: Misinformation Reports <misinformation@cisecurity.org>
Cc: [REDACTED] <[REDACTED]@pa.gov>
Subject: [External] Misleading Post about Election Results Timing

Summary: Misleading Post about Election Results Timing

Description: This post is misleading to voters. It is insinuating that because election results are not available on election night, something nefarious is happening in the counting process.

Name and Title: Scott Parker, Digital Director of the PA Department of State

Jurisdiction: Pennsylvania

Platform: Twitter and Facebook

URL: <https://twitter.com/tedcruz/status/1585671399133282304>

<https://www.facebook.com/tedcruzpage/posts/pfbid0hGVnZAx6uqspQuAVCRSeDszwyVabVJBUVuxd7mmKhrspvF9yRn3Tr7ViapH2j74ul>

Seen on: 10/27/2022

Screenshot:



Ted Cruz
@tedcruz

Why is it only Democrat blue cities that take “days” to count their votes?

The rest of the country manages to get it done on election night.

New York Post @nypost · 17h

Pennsylvania election results could take 'days,' secretary of the commonwealth says trib.al/OKni8Pg



12:34 PM · Oct 27, 2022 · Twitter for iPhone

1,746 Retweets 481 Quote Tweets 7,880 Likes



██████████ | Digital Director (he/him/his)
Office of Press and Communications
Department of State
401 North Street, Harrisburg, PA 17120
Office: ██████████
Are you ready to vote on November 8, 2022?
dos.pa.gov | vote.pa.gov | [Facebook](#) | [Twitter](#)

.....

EXHIBIT 20

From: Kate Starbird <[REDACTED]@uw.edu>
To: Alex Stamos <[REDACTED]@stanford.edu>
Subject: Re: Election research collaboration - chat this afternoon?
Date: Wed, 8 Jul 2020 10:26:21 -0700

Hi Alex,

Happy to chat. I'm booked solid this afternoon. Could we do something tomorrow afternoon? I could do something between 2 and 3pm tomorrow or after 5pm...

Kate

On Jul 8, 2020, at 9:41 AM, Alex Stamos <[REDACTED]@stanford.edu> wrote:

Hey, Kate-

Do you have any time this afternoon to chat? We are working on some election monitoring ideas with CISA and I would love your informal feedback before we go too far down this road.

Sorry for the last minute ask, but things that should have been assembled a year ago are coming together quickly this week.

Alex

--

Alex Stamos

Director, Stanford Internet Observatory

[REDACTED]@stanford.edu

EXHIBIT 21

[External] EIP-833 Case #CIS-MIS000164: inaccurate number of rejected absentee ballots in DeKalb County, GA

From: Elena Cryst [Redacted - Personal Information]
To: [Redacted - Personal Information]
Bcc: [Redacted - Personal Information]
Date: Wed, 04 Nov 2020 19:41:38 -0600

Reply above this line.

Elena Cryst shared this with your organization.

View the request and select **Get notifications** to follow along.

[View request](#) · [Turn off this request's notifications](#)

This is shared with TikTok, Facebook, EI-ISAC, Twitter, CIS Misinformation Reporting, and CISA CFITF

Powered by Jira Service Desk

EXHIBIT 22



reddit.com>

Re: EIP-651 Livestream of "riots" between Trump and Biden supporters

1 message

reddit.com>
To: Alex Stamos <@stanford.edu>

Tue, Nov 3, 2020 at 12:36 PM

Thanks. Unfortunately as we mentioned at the beginning of this project we are unable to participate in external jiras, but we are happy to receive info over email.

On Tue, Nov 3, 2020 at 12:35 PM Alex Stamos <@stanford.edu> wrote:

There is a widely watched YouTube livestream replaying old videos and claiming they are of live violence in the streets between Biden and Trump supporters. YouTube is looking into it, but here are the Reddit links we found:

https://www.reddit.com/r/Bad_Cop_No_Donut/comments/jnfnw/ive_us_e_ection_protests_riots_trump_vs_biden/
https://www.reddit.com/r/ThatsInsane/comments/jnfo0a/ive_us_e_ection_protests_riots_trump_vs_biden/

It would be great if we could get somebody from Reddit on the JIRA, just like Facebook, Google, Twitter, TikTok, Instagram, CISA, EI-ISAC...

From: <reddit.com>
Date: Tuesday, November 3, 2020 at 12:31 PM
To: Alex Stamos <@stanford.edu>
Subject: Re: EIP-651 Livestream of "riots" between Trump and Biden supporters

Me again. :) T;DR please?

On Tue, Nov 3, 2020 at 12:29 PM Alex Stamos <jira@2020partnership.atlassian.net> wrote:

Reply above this line.

Alex Stamos shared this with your organization.

View the request and select **Get notifications** to follow along.

[View request](#) · [Turn off this request's notifications](#)

This is shared with Reddit, Google, Twitter, and

Powered by Jira Service Desk

Director of Policy
Reddit
reddit.com

Director of Policy
Reddit
reddit.com

EXHIBIT 23

Message

From: Elena Cryst [jira@2020partnership.atlassian.net]
Sent: 11/2/2020 7:03:06 PM
To: [REDACTED]@google.com
Subject: EIP-556 Tweets and edited recordings of Zoom call(s) claim to show federal employees and contractors conspiring to leak info, shutdown DC, and label results as a coup after election

Reply above this line.

Elena Cryst shared this with your organization.

View the request and select **Get notifications** to follow along.

[View request](#) - Turn off this request's notifications

This is shared with Reddit, GEC, Facebook, 2 other organizations, and William Beebe.

Powered by Jira Service Desk

Confidential - Not For Public Release

EXHIBIT 24

1

2

3

4

5 COMMITTEE ON THE JUDICIARY,

6 U.S. HOUSE OF REPRESENTATIVES,

7 WASHINGTON, D.C.

8

9

10

11

12

13 INTERVIEW OF: ALEXANDER STAMOS

14

15

16

17

18

June 23, 2023

19

20

Washington, D.C.

21

22

23 The interview in the above matter was held in room 2237, Rayburn House Office

24 Building, commencing at 9:30 a.m.

25

Present: Representative Jordan

1

2 Appearances:

3

4

5 For the COMMITTEE ON THE JUDICIARY:

6

7 [REDACTED] LAW CLERK

8 [REDACTED] DIGITAL ASSISTANT

9 [REDACTED] CHIEF COUNSEL FOR OVERSIGHT

10 [REDACTED] SENIOR SPECIAL COUNSEL

11 [REDACTED] DIGITAL DIRECTOR

12 [REDACTED] SENIOR SPECIAL COUNSEL

13 [REDACTED] COUNSEL

14 [REDACTED] MINORITY OVERSIGHT COUNSEL

15 [REDACTED] MINORITY INTERN

16 [REDACTED] MINORITY CHIEF OVERSIGHT COUNSEL

17 [REDACTED] MINORITY PROFESSIONAL STAFF MEMBER

18

19

20 For the SUBCOMMITTEE ON THE CONSTITUTION AND LIMITED GOVERNMENT:

21

22 [REDACTED] MINORITY DEPUTY CHIEF COUNSEL

1

2 For ALEXANDER STAMOS:

3

4 JOHN B. BELLINGER, III, ESQ.

5 CALEB THOMPSON, ESQ.

6 ARNOLD & PORTER KAYE SCHOLER, LLP

7 601 Massachusetts Ave, NW

8 Washington, DC 20001

1

2 MAJORITY COUNSEL 1. We'll go on the record.

3 Good morning. This is a transcribed interview of Mr. Alex Stamos. Chairman
4 Jordan has requested this interview as part of the committee's investigation of how and
5 the extent to which the executive branch has coerced and colluded with companies and
6 other intermediaries to censor speech.

7 Would the witness please state your name for the record?

8 Mr. Stamos. Alexander Stamos.

9 MAJORITY COUNSEL 1. We encourage witnesses who appear before the
10 committee to freely consult with counsel if they so choose, and it is my understanding
11 that you are appearing today with counsel. Is that correct?

12 Mr. Stamos. Yes.

13 MAJORITY COUNSEL 1. Could counsel please state your name for the record?

14 Mr. Bellinger. John Bellinger, Arnold & Porter.

15 Mr. Thompson. Caleb Thompson, Arnold & Porter.

16 MAJORITY COUNSEL 1. Thank you.

17 On behalf of the committee, I want to thank you for appearing here today to
18 answer our questions. The chairman also appreciates your willingness to appear
19 voluntarily.

20 My name is [REDACTED] and I am with Chairman Jordan's staff.

21 I will now have everyone else in the room who is with the committee introduce
22 themselves as well.

23 MAJORITY COUNSEL 2. [REDACTED] with Chairman Jordan's staff.

24 MAJORITY COUNSEL 3. [REDACTED] Chairman Jordan's staff.

25 MINORITY COUNSEL 1. [REDACTED] chief oversight counsel for the House

1 Judiciary Democratic staff.

2 [REDACTED] [REDACTED] House Judiciary Democratic staff.

3 [REDACTED] [REDACTED] [REDACTED] House Judiciary Democratic staff.

4 [REDACTED] [REDACTED] House Judiciary Democratic staff.

5 [REDACTED] [REDACTED] House Judiciary Democratic staff.

6 [REDACTED] [REDACTED] Mr. Jordan's staff.

7 [REDACTED] [REDACTED] Chairman Jordan's staff.

8 MAJORITY COUNSEL 1. Thank you.

9 I would now like to go over the ground rules and guidelines that we will follow
10 during today's interview. Our questioning will proceed in rounds. The majority will ask
11 questions first for 1 hour, and then the minority will have an opportunity to ask questions
12 for an equal period of time if they so choose.

13 We will alternate back and forth until there are no more questions and the
14 interview is over. Typically we take a break at the end of each hour, but if you would
15 like to take a break apart from that, please just let us know.

16 As you can see, there's an official court reporter taking down everything we say to
17 make a written record, so we ask that you give verbal responses to all questions.

18 Do you understand that?

19 Mr. Stamos. I do.

20 MAJORITY COUNSEL 1. So the court reporter can take down a clear record, we
21 will do our best to limit the number of people directing questions at you during any given
22 hour to just those people on the staff whose turn it is.

23 Please try and speak clearly so the court reporter can understand and so the folks
24 down at the end of the cable can hear you as well. It is important that we don't talk
25 over one another or interrupt each other if we can help that, and that goes for everybody

1 present at today's interview.

2 We want you to answer our questions in the most complete and truthful manner
3 as possible, so we'll take our time. If you have any questions or if you do not understand
4 one of our questions, please just let us know. Our questions will cover a wide range of
5 topics so if you need clarification at any point just ask.

6 If you honestly don't know the answer to a question or do not remember, it is best
7 not to guess. Please give us your best recollection, and it is okay to tell us if you learned
8 information from someone else. Just indicate how you came to know the information.
9 If there are things you don't know or can't remember, just say so and please inform us
10 who, to the best of your knowledge, might be able to articulate.

11 You should also understand that by law you are required to answer questions
12 from Congress truthfully.

13 Do you understand that?

14 Mr. Stamos. Yes.

15 MAJORITY COUNSEL 1. This also applies to questions posed by congressional
16 staff in an interview.

17 Do you understand this?

18 Mr. Stamos. Yes.

19 MAJORITY COUNSEL 1. Witnesses that knowingly provide false testimony could be
20 subject to criminal prosecution for making false statements under 18, U.S.C., Section
21 1001.

22 Do you understand this?

23 Mr. Stamos. Yes.

24 MAJORITY COUNSEL 1. Is there any reason you are unable to provide truthful
25 answers to today's questions?

1 Mr. Stamos. No.

2 MAJORITY COUNSEL 1. Finally, I would like to make note that the content of
3 what we discuss here today is confidential. We ask that you not speak about what we
4 discuss in this interview to any outside individuals to preserve the integrity of our
5 investigation.

6 For that same reason, the marked exhibits that we will use today will remain with
7 the court reporters, and we will collect any copies of the exhibits at the end of the
8 interview.

9 Okay. That's the end of my preamble.

10 Do my colleagues from the minority have anything?

11 MINORITY COUNSEL 1. We would just like to thank the witness for flying out
12 from California to join us today.

13 MAJORITY COUNSEL 1. Thank you.

14 Mr. Stamos I understand you have an opening statement. You may proceed.

15 Mr. Stamos. I do. Thank you.

16 Good morning. I'm glad to have this opportunity to describe the work of the
17 Stanford Internet Observatory and to address misperceptions about its participation in
18 the Election Integrity Partnership and the Virality Project.

19 The Stanford Internet Observatory studies misuses of the internet with the goals
20 of publishing research, suggesting technical and policy mitigations, and educating the
21 next generation of cyber specialists. I'm the founder and the director of the observatory
22 and a lecturer in the computer science department at Stanford.

23 To that end, I teach courses in cybersecurity and online safety at Stanford, along
24 with supervising our research efforts. Our research includes work on child safety, online
25 promotion of self-harm, generative AI, and influence campaigns by China, Iran, Russia,

1 Q You mentioned that the Global Engagement Center was one of the entities
2 that can submit reports, tickets as well?

3 A Yes. They could send -- they could send emails in to us for us to open and
4 to look into, yes.

5 Q Do you recall who at the GEC you interacted with?

6 A I don't- -- I mean, personally I had -- there was a meeting in which I believe
7 the director of the GEC was at here in D.C. I don't recall her name. I -- I didn't have
8 most of those conversations.

9 Q The meeting in D.C. that you just referenced, what was the purpose of that
10 meeting?

11 A I believe it was to tell them about what EIP was doing and telling them that
12 they could send into us reports of foreign influence that they saw, potential foreign
13 influence.

14 Q Do you know who first connected GEC and EIP together?

15 A I believe that we had already had preexisting relationships with GEC because
16 they had published in this area before the EIP.

17 Q In addition to CISA and GEC, do you recall any other Federal agencies that
18 played either informal, like, external stakeholder role or otherwise consulted EIP?

19 A So the only groups that could and did report from the Federal Government
20 report anything to us was the GEC, which is actually part of the government and then the
21 EI-ISAC external, you know. And you'd have to give it your own determination of how
22 much of the government that is. But those are the only two groups that did send
23 anything in to us. We did do briefings for several other agencies and we had one ticket
24 that we then sent out to the FBI.

25 Q Which other Federal agencies did EIP briefly?

1 A I did a briefing for General Nakasone then the director of NSA and Cyber
2 Command.

3 Q And did these briefings -- when did they occur in the process? Is it
4 pre-election?

5 A Pre-election, yes. Like in the late summer, early fall we did a briefing. He
6 had come to campus and had heard us talk about our foreign work. And he asked me to
7 brief his executive staff on our concerns and what kind of foreign influence who happen
8 during the election.

9 Q And the FBI mentioned -- received the ticket. Did the FBI also receive
10 briefings for the election?

11 A The FBI was part of that briefing, so I did it from the FBI office in -- in San
12 Francisco because I just can't Zoom in to the NSA.

13 Q Do you recall who set up the meeting between you and the NSA?

14 A Elvis Chan had set up the -- so the meeting was set up because Nakasone
15 had come to campus. Elvis was the facilitator who provided the space and participated,
16 listened to the briefing in San Francisco.

17 Q Yeah. Did you know Mr. Chan before this meeting had occurred?

18 A I did.

19 Q And how did you know special agent Chan?

20 A Yeah, he runs the group in the San Francisco office of the FBI that handles
21 high profile national security cyber attacks and so had I worked with him both at Yahoo.
22 At Yahoo we had been attacked by the -- by contractors working for the Russian FSB.

23 And then at Facebook we had a number of attempted attacks, as well as
24 manipulations of the platform to cause attacks by a variety of government agencies,
25 foreign government agencies. And so Elvis was the primary contact for all of that

1 because he ran the group that would investigate those kinds of foreign actions.

2 Q Do you recall anyone else from the FBI attending this meeting?

3 A There were some other people from his squad. I don't recall their names.

4 Q And so in addition to the NSA, FBI, do you recall any other entities that were
5 present at the meeting?

6 A The -- it was a video conference. In the room were only FBI agents. The
7 only people I knew of who were on the other link were NSA.

8 Q So you mentioned FBI, NSA, GEC and CISA. Were there any other
9 government agencies that received a briefing from EIP?

10 A Not to my knowledge.

11 Q Did you -- in addition to this briefing that the FBI helped facilitate between
12 EIP and NSA, did you have any other interactions with the FBI as a function of EIP's work?

13 A We did the preemptive briefing and we sent them one report related to
14 Arabian action in the election and I believe that was our only interaction with them.

15 Q When EIP was organized, were there new EIP email addresses created for
16 folks?

17 A No. We have a domain that has one working email address info@, which
18 was a mailing list that went to three or four different people.

19 Q Okay. Do you know who those three or four people are?

20 A It was me, probably Elena Cryst or deputy director of SIO, Kate Starbird and I
21 believe there's a comms person at UW, I forgot his name, who'd receive those emails.
22 Because often that would be media requests and he would be the one who handled
23 those.

24 Q So I think we started to touch upon this, but how would members of EIP
25 communicate with one another?

1

2 [4:42 p.m.]

3 BY MAJORITY COUNSEL 2:

4 Q Who was the EIP's primary point of contact at Reddit?

5 A I've forgotten her name. There was a woman in the policy team. We can
6 come back to you.

7 Q Do you recall with respect to Alphabet if there was different points of
8 contact for Google as opposed to YouTube or if it was the same point of contact?

9 A I believe it was the same. For these purposes, the central Google team was
10 the one who was coordinating on their election policies.

11 Q In 2020, who was EIP's primary former contact with Discord?

12 A I don't recall with Discord.

13 Q What about with respect to Wikimedia?

14 A Yes. There's a -- I don't remember what the name is of the person at
15 Wikimedia. I wasn't a part of those meetings.

16 Q Who would have been part of those meetings?

17 A Probably [REDACTED] or some of the students who were doing onboarding.

18 Q Who is EIP's primary point of contact with Pinterest?

19 A I don't recall.

20 Q Are there plans to -- you mentioned that EIP -- obviously, this is the 2020
21 iteration. In 2022, you said there were some differences. Are there any plans to have
22 some continuation of the partnership for the 2024 election?

23 A That's an interesting question. I'm going to have to have a discussion with
24 Stanford's leadership. Since this investigation has cost the university now approaching
25 seven figures legal fees, it's been pretty successful I think in discouraging us from making

1 it worthwhile for us to do a study in 2024.

2 MAJORITY COUNSEL 2. Do you recall which exhibit we're on?

3 [REDACTED]. 21 -- 22.

4 MAJORITY COUNSEL 2. 22. All right.

5 [Stamos Exhibit No. 22

6 Was marked for identification.]

7 BY MAJORITY COUNSEL 2:

8 Q Do you know who [REDACTED] is? I don't know if I'm pronouncing her
9 name right.

10 A Yeah. She was the woman I was thinking of, the head of policy for Reddit.

11 Q Great. And at her email at the top of the page, she says that

12 "We" -- assuming referring to Reddit -- "are unable to participate in Jiras, but we are
13 happy to receive info over email."

14 Do you recall that Reddit didn't respond in Jira directly?

15 A Right. They did not -- for whatever reason, did not want to have something
16 they had to log into. They wanted things to be put in the email and sent directly to
17 them.

18 Q Okay. And then there's an email below from you. You explain the
19 situation. There are a couple of links. And then below you say: "It would be great if
20 we could get somebody from Reddit on the Jira, just like Facebook, Google, Twitter,
21 TikTok, Instagram, CISA, EI-ISAC."

22 Were you referring to CISA, the government agency?

23 A I was probably making a mistake there talking about CISA because EI-ISAC
24 were the people who had access to the Jira.

25 Q But you list both EI-ISAC and CISA. Is that right?

No. 23-411

In the Supreme Court of the United States

VIVEK H. MURTHY, SURGEON GENERAL, ET AL.,
Petitioners,

v.

STATE OF MISSOURI, ET AL.,
Respondents.

*ON WRIT OF CERTIORARI TO THE UNITED STATES
COURT OF APPEALS FOR THE FIFTH CIRCUIT*

**BRIEF FOR REPRESENTATIVE JIM JORDAN
AND 44 OTHER MEMBERS OF CONGRESS AS
AMICI CURIAE IN SUPPORT
OF RESPONDENTS**

GENE P. HAMILTON
REED D. RUBINSTEIN
MICHAEL DING

America First Legal
Foundation
611 Pennsylvania Ave. SE
#231
Washington, DC 20003
(202) 964-3721
gene.hamilton@aflegal.org

CHRISTOPHER E. MILLS
Counsel of Record
Spero Law LLC
557 East Bay Street
#22251
Charleston, SC 29413
(843) 606-0640
cmills@spero.law

TABLE OF CONTENTS

	Page
Table of Contents.....	i
Table of Authorities.....	ii
Interest of <i>Amici Curiae</i>	1
Summary of the Argument	3
Argument.....	6
I. The United States has coerced speech about COVID.....	6
II. The United States has coerced speech about Biden Family influence peddling.	15
III. The United States has coerced speech about elections.....	23
A. Cybersecurity and Infrastructure Security Agency (CISA).....	23
B. The Election Integrity Partnership (EIP)..	27
IV. The United States is funding research and tools to enable censorship at scale.	34
Conclusion.....	36

TABLE OF AUTHORITIES

CASES

<i>Anderson v. Bessemer City</i> , 470 U.S. 564 (1985)	4
<i>Arizona Free Enter. Club’s Freedom Club PAC v. Bennett</i> , 564 U.S. 721 (2011)	4, 5
<i>Barr v. Am. Ass’n of Pol. Consultants, Inc.</i> , 140 S. Ct. 2335 (2020)	5
<i>Dennis v. United States</i> , 341 U.S. 494 (1951)	4
<i>Easley v. Cromartie</i> , 532 U.S. 234 (2001)	5
<i>Kennedy v. Warren</i> , 66 F.4th 1199 (9th Cir. 2023)	4
<i>McIntyre v. Ohio Elections Comm’n</i> , 514 U.S. 334 (1995)	23
<i>Norwood v. Harrison</i> , 413 U.S. 455 (1973)	34
<i>Snyder v. Phelps</i> , 562 U.S. 443 (2011)	3, 5
<i>Texas v. Johnson</i> , 491 U.S. 397 (1989)	3

CONSTITUTIONAL AND STATUTORY PROVISIONS

U.S. Const. amend. I	1, 3, 4, 5, 13, 15, 22, 23, 28
----------------------------	--------------------------------

6 U.S.C. § 652	23
----------------------	----

OTHER AUTHORITIES

Nandita Bose and Elizabeth Culliford, <i>Biden Says Facebook, Others ‘Killing People’ by Carrying COVID Misinformation</i> , Reuters (Jul. 16, 2021), https://tinyurl.com/zpt53rna	11
Center for Internet Sec., EI-ISAC, https://www.cisecurity.org/ei-isac (last visited Jan. 5, 2024)	26
Cybersecurity and Infrastructure Sec. Agency, Mis-, Dis-, and Malinformation Planning and Incident Response Guide for Election Officials 1 (2022), https://tinyurl.com/52pvpn5d	24
Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Commission MUR 7821, (Dec. 17, 2020), https://tinyurl.com/3mmzx2bk	18
Deposition of Brian Scully, 11:19–12:6, (available at https://tinyurl.com/2epb2mw9) (D. Ct. Doc. 209-1)	24, 25
Deposition of Elvis Chan at 248:5–250:21 (D. Ct. Doc. 204-1).....	18, 20, 21
Miranda Devine, <i>Media Helped Hide the Real Joe Biden by Censoring Hunter Stories</i> , New York Post (Nov. 28, 2021), https://tinyurl.com/mvp474ba	22
Election Integrity P’ship, <i>The Long Fuse: Misinformation and the 2020 Election 2</i> (2021), https://tinyurl.com/4frucxab	27, 28, 29, 33, 34

Bruce Golding, <i>Zuckerberg Says Facebook Censored the Post’s Hunter Biden Stories Because FBI Warned of Russian Misinfo ‘Dump,’</i> New York Post (Aug. 26, 2022), https://tinyurl.com/5n8xz6xd	17
Betsy Klein, <i>White House Reviewing Section 230 Amid Efforts to Push Social Media Giants to Crack Down on Misinformation,</i> CNN (Jul. 20, 2021), https://tinyurl.com/73hnfk3h	14
Letter from John B. Bellinger III to the Hon. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023) (on file with the H. Comm. on the Judiciary)	31
Letter from John B. Bellinger III to the Hon. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 7, 2023) (on file with the H. Comm. on the Judiciary)	31
Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 27, 2023) (on file with the H. Comm. on the Judiciary)	29
Letter from Rep. Jordan, Chairman, House Comm on the Jud., to the Hon. Christopher Wray, Director, FBI (July 20, 2023), https://tinyurl.com/3m7a6wsa	15, 16, 17, 18, 19, 20, 21, 22
Emma-Jo Morris & Gabrielle Fonrouge, <i>Smoking-gun Email Reveals how Hunter Biden Introduced Ukrainian Businessman to VP Dad,</i> New York Post (Oct. 14, 2020), https://tinyurl.com/v7maymv8	16

Steven Nelson, <i>The Post’s FB Traffic Tanked After WH Aide’s False Claim of ‘Churning Out Articles Every Day About People Dying’ From COVID Vax</i> , New York Post (Aug. 4, 2023), https://tinyurl.com/rrmtzkk	9
Office of Inspector Gen., Dep’t of Homeland Sec., OIG-22-58, DHS Needs a Unified Strategy to Counter Disinformation Campaigns 5 (Aug. 10, 2022), https://tinyurl.com/2p9h2p75	24
Oversight of the Department of Homeland Security: Hearing Before the H. Comm. on the Judiciary, 118th Cong. (July 26, 2023)	25
Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary, 118th Cong. (July 12, 2023)	22
Rep. Jim Jordan (@Jim_Jordan), Twitter (July 27, 2023, 12:03 PM), https://tinyurl.com/5nz8sn3b (“THE FACEBOOK FILES PART 1”)	7
Rep. Jim Jordan (@Jim_Jordan), Twitter (July 28, 2023, 12:03 PM), https://tinyurl.com/3z5npf92 (“THE FACEBOOK FILES PART 2”)	7
Rep. Jim Jordan (@Jim_Jordan), Twitter (Aug. 3, 2023, 11:00 AM), https://tinyurl.com/4kjvehbb (“THE FACEBOOK FILES PART 3”)	7
Rep. Jim Jordan (@Jim_Jordan), Twitter (Aug. 7, 2023, 10:11 AM), https://tinyurl.com/yebawzjr (“THE FACEBOOK FILES PART 4”)	7
Rep. Jim Jordan (@Jim_Jordan), Twitter (Sept. 5, 2023, 6:17 PM), http://tinyurl.com/4e7a65xx (“THE FACEBOOK FILES PART 5”)	7

Rep. Jim Jordan (@Jim_Jordan), Twitter (Nov. 30, 2023, 8:44 AM), <http://tinyurl.com/3ma78m8x> (“THE YOUTUBE FILES PART 1”)..... 7

Rep. Jim Jordan (@Jim_Jordan), Twitter (Nov. 30, 2023, 8:44 AM), <http://tinyurl.com/4hpkfz39> (“THE YOUTUBE FILES PART 1”) 10

Rep. Jim Jordan (@Jim_Jordan), Twitter (Dec. 1, 2023, 2:26 PM), <http://tinyurl.com/ms7amj7x> (“THE YOUTUBE FILES PART 2”) 7

Rep. Jim Jordan (@Jim_Jordan), Twitter (Feb. 5, 2024, 5:44 PM), <http://tinyurl.com/mwxmzb79> (“THE AMAZON FILES”)..... 7, 11

Sen. Ted Cruz (@tedcruz), Twitter (Oct. 27, 2022, 12:34 PM), <https://tinyurl.com/2s9dce95>..... 26

Staff of the H. Comm. on the Jud., 118th Cong., Interim Staff Report: The Weaponization of CISA (June 26, 2023), available at <https://bit.ly/45jYPke> (D. Ct. Doc. 291-2)..... 23, 24

Staff of the H. Comm. on the Jud., 118th Cong., Interim Staff Report: The Weaponization of “Disinformation” 20 (Nov. 6, 2023), available at <http://tinyurl.com/2n53pdy5> ... 25, 26, 27, 28, 29, 30, 32, 33, 34

Staff of H. Comm. on the Jud., Select Subcomm. on the Weaponization of the Fed. Gov’t, & Permanent Select Comm. on Intel., 118th Cong., The Hunter Biden Statement: How Senior Intelligence Community Officials and the Biden Campaign Worked to Mislead American Voters 1 (2023), <https://tinyurl.com/47v4fxb8>..... 16

Staff of H. Comm. on the Jud., Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary, 118th Cong., The Weaponization of The National Science Foundation: How NSF Is Funding The Development of Automated Tools to Censor Online Speech “At Scale” and Trying to Cover Up Its Actions (Comm. Print Feb. 2024), http://tinyurl.com/2532hdp5	34, 35, 36
Stanford Internet Observatory, the University of Washington’s Center for an Informed Public, the Atlantic Council’s Digital Forensics Research Lab, and Graphika.	28
Matt Taibbi (@mtaibbi), Twitter (Mar. 2, 2023, 12:00 PM), https://tinyurl.com/3pmhu8j6	30
Ryan Tracy, <i>Facebook Bowed to White House Pressure, Removed Covid Posts</i> , The Wall Street Journal (July 28, 2023), https://tinyurl.com/2bepvs5t	15
Transcribed Interview of Alex Stamos before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 23, 2023)	30, 31
Transcribed Interview of David Agranovich before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (May 16, 2023)	19
Transcribed Interview of Laura Dehmlow before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (July 17, 2023)	16, 19, 20, 21

Transcribed Interview of Nathaniel Gleicher before
the House Committee on the Judiciary and the
Select Subcommittee on the Weaponization of the
Federal Government (June 21, 2023)..... 19

U.S. Dep’t of State, About Us—Global Engagement
Center, <https://tinyurl.com/43dmawd9> (last visited
Jan. 5, 2024) 30

INTEREST OF *AMICI CURIAE*

Amici curiae are Representative Jim Jordan and 44 other Members of Congress. The full list of *amici* appears on the following page.*

Each Member of Congress has taken an oath to uphold the Constitution and laws of the United States, and they have an institutional interest in protecting First Amendment rights from encroachment by the executive branch, protecting the rule of law, and holding the executive branch accountable when it overreaches. This interest also includes ensuring that the courts police those constitutional boundaries.

Each Member signatory is concerned that the Biden Administration has violated the Constitution and abridged Americans' civil liberties. Congress—and the House Judiciary Committee and the Weaponization Subcommittee, in particular—has been investigating the executive branch's coercion and collusion with social media companies to censor speech. Evidence recently obtained by these investigations further corroborates the district court's findings and the opinions below. Thus, each Member signatory has a substantial interest in this case and offers a unique perspective by virtue of his or her role in Congress.

* Under Rule 37.6, no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

The following is the full list of *amici*:

United States Senate

Mike Braun	Ron Johnson
Ted Cruz	Roger Marshall, M.D.
Josh Hawley	Rand Paul

United States House of Representatives

Jim Jordan

Elise M. Stefanik	Ronny Jackson
Kelly Armstrong	Anna Paulina Luna
Jim Banks	Thomas Massie
Aaron Bean	Mary E. Miller
Andy Biggs	Max L. Miller
Dan Bishop	Alexander X. Mooney
Eric Burlison	Barry Moore
Kat Cammack	Troy E. Nehls
Jerry L. Carl	Ralph Norman
Ben Cline	Andy Ogles
Michael Cloud	Guy Reschenthaler
Andrew S. Clyde	Matthew M. Rosendale, Sr.
Jeff Duncan	Keith Self
Scott Fitzgerald	Gregory W. Steube
Russell Fry	Claudia Tenney
Matt Gaetz	William R. Timmons, IV
Lance Gooden	Michael Waltz
Harriet M. Hageman	Daniel Webster
Erin Houchin	
Darrell E. Issa	

SUMMARY OF THE ARGUMENT

Wielding threats of intervention, the executive branch of the federal government has engaged in a sustained effort to coerce private parties into censoring speech on matters of public concern. On issue after issue, the Biden Administration has distorted the free marketplace of ideas promised by the First Amendment, bringing the weight of federal authority to bear on any speech it dislikes—including memes and jokes. Of course, Big Tech companies often required little coercion to do the Administration’s bidding on some issues. Generally eager to please their ideological allies and overseers in the federal government, these companies and other private entities have repeatedly censored accurate speech on important public issues. When the censors were too slow to suppress speech that the partisans in the Administration disliked, the federal government prodded them back into action with continual and increasing pressure.

Official pressure to suppress speech violates the First Amendment. “[A] principal function of free speech under our system of government is to invite dispute. It may indeed best serve its high purpose when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger.” *Texas v. Johnson*, 491 U.S. 397, 408–09 (1989) (cleaned up). No doubt, the government may find some individuals’ speech “misguided, or even hurtful,” but “the point of all speech protection is to shield just those choices of content.” *Snyder v. Phelps*, 562 U.S. 443, 458 (2011) (cleaned up). “The First Amendment embodies our choice as a Nation that,

when it comes to such speech, the guiding principle is freedom—the unfettered interchange of ideas—not whatever the State may view as fair.” *Arizona Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721, 750 (2011) (cleaned up). The First Amendment is founded on “the hypothesis that speech can rebut speech, propaganda will answer propaganda, [and] free debate of ideas will result in the wisest governmental policies.” *Dennis v. United States*, 341 U.S. 494, 503 (1951). Thus, the First Amendment stands against any governmental effort to coerce or otherwise burden the free speech of private entities—even if that action falls short of outright suppression. Cf. *Kennedy v. Warren*, 66 F.4th 1199, 1213 (9th Cir. 2023) (Bennett, J., concurring) (“[W]e do not require a government official to list specific consequences in order to find a constitutional violation.”).

Censorship-by-proxy is an especially nefarious form of state action, given that it is designed to evade detection, oversight efforts, and public records requests. The district court found, as a matter of fact, that “the United States Government, through the White House and numerous federal agencies, pressured and encouraged social-media companies to suppress free speech.” J.A. 201. The Fifth Circuit agreed. These factual findings must be upheld unless clearly erroneous. “Where there are two permissible views of the evidence, the factfinder’s choice between them cannot be clearly erroneous.” *Anderson v. Bessemer City*, 470 U.S. 564, 574 (1985). And “[w]here an intermediate court reviews, and affirms, a trial court’s factual findings”—as here—“this Court will not lightly overturn the concurrent findings of the two

lower courts.” *Easley v. Cromartie*, 532 U.S. 234, 242 (2001).

The district court’s findings are easily “permissible”; they are clearly correct. Beyond the ample evidence cited by the courts below and the Plaintiffs, even more recent evidence obtained by the House Judiciary Committee and the Weaponization Subcommittee confirms the conclusions reached below. That evidence shows that the Biden Administration has relentlessly pressured private entities—sometimes in cooperation with other private entities—to censor speech that the Administration disliked. As detailed below, this official coercion has undermined the marketplace of ideas on issues of public importance ranging from COVID to federal elections to Biden family misdeeds. And the suppression “does not simply have an effect on speech, but is directed at certain content and is aimed at particular speakers”: conservative voices opposed to the current Administration. *Barr v. Am. Ass’n of Pol. Consultants, Inc.*, 140 S. Ct. 2335, 2347 (2020). “This sort of ‘beggar thy neighbor’ approach to free speech—restricting the speech of some elements of our society in order to enhance the relative voice of others—is wholly foreign to the First Amendment.” *Bennett*, 564 U.S. at 741 (cleaned up). Likewise foreign to the First Amendment are governmental efforts to coerce the speech of private Americans. “As a Nation we have chosen a different course—to protect even hurtful speech on public issues to ensure that we do not stifle public debate.” *Snyder*, 562 U.S. at 461.

Because the Biden Administration has repeatedly used government coercion to stifle public debate—and

the injunction below rightfully halts the Administration's unlawful conduct—the Court should affirm.

ARGUMENT

I. The United States has coerced speech about COVID.

As the district court found, the federal government “suppressed alternative views” about COVID-related matters, including the origination of the virus, the efficacy of vaccines and masks, and the adverse effects of lockdowns, effectively forcing social media companies to enforce the government’s view as “the truth.” J.A. 213. The district court listed over twenty examples of the government engaging in coercive acts directed toward social media companies to bring about censorship. J.A. 205–09. And the government’s pressure campaign worked. Facebook agreed to moderate certain COVID-related speech in response to pressure from the Biden Administration, telling the government that Facebook would rely on their “authorities” to determine what content to censor. J.A. 98. Echoing the White House’s own description, the district court described the government’s direction of the companies’ content choices as a “partner[ship].” J.A. 210. The Fifth Circuit agreed, finding that the social media companies “not only continued to take down content the officials flagged, and provided requested data to the White House, but they also changed their moderation policies expressly in accordance with the officials’ wishes.” J.A. 7; see J.A. 49–68 (finding coercion and significant pressure by the White House, FBI, CDC, and CISA based on a detailed examination of the factual record).

Recent evidence corroborates these findings. The House Judiciary Committee subpoenaed internal documents from Meta, the parent entity of Facebook and Instagram; Alphabet, the parent entity of Google and YouTube; and Amazon. The documents obtained confirm that the companies censored information and altered their content moderation policies because of pressure from the Biden Administration to rid their platforms of purported “misinformation.”¹

This pressure was direct and coercive. For example, the Administration tried to suppress discussion of COVID’s origins: when a Facebook executive asked in July 2021 why the company censored the COVID lab leak theory, an executive in charge of content policy development said, “[b]ecause we were under pressure from the [A]dministration” to

¹ Rep. Jim Jordan (@Jim_Jordan), Twitter (July 27, 2023, 12:03 PM), <https://tinyurl.com/5nz8sn3b> (“THE FACEBOOK FILES PART 1”); Rep. Jim Jordan (@Jim_Jordan), Twitter (July 28, 2023, 12:03 PM), <https://tinyurl.com/3z5npf92> (“THE FACEBOOK FILES PART 2”); Rep. Jim Jordan (@Jim_Jordan), Twitter (Aug. 3, 2023, 11:00 AM), <https://tinyurl.com/4kjvehbb> (“THE FACEBOOK FILES PART 3”); Rep. Jim Jordan (@Jim_Jordan), Twitter (Aug. 7, 2023, 10:11 AM), <https://tinyurl.com/yebawzjr> (“THE FACEBOOK FILES PART 4”); Rep. Jim Jordan (@Jim_Jordan), Twitter (Sept. 5, 2023, 6:17 PM), <http://tinyurl.com/4e7a65xx> (“THE FACEBOOK FILES PART 5”); Rep. Jim Jordan (@Jim_Jordan), Twitter (Nov. 30, 2023, 8:44 AM), <http://tinyurl.com/3ma78m8x> (“THE YOUTUBE FILES PART 1”); Rep. Jim Jordan (@Jim_Jordan), Twitter (Dec. 1, 2023, 2:26 PM), <http://tinyurl.com/ms7amj7x> (“THE YOUTUBE FILES PART 2”); Rep. Jim Jordan (@Jim_Jordan), Twitter (Feb. 5, 2024, 5:44 PM), <http://tinyurl.com/mwxmzb79> (“THE AMAZON FILES”).

do so.² The same Facebook executive confessed that the company “shouldn’t have done it.”³

Yet Facebook continued to do the Administration’s bidding, repeatedly removing and reducing content the federal government disfavored. The Biden White House’s successful monthslong campaign to censor views expressing or supporting vaccine hesitancy is the clearest example of how the government coerced social media companies to change the scope and enforcement of their content moderation policies.

In a draft of an internal email, a Facebook employee explained to CEO Mark Zuckerberg and COO Sheryl Sandberg: “We are facing continued pressure from external stakeholders, including the [Biden] White House and the press, to *remove* more COVID-19 vaccine discouraging content.”⁴

Mark, Sheryl:

We are seeking your guidance on whether to take more aggressive action against certain vaccine discouraging content.

We are facing continued pressure from external stakeholders, including the White House and the press, to *remove* more COVID-19 vaccine discouraging content. For example, we recently shared with the White House a list of the top 100 vaccine-related posts on FB in the U.S. for the week of 4/5-4/11. While authoritative information dominated the list, the White House was concerned that the #3 post was a vaccine discouraging humorous meme, and they called on us to delete the meme.

Another Facebook executive notified his team that a senior advisor to President Biden was “outraged”

² Ex. 1 (e-mail from Nick Clegg to Facebook employees (July 14, 2021, 11:46 AM)). All Exhibit cites are to the Appendix attached to *amici*’s brief in the Fifth Circuit. See CA5 Doc. 224.

³ *Ibid.*

⁴ Ex. 2 (e-mail from Facebook employee to Facebook employees (Apr. 27, 2021, 11:58 AM)) (emphasis in original).

“that [Facebook] did not remove” a meme that bothered the Administration.⁵ Likewise, to appease the Administration, Facebook demoted a video posted by journalist Tucker Carlson that was critical of the COVID vaccine, even though Facebook admitted that the video did not violate company policy.⁶

Tucker Carlson was not the only prominent media critic of the Biden Administration to be targeted by the Administration’s censorship efforts. According to Facebook’s internal notes of meetings with White House senior advisors, White House officials questioned whether Facebook’s enforcement of its content moderation policies against the *New York Post* was aggressive enough.⁷ Similarly, in April 2021, a White House official questioned whether Facebook could “change [its] algorithm so that people were more likely to see [the *New York Times*], [the *Wall Street Journal*], any authoritative news source over [the] Daily Wire, Tomi Lahren, polarizing people.”⁸ The White House’s requests were rooted in the paternalistic notion that Americans cannot decide for

⁵ Ex. 3 (e-mail from Nick Clegg to Facebook employees (Apr. 19, 2021, 9:40 AM)).

⁶ *Ibid.*

⁷ Ex. 4 (Facebook employee’s notes of a call between White House personnel and Facebook employees on March 26, 2021). The *New York Post*’s traffic on Facebook subsequently plummeted by over 50 percent before rebounding to “normal levels” by fall 2021. Steven Nelson, *The Post’s FB Traffic Tanked After WH Aide’s False Claim of ‘Churning Out Articles Every Day About People Dying’ From COVID Vax*, *New York Post* (Aug. 4, 2023), <https://tinyurl.com/rrmtzkk>.

⁸ Ex. 5 (Facebook employee’s notes of a call between White House personnel and Facebook employees on April 14, 2021).

themselves what information should or should not be believed. As a White House staffer condescendingly remarked in a meeting with Facebook in April 2021, “[i]f someone in rural Arkansas sees something on [Facebook], it’s the truth.”⁹ In a June 2021 meeting, the White House pushed Facebook to “reduce the spread of bad information,” *i.e.*, “bad” information according to the White House.¹⁰

The White House exerted similar pressure on YouTube. The government’s demands for meetings and information on YouTube’s policies and removals led to warnings within YouTube that the Biden “White House is very interested in our work on borderline content” and should be briefed again “to prevent anything from potentially spiraling out of control.”¹¹ YouTube considered this approach necessary because it was “seek[ing] to work closely with [the Biden] administration on multiple policy fronts.”¹²

The White House’s pressure extended to Amazon, the world’s largest online bookstore. Senior White House officials ran key searchers for topics such as “vaccine” and emailed Amazon employees directly when displeased with how the search results

⁹ Ex. 6 (Facebook employee’s notes of a call between White House personnel and Facebook employees on April 5, 2021).

¹⁰ Ex. 7 (Facebook employee’s notes of a call between White House personnel and Facebook employees on June 15, 2021).

¹¹ Rep. Jim Jordan (@Jim_Jordan), Twitter (Nov. 30, 2023, 8:44 AM), <http://tinyurl.com/4hpkfz39> (“THE YOUTUBE FILES PART 1”).

¹² *Ibid.*

appeared.¹³ One internal Amazon email regarding a “Pre-Brief for Meeting w/ the White House” started with this “Top Talking Point[]”: “Is the Admin asking us to remove books, or are they more concerned about search results/order (or both)?”¹⁴ Other internal emails reveal that Amazon was “feeling pressure from the White House” on this issue.¹⁵ The Committee’s investigation remains ongoing, but there is evidence that Amazon adopted new policies, including “enabl[ing] Do Not Promote for anti-vax books,” because of pressure from the White House.¹⁶

Not only did the Biden Administration privately coerce Facebook and other companies into censoring information, it also engaged in a public relations campaign against the companies to pressure them into submission. In July 2021, President Biden publicly denounced these companies, particularly Facebook, claiming they were “killing people” by not censoring alleged “misinformation” to the government’s satisfaction.¹⁷ Facebook employees internally lamented that the Biden White House’s “definition of ‘misinfo’ is completely unclear.”¹⁸ Following the White House’s pressure, Facebook leadership—internally

¹³ Rep. Jim Jordan (@Jim_Jordan), Twitter (Feb. 5, 2024, 5:44 PM), <http://tinyurl.com/mwxmzb79> (“THE AMAZON FILES”).

¹⁴ *Ibid.*

¹⁵ *Ibid.*

¹⁶ *Ibid.*

¹⁷ Nandita Bose and Elizabeth Culliford, *Biden Says Facebook, Others ‘Killing People’ by Carrying COVID Misinformation*, Reuters (Jul. 16, 2021), <https://tinyurl.com/zpt53rna>.

¹⁸ Ex. 8 (e-mail from Facebook employee to Facebook employees (July 16, 2021, 8:14 PM)).

admitting that the move was “stemming from the continued criticism of our approach from the [Biden] administration”—directed employees to “brainstorm some additional policy levers we can pull to be more aggressive against . . . misinformation.”¹⁹ Ultimately, the company adopted four new, more aggressive policy options one month later.²⁰

Likewise, before meeting with the Biden Administration’s Office of the Surgeon General (OSG), a Facebook employee wrote that Sheryl Sandberg “is keen that we continue to explore some moves that we can make to show that we are trying to be responsive to the [White House].”²¹ The email continued: “My sense is that our current course—in effect explaining ourselves more fully, but not shifting on where we draw the lines . . . is a recipe for protracted and increasing acrimony with the [White House].”²² Internal documents obtained by the House Judiciary Committee and the Weaponization Subcommittee show that the Biden Administration pressured Facebook to censor information about the COVID vaccine’s side effects, even if the information was true.²³ In a July 2021 meeting with OSG, a Facebook

¹⁹ Ex. 9 (e-mail from Facebook employee to Facebook employees (Aug. 6, 2021, 7:13 PM)).

²⁰ Ex. 10 (e-mail from Nick Clegg to Facebook employees (Aug. 19, 2021, 5:25 PM)).

²¹ Ex. 11 (e-mail from Facebook employee to Facebook employees (July 22, 2021, 12:17 PM)).

²² *Ibid.*

²³ Ex. 12 (e-mail from Sheryl Sandberg to Nick Clegg (Jul. 21, 2021, 4:49 PM)) (“The Surgeon General wants us to remove true information about side effects.”).

employee confirmed that Facebook was demoting content that questioned whether vaccine mandates constituted “government overreach,” despite acknowledging “[t]hat’s not false information.”²⁴

Worse still, when Facebook questioned censoring information, the Biden Administration showed disdain and contempt for the First Amendment. For example, when the Administration flagged satirical content about the COVID vaccine, a Facebook executive first warned that removing satirical content would “represent a significant incursion into traditional boundaries of free expression in the US.”²⁵ But the Biden Administration was unpersuaded, insisting that the content “inhibits confidence” in the COVID vaccine.²⁶

A Facebook vice president warned internally that the company was at “a crossroads” with the Administration over its censorship efforts.²⁷ Facebook executives grasped the connection between the company’s business prospects and remaining in the Administration’s good graces. One executive, recommending that the company consider bending to the Administration’s censorship requests, cautioned COO Sheryl Sandberg that Facebook had “bigger fish

²⁴ Ex. 13 (Facebook employee’s notes of a call between OSG personnel and Facebook employees on July 16, 2021).

²⁵ Ex. 3 (e-mail from Nick Clegg to Facebook employees).

²⁶ *Ibid.*

²⁷ *Ibid.*

we have to fry with the Administration — data flows etc.”²⁸

Another looming issue was—and still is—reform of Section 230 of the Communications Decency Act. As the district court explained, Section 230 is “valuable” to Big Tech because of its legal protections. J.A. 210. And the district court found that the federal government “threat[ened]” Big Tech with the repeal of Section 230 to induce compliance with its censorship campaign. *Ibid.* Mark Zuckerberg has referred to the possibility of antitrust enforcement as an “existential threat” to his empire. J.A. 95. Four days after President Biden publicly accused Facebook of “killing people,” the White House Communications Director publicly said the Administration was “reviewing” Section 230 reform as an option because the social media companies “should be held accountable.”²⁹ Internal documents show that Facebook executives feared that the Biden Administration would retaliate against the company for not censoring enough: one executive commented that the dispute over content was not “a great place for us to be,” and he would be “grateful for any further creative thinking on how we can be responsive to their [content] concerns.”³⁰ In response to mounting pressure, Facebook capitulated: “By August 2021, Facebook executives were emailing

²⁸ Ex. 11 (e-mail from Facebook employee to Facebook employees).

²⁹ Betsy Klein, *White House Reviewing Section 230 Amid Efforts to Push Social Media Giants to Crack Down on Misinformation*, CNN (Jul. 20, 2021), <https://tinyurl.com/73hnfk3h>.

³⁰ Ex. 11 (e-mail from Facebook employee to Facebook employees).

each other about new planned changes to their Covid content policies,” including increased punishments for violators.³¹

In short, the Biden Administration used its power to commandeer the apparatuses of social media companies to affect their COVID-related content policies. And out of self-interest, the companies complied and censored content beyond what they otherwise would have. This government coercion violates the First Amendment.

II. The United States has coerced speech about Biden Family influence peddling.

The federal government, specifically the FBI’s Foreign Influence Task Force (FITF), also used its power and influence to deceive and coerce social media companies into suppressing factual information during the 2020 election about the Biden family that the FBI knew to be true.³² The district court rightly labeled “[t]he FBI’s failure to alert social-media companies that the Hunter Biden laptop story was real, and not mere Russian disinformation,” as “particularly troubling.” J.A. 218. The laptop contained documents and emails with incriminating details about foreign business dealings that also

³¹ Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, The Wall Street Journal (July 28, 2023), <https://tinyurl.com/2bepvs5t>; see also Ex. 10 (E-mail from Nick Clegg to Facebook employees).

³² Letter from Rep. Jordan, Chairman, House Comm on the Jud., to the Hon. Christopher Wray, Director, FBI, at 1 (July 20, 2023), <https://tinyurl.com/3m7a6wsa>.

implicated Hunter Biden’s father—then-presidential candidate, Joe Biden.³³

In a transcribed interview before the House Judiciary Committee and Weaponization Subcommittee, the current Section Chief of FITF, Laura Dehmlow, testified that (1) FBI agents who knew the laptop was real were some of the same FBI agents who repeatedly warned social media companies about a potential “hack-and-leak” likely to occur in October 2020; and (2) despite direct requests from Twitter and Facebook for information on the day the *New York Post* story was published, the FBI decided to deliberately withhold critical information from the social media companies.³⁴

Although the FBI had the authenticated laptop in its possession since December 2019, it did not publicly acknowledge that it was real until after the November 3, 2020, election.³⁵ Rather than acknowledge the truth, the FBI actively influenced and deceived the

³³ Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun Email Reveals how Hunter Biden Introduced Ukrainian Businessman to VP Dad*, New York Post (Oct. 14, 2020), <https://tinyurl.com/v7maymv8>; Staff of H. Comm. on the Jud., Select Subcomm. on the Weaponization of the Fed. Gov’t, & Permanent Select Comm. on Intel., 118th Cong., *The Hunter Biden Statement: How Senior Intelligence Community Officials and the Biden Campaign Worked to Mislead American Voters* 1, 6 (2023), <https://tinyurl.com/47v4fxb8>.

³⁴ Ex. 14 (excerpts of Transcribed Interview of Laura Dehmlow before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (July 17, 2023)), at 29–37, 173–174.

³⁵ Jordan, *supra* note 32, at 5.

social media companies to censor the story when it inevitably came out.³⁶ In a well-executed, monthslong plan, the FBI primed the narrative, telling social media companies to “look for a ‘hack and dump’ operation by the Russians prior to the 2020 election.”³⁷ Then, once the laptop’s contents were exposed, the FBI refused to answer questions and let the narrative it had constructed do its work of distracting from and minimizing the truth. Mark Zuckerberg’s justification for censoring the story illustrates the effectiveness of this plan: “the FBI basically came to us” and said, “you should be on high alert.”³⁸ Facebook censored the story because when “[the FBI] come[s] to us and tell[s] us that we need to be on guard about something, then I want to take that seriously,” and the story “basically fit the pattern” the FBI warned about.³⁹ This federal coercion led to the censorship of accurate information.

In “the nine months leading up to the 2020 election, the FBI met over 30 times with social media platforms—all while in possession of Hunter Biden’s laptop.”⁴⁰ The FBI had “at least five meetings with Facebook, Google, Microsoft, [and] Yahoo!, in addition to multiple meetings with Twitter and Reddit.”⁴¹ Yoel

³⁶ *Id.* at 1.

³⁷ *Id.* at 4.

³⁸ Bruce Golding, *Zuckerberg Says Facebook Censored the Post’s Hunter Biden Stories Because FBI Warned of Russian Misinfo ‘Dump,’* New York Post (Aug. 26, 2022), <https://tinyurl.com/5n8xz6xd>.

³⁹ *Ibid.*

⁴⁰ Jordan, *supra* note 32, at 1.

⁴¹ *Ibid.*

Roth, former Head of Site Integrity at Twitter, confirmed in a sworn declaration that he had regular meetings in 2020 with different federal agencies, including the FBI, in which they “communicated that they expected ‘hack-and-leak operations’” against those associated with political campaigns “shortly before the 2020 presidential election, likely in October.”⁴² “These expectations of hack-and-leak operations were discussed throughout 2020.”⁴³ He was also told “that material obtained through those hacking attacks would likely be disseminated over social media platforms, including Twitter” and even that there were rumors the materials could involve Hunter Biden.⁴⁴

The companies also participated together in regular “USG-Industry” meetings, including four in October 2020, with representatives from federal agencies, including the FBI.⁴⁵ During these meetings, the FBI asked social media companies what their “hack and leak” policies were, how the companies would handle a potential “hack and leak,” and whether the companies would remove hacked materials from their platforms.⁴⁶ In response, some companies without a specific “hack and leak” policy,

⁴² Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Commission MUR 7821, (Dec. 17, 2020), <https://tinyurl.com/3mmzx2bk> [hereinafter Roth Decl.].

⁴³ *Ibid.*

⁴⁴ *Ibid.*

⁴⁵ Jordan, *supra* note 32, at 1.

⁴⁶ Deposition of Elvis Chan at 248:5–250:21 (D. Ct. Doc. 204-1) [hereinafter Chan Dep.]; see also Roth Decl., *supra* note 42, ¶ 11.

such as Facebook, developed and adopted a new policy during summer 2020.⁴⁷

Dehmlow confirmed that “the FBI could—and did—share information with companies regarding foreign malign influence operations, like hack-and-leak operations, including those conducted by Russia-aligned actors.”⁴⁸ For example, the agenda for the October 7, 2020 “USG-Industry” meeting—one week before the October 14 *New York Post* story—lists “Hack/Leak Concerns” as a topic.⁴⁹

According to Dehmlow, on the day the article was published, FBI met with Twitter, and a company representative asked if the laptop was real.⁵⁰ Dehmlow testified that, in response, “one of the FBI folks who was on the call” confirmed that the laptop was real before “another participant jumped in and said, ‘no further comment.’”⁵¹ After the meeting, FBI personnel “deliberated internally” and determined that—even though they knew the laptop was not Russian disinformation—in all further

⁴⁷ See Ex. 15 (excerpts of Transcribed Interview of David Agranovich before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (May 16, 2023)); Ex. 16 (excerpts of Transcribed Interview of Nathaniel Gleicher before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 21, 2023)).

⁴⁸ Jordan, *supra* note 32, at 2; Ex. 14 (Laura Dehmlow Transcribed Interview), at 173–74.

⁴⁹ Ex. 17 (e-mail from Facebook employee to Matthew Masterson and Brian Scully (Sept. 29, 2020, 11:41 AM)).

⁵⁰ Ex. 14 (Laura Dehmlow Transcribed Interview), at 29.

⁵¹ *Ibid.*

communications with social media companies the FBI would reply with “no comment.”⁵²

According to Dehmlow, later that same day, the FBI met with Facebook. This time the FBI had its story straight. When Facebook asked whether the laptop was real, Dehmlow, on behalf of the FBI, said, “no comment.”⁵³ The FBI has thus far refused to reveal to Congress the identities of the FBI official who told Twitter that the laptop was real, the FBI lawyer who instructed “no further comment” during the call with Twitter, or the FBI official who determined that the agency would respond only “no comment” when asked about Hunter Biden laptop’s authenticity going forward.⁵⁴

Facebook followed up again the next day, October 15.⁵⁵ According to an internal Facebook document obtained by the House Judiciary Committee and the Weaponization Subcommittee, a Facebook employee (and former FBI official) “spoke with SSA Elvis Chan (FBI San Francisco) on 15 October 2020, as a follow up to the call with the Foreign Influence Task Force on 14 October.”⁵⁶ Facebook again asked if the FBI had any new information, to which “Chan advised that he was up to speed on the current state of the matter

⁵² *Id.* at 33.

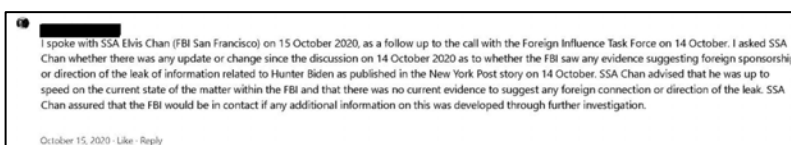
⁵³ *Id.* at 33; see also Chan Dep., *supra* note 46, at 215.

⁵⁴ See Ex. 14 (Laura Dehmlow Transcribed Interview), at 29–31; Jordan, *supra* note 32, at 5–6 (requesting a response by August 3, 2023).

⁵⁵ Ex. 18 (entry on internal Facebook case file by Facebook employee (Oct. 15, 2020)).

⁵⁶ *Ibid.*

within the FBI and that there was no current evidence to suggest any foreign connection or direction of the leak.”⁵⁷ But of course, the FBI knew not just of the *absence* of evidence suggesting any foreign connection; the FBI knew the laptop was real.⁵⁸



This internal Facebook document directly conflicts with the deposition testimony FBI Special Agent Elvis Chan provided in this case. Chan testified that he was “confident” that he “was not a party to any meeting with social media companies where Hunter Biden was discussed outside of the [October 14 FITF-Facebook meeting where Laura Dehmlow responded ‘no comment’].”⁵⁹ Later, when asked if, other than the October 14 FITF-Facebook meeting, he was “aware of any communications between anyone at Facebook and anyone at the FBI related to the Hunter Biden laptop story,” Chan responded, “No.”⁶⁰

⁵⁷ *Id.* Chan testified in his deposition that, unlike Dehmlow, FITF Section Chief Bradley Benavides, the Russia Unit Chief of FITF, and other FITF personnel, he did not know prior to October 14 that the FBI had the laptop. Cf. Chan Dep., *supra* note 46, at 230:7–19; Ex. 14 (Laura Dehmlow Transcribed Interview), at 37.

⁵⁸ Jordan, *supra* note 32; Ex. 14 (Laura Dehmlow Transcribed Interview), at 37.

⁵⁹ Cf. Chan Dep., *supra* note 46, at 215:22–216:16; Ex. 18 (entry on internal Facebook case file by Facebook employee (Oct. 15, 2020)).

⁶⁰ Chan Dep., *supra* note 46, at 233:22–234:3.

As a result of the FBI's withholding critical information on the day of (and in the days after) the *New York Post* article's publication, the social media companies began to do precisely what the FBI intended: suppress truthful First Amendment-protected speech less than three weeks before the presidential election.⁶¹ The story implicating one of the two major party candidates was blocked by Twitter and deamplified by Facebook, "significantly reducing its circulation and prevalence in users' newsfeeds,"⁶² all because the FBI—an organization that the companies felt compelled to follow—had led them to believe the laptop story was Russian disinformation.⁶³ The story was not Russian disinformation, and FBI personnel meeting with Twitter and Facebook knew *at the time* that it was not Russian disinformation.⁶⁴ The government's coercive manipulation of the marketplace of ideas no doubt affected the 2020 election.⁶⁵ The district court's

⁶¹ Jordan, *supra* note 32.

⁶² *Ibid.*

⁶³ FBI Director Wray testified that "the FBI is not in the business of moderating content or causing any social media company to suppress or censor" speech. Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary, 118th Cong. (July 12, 2023). On July 18, Chairman Jordan and Representative Mike Johnson, Chairman of the Subcommittee on the Constitution and Limited Government, wrote a letter to Director Wray providing him the opportunity to amend his testimony. Director Wray has not responded.

⁶⁴ Jordan, *supra* note 32.

⁶⁵ See Miranda Devine, *Media Helped Hide the Real Joe Biden by Censoring Hunter Stories*, *New York Post* (Nov. 28, 2021), <https://tinyurl.com/mvp474ba>.

findings that the federal government unlawfully coerced private speech are amply supported by the evidence.

III. The United States has coerced speech about elections.

The United States also flouted the First Amendment by coercing platforms into suppressing election-related speech. This coercion is especially troubling because speech pertaining to elections “occupies the core of the protection afforded by the First Amendment.” *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 346 (1995). Yet the federal government has repeatedly coerced social media companies to censor election-related speech. It has done so directly, through DHS’s Cybersecurity and Infrastructure Security Agency (CISA), and indirectly, through the private-sector Election Integrity Partnership (EIP).⁶⁶

A. Cybersecurity and Infrastructure Security Agency (CISA)

Congress established CISA in 2018 to “lead cybersecurity and critical infrastructure security programs, operations, and associated policy.”⁶⁷ CISA’s “Countering Foreign Influence Task Force” (CFITF)

⁶⁶ Staff of the H. Comm. on the Jud., 118th Cong., Interim Staff Report: The Weaponization of CISA (June 26, 2023), available at <https://bit.ly/45jYPke> (D. Ct. Doc. 291-2) [hereinafter Interim CISA Report].

⁶⁷ 6 U.S.C. § 652.

focused “on election infrastructure disinformation.”⁶⁸ But in an effort to expand its focus on foreign misinformation to domestic misinformation, “CISA transitioned its [CFITF] to promote more flexibility to focus on general MDM,” or so-called “Mis-, Dis-, and Malinformation.”⁶⁹

CISA’s focus on so-called “malinformation” is particularly alarming. According to CISA, “[m]alinformation is based on fact, but used out of context to mislead, harm, or manipulate.”⁷⁰ Put more plainly, “malinformation is *factual* information that is objectionable not because it is false or untruthful, but because it is provided without adequate ‘context’—context as determined by the government.”⁷¹

In his deposition, Brian Scully, the first head of the CFITF and later the head of the MDM team at CISA,⁷² said that CISA engaged in “switchboarding,” a practice in which CISA would flag alleged disinformation to social media platforms.⁷³ According to Scully, “switchboarding” involves CISA officials first receiving alleged “misinformation” reports from election officials and then forwarding those reports to

⁶⁸ Office of Inspector Gen., Dep’t of Homeland Sec., OIG-22-58, DHS Needs a Unified Strategy to Counter Disinformation Campaigns 5 (Aug. 10, 2022), <https://tinyurl.com/2p9h2p75>.

⁶⁹ *Id.* at 7.

⁷⁰ Cybersecurity and Infrastructure Sec. Agency, Mis-, Dis-, and Malinformation Planning and Incident Response Guide for Election Officials 1 (2022), <https://tinyurl.com/52pvpn5d>.

⁷¹ Interim CISA Report, *supra* note 66, at 10.

⁷² Deposition of Brian Scully, 11:19–12:6, (available at <https://tinyurl.com/2epb2mw9>) (D. Ct. Doc. 209-1).

⁷³ *Id.* at 23:16–24:2.

social media companies so that they could take enforcement measures against the reported content.⁷⁴ Scully admitted that CISA was aware that its outreach to social media companies about alleged misinformation would trigger content moderation.⁷⁵

Petitioners highlight that CISA stated in its communications with platforms that no “favorable or unfavorable” action would be taken against them. Br. 6. But CISA’s disclaimer pointedly did *not* make a similar promise on behalf of other government agencies (including the FBI) with whom CISA shared ticket information.⁷⁶ In other words, the disclaimer “emphasized that CISA would involve law enforcement agencies and that CISA would not (or could not) commit that law enforcement agencies would not take an unfavorable action based on how the social media platforms decided to respond to the misinformation report.”⁷⁷ This omission was significant. As the former Chief Security Officer of Facebook explained, “I think all executives of all

⁷⁴ *Id.* at 17:1–18:1.

⁷⁵ *Id.* at 17:15–18:1. In response to a question from Representative Dan Bishop, DHS Secretary Mayorkas testified that he believed that “it is true” that “CISA does not flag anything to social media organizations at all,” but that he would “verify that.” Oversight of the Department of Homeland Security: Hearing Before the H. Comm. on the Judiciary, 118th Cong. (July 26, 2023). Secretary Mayorkas has failed to provide the Judiciary Committee with any information to verify his testimony.

⁷⁶ Staff of the H. Comm. on the Jud., 118th Cong., Interim Staff Report: The Weaponization of “Disinformation” 20 (Nov. 6, 2023), available at <http://tinyurl.com/2n53pdy5> [hereinafter Interim EIP Report].

⁷⁷ *Id.* at 17.

public companies understand that there's lots of parts of the government that can punish you for activity that you thought was appropriate."⁷⁸

CISA also funded and utilized third parties, such as the Center for Internet Security (CIS), to achieve these aims. CIS is the nonprofit entity responsible for operating the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).⁷⁹ The "EI-ISAC is federally funded by CISA and a division of the Center for Internet Security."⁸⁰ The EI-ISAC allows election officials around the country to send reports of alleged "misinformation" to CIS, which CIS then forwards to the relevant social media platforms.⁸¹

For example, a state government official working for Pennsylvania's Secretary of State, a Democrat, reported to the EI-ISAC posts on Twitter and Facebook from Senator Ted Cruz's accounts.⁸² In the offending post, Senator Cruz, a Republican, asked: "Why is it only Democrat blue cities that take 'days' to count their votes? The rest of the country manages to get it done on election night."⁸³ Emblematic of this

⁷⁸ *Id.* at 20.

⁷⁹ Center for Internet Sec., EI-ISAC, <https://www.cisecurity.org/ei-isac> (last visited Jan. 5, 2024).

⁸⁰ *Ibid.*

⁸¹ *Ibid.*

⁸² Ex. 19 (e-mail from misinformation@cisecurity.org to Facebook employees (Oct. 27, 2022, 5:06 PM)).

⁸³ Sen. Ted Cruz (@tedcruz), Twitter (Oct. 27, 2022, 12:34 PM), <https://tinyurl.com/2s9dce95>.

“switchboarding,” the federally funded EI-ISAC forwarded the report to Facebook.⁸⁴

B. The Election Integrity Partnership (EIP)

The United States, primarily CISA, also coerced social media companies into censoring speech about the 2020 election through the private-sector Election Integrity Partnership (EIP), led by Stanford University. Formed in the summer of 2020, EIP was a coalition of research entities created “in consultation with CISA and other stakeholders,”⁸⁵ which “united government, academia, civil society, and industry, analyzing across platforms, to address misinformation in real time.”⁸⁶ “[F]rom the beginning,” “Stanford and CISA envisioned the partnership connecting federal agencies with social media platforms,” and CISA officials were intimately involved.⁸⁷

As one senior EIP figure explained, EIP was “set up at the request of DHS/CISA.”⁸⁸ Because the four entities comprising EIP were not government

⁸⁴ Ex. 19 (e-mail from misinformation@cisecurity.org to Facebook employees).

⁸⁵ Election Integrity P’ship, *The Long Fuse: Misinformation and the 2020 Election 2* (2021), <https://tinyurl.com/4frucxab> [hereinafter EIP].

⁸⁶ *Id.* at 241.

⁸⁷ Interim EIP Report, *supra* note 76, at 36; see, e.g., Ex. 20 (e-mail from Kate Starbird to Alex Stamos (July 8, 2020, 10:26 AM)).

⁸⁸ Interim EIP Report, *supra* note 76, at 39 (ellipsis and emphasis omitted).

entities,⁸⁹ the United States sought to use EIP to do things that the government could not do without violating the First Amendment—namely, directly monitoring and censoring speech. By its own account, EIP filled the “gap” in the government’s ability to police so-called “misinformation” and “disinformation” about elections on social media because “no government agency in the United States has the explicit mandate to monitor and correct election mis- and disinformation”⁹⁰—and because of “[u]nclear legal authorities including *very real 1st amendment questions*.”⁹¹

EIP used the Jira Service Desk, an internal ticketing software to allow approved entities (government agencies, EI-ISAC, and others) to submit “misinformation” reports, in the form of a “Jira ticket.”⁹² From there, EIP personnel analyzed the submission and could comment on the ticket, before a manager would assess whether to forward the ticket to the relevant social media platform(s).⁹³ EIP’s final report illustrates this workflow:⁹⁴

⁸⁹ Stanford Internet Observatory, the University of Washington’s Center for an Informed Public, the Atlantic Council’s Digital Forensics Research Lab, and Graphika.

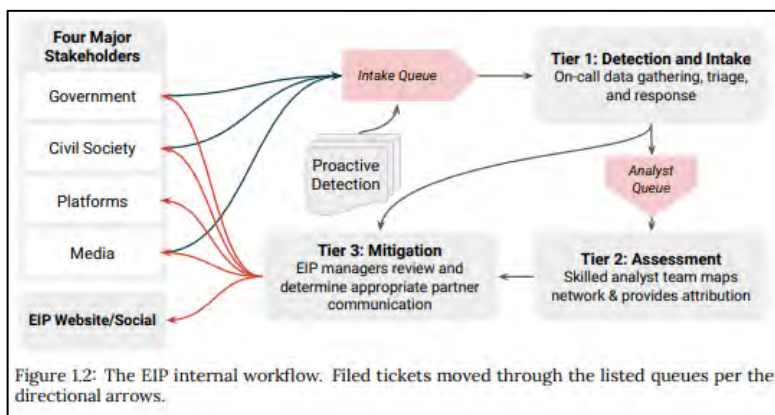
⁹⁰ EIP, *supra* note 85, at v, 2.

⁹¹ Interim EIP Report, *supra* note 76, at 41; see J.A. 222.

⁹² See generally EIP, *supra* note 85.

⁹³ *Ibid.*

⁹⁴ *Id.* at 8.



EIP was thoroughly intertwined with CISA, which aided EIP in the process of reporting undesirable election-related speech to social media platforms.⁹⁵ Stanford confirmed in a letter to Chairman Jordan that CISA was directly “tagged” in a number of Jira tickets “rather than or in addition to” the CISA-funded EI-ISAC.⁹⁶ Some of those involved with EIP worked for CISA, giving them (and CISA) direct access to the tickets.⁹⁷ Other documents obtained by the House Judiciary Committee and Weaponization Subcommittee confirm CISA’s involvement.⁹⁸ “As a consequence, CISA had visibility on what was being submitted to the EIP”—and “social media platforms

⁹⁵ *Id.* at 13.

⁹⁶ Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 27, 2023) (on file with the H. Comm. on the Judiciary).

⁹⁷ Interim EIP Report, *supra* note 76, at 44–54.

⁹⁸ See generally Interim EIP Report, *supra* note 76; Ex. 21 (e-mail from Elena Cryst to TikTok employee (Nov. 4, 2020, 7:41 PM)); Ex. 22 (e-mail from Reddit employee to Alex Stamos (Nov. 3, 2020, 12:36 PM)).

knew that CISA had knowledge of the EIP’s intake.”⁹⁹ So even while “CISA did not directly report content to the EIP, CISA could see what was being reported to the EIP and simultaneously report the same content directly to the social media platforms.”¹⁰⁰

The FBI, the National Security Agency (NSA), and the Global Engagement Center (GEC) were also involved. The GEC is a federal government interagency organization housed within the State Department with the stated mission of countering foreign “propaganda and disinformation efforts.”¹⁰¹ Most notably, the GEC submitted tickets to EIP through Jira and “was one of the most frequently tagged organizations in” Jira.¹⁰² In addition, before the 2020 election, EIP briefed the NSA, and sent one Jira ticket to the FBI.¹⁰³ Social media platforms could

⁹⁹ Interim EIP Report, *supra* note 76, at 47.

¹⁰⁰ *Id.* at 55.

¹⁰¹ U.S. Dep’t of State, About Us—Global Engagement Center, <https://tinyurl.com/43dmawd9> (last visited Jan. 5, 2024); see also Matt Taibbi (@mtaibbi), Twitter (Mar. 2, 2023, 12:00 PM), <https://tinyurl.com/3pmhu8j6> (“GEC’s ‘Chinese’ list included multiple Western government accounts and at least three CNN employees based abroad.”).

¹⁰² Interim EIP Report, *supra* note 76, at 47; see, e.g., Ex. 23 (e-mail from Elena Cryst to Google employee (Nov. 2, 2020, 7:03 PM)).

¹⁰³ Ex. 24 (Excerpts of Transcribed Interview of Alex Stamos before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 23, 2023)).

see which entity submitted a ticket, including federal government entities.¹⁰⁴

The federally funded EI-ISAC also submitted tickets.¹⁰⁵ CISA even coordinated “an agreement” between CIS and EIP to avoid double reporting.¹⁰⁶ The two admittedly became “partners,”¹⁰⁷ sharing personnel.¹⁰⁸ Information obtained to date during the House Judiciary Committee and Weaponization Subcommittee’s investigation confirms that the government-funded EI-ISAC submitted over 100 Jira tickets in the lead-up to the 2020 election.¹⁰⁹

This close affiliation with the federal government heightened the coerciveness of EIP’s interactions with social media platforms. Stanford’s *amicus* brief in this Court claims that “EIP’s decisions about what to escalate to social media platforms were made completely independently.” Br. 25. It also suggests “that CISA did not share tips about instances of misinformation with EIP, did not have general access to EIP tickets identifying instances of misinformation,

¹⁰⁴ Letter from John B. Bellinger III to the Hon. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 7, 2023) (on file with the H. Comm. on the Judiciary).

¹⁰⁵ Ex. 24 (Excerpts of Transcribed Interview of Alex Stamos before the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government (June 23, 2023)), at 114–115.

¹⁰⁶ *Id.* at 212:07–12.

¹⁰⁷ *Id.* at 369:01–11.

¹⁰⁸ *Id.* at 168:22–171:16, 183:20–22.

¹⁰⁹ Letter from John B. Bellinger III to the Hon. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023) (on file with the H. Comm. on the Judiciary).

and did not ‘coordinate’ EIP’s contacts with social media platforms.” *Id.* at 24–25. These claims continue Stanford’s identified pattern of misrepresentations and deceitful public statements about EIP, including to congressional investigators.¹¹⁰

Initially, Stanford told Congress—and still continues to claim on its website—that “EIP did not make recommendations to the platforms about what actions they should take.”¹¹¹ That was and continues to be provably false: despite Stanford’s best efforts to avoid a subpoena, the Committee eventually received dozens of tickets “in which the EIP made a direct recommendation to platforms on what action should be taken.”¹¹²

Then, Stanford claimed that only the GEC submitted tickets, and otherwise it “did not use Jira to receive information from, or share information with, any federal government agencies or officials.”¹¹³ That too was wrong: besides the overlap between CISA personnel and EIP, the Committee obtained documents showing that “CISA personnel were receiving information from or generated by the Jira system” and that “CISA personnel referenced the ‘EIP-’ codes when switchboarding.”¹¹⁴

“[M]ore than a month after” the Committee interviewed a senior Stanford official (Alex Stamos)

¹¹⁰ See Interim EIP Report, *supra* note 76, at 84–92.

¹¹¹ *Id.* at 84.

¹¹² *Ibid.*; see *id.* at 86–87.

¹¹³ *Id.* at 88.

¹¹⁴ *Id.* at 90.

involved with EIP, “Stanford’s counsel finally admitted in a letter to the Committee that CISA was, in fact, involved with the EIP’s Jira system and that CISA had been directly ‘tagged’ on a number of tickets.” Stanford’s counsel claimed that “[a]t the time of Mr. Stamos’s interview, Mr. Stamos was not aware that CISA or CFITF had been “tagged” in any Jira tickets.”¹¹⁵ This assertion was dubious, as tickets that were shared with CISA “were assigned to Stamos.”¹¹⁶ Given that CISA was intimately involved in EIP’s creation and operation, CISA was directly tagged in tickets, CISA personnel had access to the ticket system, and both CISA and EIP were sharing the same information with social media companies, Stanford’s claims before this Court that CISA had no “general access to EIP tickets” and that EIP’s communications were “completely independent[]” (Br. 24–25) are hard to take seriously.

EIP onboarded major social media platforms, gaining privileged access to some of these platforms’ data and the ability to collect such data in real time.¹¹⁷ EIP’s direct recommendations for censorship resulted in the suppression of disfavored speech about the 2020 election. Thirty-five percent of the URLs that EIP “shared with Facebook, Instagram, Twitter, TikTok, and YouTube were either labeled, removed, or soft-blocked.”¹¹⁸ Every Twitter account holder that EIP

¹¹⁵ *Id.* at 91–92.

¹¹⁶ *Id.* at 92.

¹¹⁷ EIP, *supra* note 85, at 17, 181–82; see Ex. 22 (e-mail from Reddit employee to Alex Stamos).

¹¹⁸ EIP, *supra* note 85, at 27.

identified as a “Repeat Spreader” of election-related “disinformation” expressed “conservative or right-wing political views.”¹¹⁹

Content characterized as “disinformation” often did not refer to factually inaccurate posts. “EIP analysts were unable to identify a single external source to support its designation of a particular post or narrative as ‘mis- or disinformation’ in a *majority of posts* it flagged.”¹²⁰

The United States’ coercive tactics with social media platforms to quell election-related messages it finds undesirable are unconstitutional—even when funneled through a private-sector entity. See *Norwood v. Harrison*, 413 U.S. 455, 465 (1973) (“[A] state may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish.” (cleaned up)).

IV. The United States is funding research and tools to enable censorship at scale.

The Committee and Select Subcommittee have also uncovered how the National Science Foundation (NSF) uses taxpayer funds for research into AI-powered censorship and propaganda tools through its Convergence Accelerator Track F program.¹²¹ These

¹¹⁹ *Id.* at 187–88.

¹²⁰ Interim EIP Report, *supra* note 76, at 67.

¹²¹ Staff of H. Comm. on the Jud., Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary, 118th Cong., *The Weaponization of The National*

exchanges provide context for the federal government's other interactions with "disinformation" researchers, such as CISA's interactions with the Election Integrity Partnership.

Non-public documents obtained by the Committee and Select Subcommittee demonstrate that the federal bureaucrats, "disinformation" researchers, and non-profits understood that "content moderation" and combatting so-called misinformation is, in their words, "censorship." The Committee and Select Subcommittee have obtained October 2021 presentation slides with speaker's notes in which researchers pitch their AI-powered tool to NSF as a way for "policy makers at platforms" to "*externaliz[e] the difficult responsibility of censorship.*"¹²²

The Committee and the Select Subcommittee have obtained nonpublic emails and other documents that reveal an intentional effort by NSF to hide its role in funding these censorship and propaganda tools. From legal scholars like Jonathan Turley to conservative journalists, NSF tracked public criticisms of its work in funding censorship projects. In fact, NSF went so far as to develop a media strategy that considered blacklisting certain American media outlets because they were scrutinizing NSF's funding of censorship and propaganda tools.¹²³

Science Foundation: How NSF Is Funding The Development of Automated Tools to Censor Online Speech "At Scale" and Trying to Cover Up Its Actions (Comm. Print Feb. 2024), <http://tinyurl.com/2532hdp5>.

¹²² *Id.* at 1.

¹²³ *Id.* at 2.

Moreover, NSF provided taxpayer funding to researchers who, in their proposal to NSF, cited a study “of two conservative groups” examining the “online search practices” of Americans who hold “the Bible or the Constitution” as “sacred” and “distrust[] journalists and academics.”¹²⁴ The same study claimed that “everyday” Americans “often focused on reading a wide array of *primary* sources, and performing their own synthesis,” “unlike expert lateral readers” who rely on the “expert consensus.”¹²⁵ These types of comments unveil the worldview of “disinformation” researchers, which is paternalistic at best and contemptuous at worst.

Collectively, these documents begin to shed light on why so many in the Executive Branch, Big Tech, and academia have felt entitled to try to limit public debate on issues of national import. The Executive Branch’s self-righteous motives notwithstanding, stifling speech is not only unconstitutional, but it leads to distorted, poorer policy outcomes because ideas can no longer be fairly contested on their merits.

CONCLUSION

The Court should affirm.

¹²⁴ *Id.* at 25–26.

¹²⁵ *Id.* at 26.

Respectfully submitted,

GENE P. HAMILTON
REED D. RUBINSTEIN
MICHAEL DING
America First Legal
Foundation
611 Pennsylvania Ave. SE
#231
Washington, DC 20003
(202) 964-3721
gene.hamilton@aflegal.org

CHRISTOPHER E. MILLS
Counsel of Record
Spero Law LLC
557 East Bay Street
#22251
Charleston, SC 29413
(843) 606-0640
cmills@spero.law

Counsel for Amici Curiae

FEBRUARY 9, 2024

ABUSES OF FEDERAL LAW ENFORCEMENT AGENCIES

A major catalyst for the creation of the Select Subcommittee was the mounting evidence that the Justice Department, under Attorney General Merrick Garland, and the Federal Bureau of Investigation (FBI) under Director Christopher Wray, are broken. During the Biden-Harris Administration, the Justice Department and FBI have advanced a two-tiered system of justice—investigating and prosecuting disfavored individuals or groups with disfavored views. In particular, the FBI has targeted its employees who hold conservative viewpoints, investigated parents at school board meetings, and sought to invade the sacred spaces of Catholic churches in the name of fighting “domestic terrorism.” However, such abuses are not limited to the FBI. Federal agencies including the IRS, the Treasury Department, and other Justice Department components like the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), have misused federal funds to target Americans. The Select Subcommittee has worked to ensure that the government works for the American people, not against them.

I. The weaponization of federal law-enforcement resources against Americans

Rather than focusing its resources on addressing issues like rising crime, rampant illegal immigration, and the fentanyl crisis, federal law enforcement spent much of the Biden-Harris Administration targeting those engaged in constitutionally protected activity. Perhaps nothing is more emblematic of the Justice Department leadership’s disdain for American people than Attorney General Garland’s October 2021 anti-parent memorandum. The Select Subcommittee released a report on March 21, 2023, “[A ‘Manufactured’ Issue and ‘Misapplied’ Priorities: Subpoenaed Documents Show No Legitimate Basis for the Attorney General’s Anti-Parent Memo](#),” detailing the findings of its investigation. The Select Subcommittee conducted oversight of the Biden-Harris Administration’s use of federal law-enforcement and counterterrorism resources against parents voicing concerns about controversial curricula and education-related policies at local school board meetings. This oversight initially began during the 117th Congress, in October 2021, following the issuance of a memorandum from Attorney General Garland directing the FBI and all U.S. Attorney’s Offices—among other Department components—to examine and address threats posed by parents at school board meetings.⁸² At the outset of the 118th Congress, after Republicans resumed control of the House of Representatives, the Committee and Select Subcommittee subpoenaed the Justice Department, FBI, and Education Department for documents necessary to advance the Select Subcommittee’s oversight and inform potential legislative reforms.⁸³ The documents received pursuant to the subpoena showed that there was no legitimate basis for the Attorney General’s directive to insert federal law enforcement into local school board matters and revealed how the Administration worked with leftwing special interest groups to generate the predicate for the Attorney General’s directive.⁸⁴ These documents, along with other corroborating evidence, indicated that the Administration’s actions were a politically motivated offensive meant to quell swelling discord over controversial education curricula and unpopular local school board decisions.⁸⁵

The Select Subcommittee showed that the FBI’s and Justice Department’s disdain for Americans with conservative viewpoints did not end at school board meetings. On May 18, 2023, the Select Subcommittee published a report, “[Report on FBI Whistleblower Testimony Highlights Government Abuse, Misallocation of Resources, and Retaliation](#),” detailing whistleblower testimony from several current and former FBI employees highlighting egregious abuse, misallocation of law-enforcement resources, and misconduct by FBI leadership. These whistleblower disclosures undeniably revealed the political weaponization of the FBI under

⁸² See Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, et al., to Hon. Merrick B. Garland, Att’y Gen., U.S. Dep’t of Justice (Oct. 13, 2021); see Memorandum from Att’y Gen. Merrick Garland, U.S. Dep’t of Justice, Partnership Among Federal, State, Local, Tribal, and Territorial Law Enforcement to Address Threats Against School Administrators, Board Members, Teachers, and Staff (Oct. 4, 2021).

⁸³ See Subpoena from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (Feb. 3, 2023); Subpoena from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Christopher Wray, Dir. Fed. Bureau of Investigation (Feb. 3, 2023); Subpoena from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Miguel Cardona, Sec’y, U.S. Dep’t of Edu. (Feb. 3, 2023).

⁸⁴ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., A “MANUFACTURED” ISSUE AND “MISAPPLIED” PRIORITIES: SUBPOENAED DOCUMENTS SHOW NO LEGITIMATE BASIS FOR THE ATTORNEY GENERAL’S ANTI-PARENT MEMO (Comm. Print Mar. 21, 2023).

⁸⁵ See *id.* at 2.

Director Wray and President Biden.⁸⁶ Additionally, the disclosures described the depths of retaliatory conduct each of the whistleblowers faced after making protected disclosures about what they believed in good faith to be wrongful conduct.⁸⁷

The FBI under Director Wray’s tenure even targeted Americans engaged in the practice of their religion. The Select Subcommittee issued a report on December 4, 2023, “[The FBI’s Breach of Religious Freedom: The Weaponization of Law Enforcement Against Catholic Americans](#),” which exposed the FBI’s categorization of certain Catholic Americans as potential domestic terrorists. This investigation began in February 2023 after a whistleblower revealed the existence of an anti-Catholic memorandum in internal FBI systems.⁸⁸ This memorandum was an official FBI document that cast “radical traditionalist Catholics” as “racially or ethnically motivated violent extremists.”⁸⁹ The memorandum even proposed opportunities for the FBI to infiltrate Catholic churches as a form of “threat mitigation.”⁹⁰ The basis for the memorandum relied on a single investigation in the Richmond Field Office’s area of responsibility in which the subject “self-described” as a “radical-traditionalist Catholic.”⁹¹ However, FBI employees could not define the meaning of “radical-traditionalist Catholic” when preparing, editing, or reviewing the memorandum.⁹² Nevertheless, this single investigation became the basis for an FBI-wide memorandum warning about the dangers of “radical” Catholics.

Through its oversight, the Select Subcommittee obtained documents that showed the FBI abused its counterterrorism tools to target Catholic Americans as potential domestic terrorists and that there was no legitimate basis for the memorandum to insert federal law enforcement into Catholic houses of worship.⁹³ The Select Subcommittee discovered that the FBI relied on at least one undercover agent to develop its assessment, and the FBI even proposed developing sources among the Catholic clergy and church leadership.⁹⁴ Not only did the FBI propose to develop sources, but at the time it released the memorandum, it had already interviewed a priest and choir director affiliated with a Catholic church in Richmond, Virginia.⁹⁵

⁸⁶ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., FBI WHISTLEBLOWER TESTIMONY HIGHLIGHTS GOVERNMENT ABUSE, MISALLOCATION OF RESOURCES, AND RETALIATION (Comm. Print May 18, 2023).

⁸⁷ *Id.*

⁸⁸ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Christopher A. Wray, Director, Fed. Bureau of Investigation at 1 (Feb. 16, 2023) (“On January 23, 2023, the FBI’s Richmond Field Office published an official document that linked ‘racially or ethnically motivated violent extremists’ (RMVEs) with a ‘radical-traditionalist Catholic’ (RTC) ideology.”).

⁸⁹ Fed. Bureau of Investigation, U.S. Dep’t of Justice, Domain Perspective, Interest of Racially or Ethnically Motivated Violent Extremist Radical-Traditionalist Catholic Ideology Almost Certain Presents New Mitigation Opportunities (Jan. 23, 2023) (hereinafter “Catholic Memorandum”).

⁹⁰ *Id.* at FBI-HJC118-DP-000282; 000285 (on file with the Committee).

⁹¹ Inspection Div., Fed. Bureau of Investigation, U.S. Dep’t of Justice, *Strategic Review Report: Richmond Field Office – Domain Perspective Strategic Review* at FBI-HJC118-DP-000294 (2023) (on file with the Committee).

⁹² *Id.* at FBI-HJC118-DP-000297.

⁹³ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE FBI’S BREACH OF RELIGIOUS FREEDOM: THE WEAPONIZATION OF LAW ENFORCEMENT AGAINST CATHOLIC AMERICANS (Comm. Print Dec. 4, 2023).

⁹⁴ *Id.* at 1, 7.

⁹⁵ *Id.* at 1-2, 11.

Under the Biden-Harris Administration, the weaponization of the Justice Department seeped into several of its components—not just the FBI. On May 22, 2024, the Select Subcommittee held a hearing examining overreach by the ATF, which highlighted the ATF’s failure to use sound judgment and follow proper protocol during the execution of a search warrant at the home of Bryan Malinowski in Little Rock, Arkansas.⁹⁶

In the early morning hours of March 19, 2024, at least ten vehicles of armed ATF agents arrived at Malinowski’s home to execute a search warrant.⁹⁷ According to the affidavit in support of the warrant, the ATF reportedly alleged that Malinowski was selling firearms without a license.⁹⁸ Footage from the Malinowskis’ doorbell camera apparently showed ATF agents approaching the house with riot shields and subsequently disabling the camera to prevent their conduct from being recorded.⁹⁹ Upon hearing the commotion and fearful of a home intrusion, Malinowski awoke and prepared to defend his family.¹⁰⁰ Malinowski apparently encountered what he and his wife believed to be home intruders.¹⁰¹ An exchange of gunfire ensued, ATF agents shot Malinowski in the head, and two days later he succumbed to his injuries.¹⁰² Only forty-six seconds transpired between the moment ATF agents first announced themselves and the time that ATF agents shot Malinowski.¹⁰³

The circumstances of Malinowski’s death showed that the ATF failed to use sound judgement and failed to follow proper protocol during the execution of this search warrant. Justice Department policy and President Biden’s Executive Order 14074 requires ATF agents—including those who conducted the search warrant on the Malinowski family home—to wear active body-worn cameras during the execution of a search warrant.¹⁰⁴ However, the Department has confirmed to the Malinowski family that, in violation of Department policy, the ATF agents were not wearing body cameras during the raid.¹⁰⁵

Despite requests from the Select Subcommittee, the ATF has not explained why it resorted to a risky, pre-dawn entry of Malinowski’s home when it could have peacefully executed the warrant while he was away from his residence. The ATF’s affidavit in support of the

⁹⁶ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Govt. of the H. Comm. on the Judiciary*, 118th Cong. (May 22, 2024).

⁹⁷ Neale Zeringue, *Attorney speaks on gun show loophole explained as cause for ATF raid on home of Bryan Malinowski*, KARK (Mar. 22, 2024).

⁹⁸ Alex Kienlen, Neale Zeringue, and Ryan Tuberville, *Released search warrant affidavit shows details of ATF case against Little Rock airport executive Bryan Malinowski*, KARK (Mar. 21, 2024).

⁹⁹ Austin Gelder, *Attorney releases video, says airport exec killed in early morning raid likely mistook ATF agents for intruders*, ARKANSAS TIMES (Apr. 7, 2024).

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ Benjamin Hardy, *UPDATE: ATF shooting of Bryan Malinowski was justified, prosecutor says after review*, ARKANSAS TIMES (Jun. 14, 2023).

¹⁰⁴ Exec. Order No. 14074, 87 C.F.R. 32945 (2022) and Memorandum from Lisa Monaco, Deputy Attorney General, U.S. Dep’t of Justice, to Bureau of Alcohol, Tobacco, Firearms, and Explosives, Drug Enforcement Administration, Federal Bureau of Investigation, United States Marshals Service, Assistant Attorney General for Administration, and Executive Office for United States Attorneys, *Body-Worn Camera Policy* (Jun. 7, 2021); Bureau of Alcohol, Tobacco, Firearms, and Explosives, U.S. Dep’t of Justice, *Special Agent Body Worn Cameras* (Jun. 2, 2022).

¹⁰⁵ Louis Casiano, *Arkansas senators say Clinton airport executive killed by ATF with no bodycam: “Violation of its own policy,”* N.Y. POST (Apr. 20, 2024).

warrant startlingly revealed that ATF agents had conducted surveillance on Malinowski and had developed a pattern of life analysis to understand when he was home or at work.¹⁰⁶ The Malinowskis' attorney, former U.S. Attorney Bud Cummins, testified to the Select Subcommittee that ATF agents strategically gathered on March 12, 2024, one week before the deadly raid, at a nearby Walmart in anticipation of executing the search warrant on the Malinowskis' home.¹⁰⁷ However, Cummins explained that the ATF agents did not execute the search warrant on March 12 as they learned that Malinowski was not at home that morning.¹⁰⁸ This evidence shows that ATF deliberately chose to execute the search warrant when they knew Malinowski was present inside his home.¹⁰⁹ Video security footage from Walmart confirms Cummins's statements.¹¹⁰

The ATF's pre-dawn raid of the Malinowskis' home coincided with the agency's implementation of a regulation to restrict the right to private lawful sales of firearms.¹¹¹ In particular, the ATF seeks to drastically expand the universe of Americans who would be classified as a "dealer" under federal law requiring them to obtain a license to become a Federal Firearms Licensee (FFL),¹¹² subjecting them to a term of imprisonment of up to five years and a fine of up to \$250,000, or both.¹¹³ In May 2024, a federal district court judge issued a temporary restraining order prohibiting enforcement of the ATF rule.¹¹⁴ However, litigation in such matter is ongoing.

The Select Subcommittee has also conducted oversight of the Biden-Harris Administration's weaponization of the Internal Revenue Service (IRS) against law-abiding Americans. In 2022, Democrats in Congress flooded the IRS with \$78.9 billion in new funding, \$45 billion of which was earmarked solely to hire as many as 87,000 agents to aggressively pursue American taxpayers.¹¹⁵ During the 118th Congress, the Republican majority in the House severely curtailed this new funding to ensure that tax dollars were used in ways more beneficial to the American public.¹¹⁶ The Select Subcommittee's oversight shows the wisdom of this action. On October 27, 2023, the Select Subcommittee published a report, "[Fighting the Weaponization of the Internal Revenue Service \(IRS\): The End of Unannounced Field Visits](#)," detailing the results of the Select Subcommittee's investigation of the IRS weaponizing unannounced field visits to intimidate journalist Matt Taibbi—the same day that he testified before the Select

¹⁰⁶ Affidavit in Support of An Application for a Search Warrant, 4:24sw00062 JJV (E.D. Ark Mar. 6, 2024).

¹⁰⁷ Phone Call between Comm. Staff, H. Comm. on the Judiciary, and Mr. Bud Cummins, Counsel for Ms. Maer Malinowski, et al. (Apr. 24, 2024).

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ Email from Bud Cummins, Counsel for Ms. Maer Malinowski, et al., to Comm. Staff, H. Comm. on the Judiciary (Apr. 30, 2024) (including video provided by Walmart) (on file with the Committee).

¹¹¹ Alcohol, Tobacco, Firearms, and Explosives Bureau, Definition of "Engaged in the Business" as a Dealer in Firearms, 88 Fed. Reg. 61993 (Sep. 8, 2023) [hereinafter "ATF Engaged in the Business Rule"].

¹¹² *Id.*

¹¹³ 18 U.S.C. § 922(a)(1)(a) (2024); 18 U.S.C. § 924(a)(1)(D) (2024).

¹¹⁴ *See* Texas v. Bureau of Alcohol, Tobacco, Firearms & Explosives, No. 2:24-CV-89, 2024 U.S. Dist. LEXIS 89647 at *1-3 (N.D. Tex. May 19, 2024).

¹¹⁵ Inflation Reduction Act, P.L. 117-169, 117th Cong. (2022); Alex Muresianu, *IRS Strategic Operating Plan Shows Promise, but Concerns Remain*, TAX FOUND. (Apr. 13, 2023).

¹¹⁶ Family and Small Business Taxpayer Protection Act, 118th Cong. (2023); Brooke Singman, *House votes to rescind billions in funding to the IRS in first major majority action with McCarthy as speaker*, FOX NEWS (Jan 9, 2023).

Subcommittee about government abuse—and to harass and threaten an unsuspecting Ohio taxpayer. Notably, in both cases, neither taxpayer owed anything to the IRS.¹¹⁷ Yet the IRS showed up unannounced at their homes and, in the case of Taibbi, compiled a dossier of information about him as part of its visit.¹¹⁸ After the Select Subcommittee uncovered the degree to which the IRS was abusing this practice, the IRS terminated its decades-long practice of allowing Revenue Officers to conduct unannounced field visits.¹¹⁹ The Select Subcommittee’s oversight resulted in a substantive change that better protects Americans’ privacy and reins in an overly aggressive federal agency.

In addition, the Select Subcommittee conducted oversight of the Justice Department after it was revealed that the Department, in an egregious violation of separation of powers, attempted to access private communications from Members of Congress and congressional staff involved in conducting oversight of the Department. In 2017, classified information about the Department’s misuse of Foreign Intelligence Surveillance Act (FISA) warrants against Trump campaign associate Carter Page was given to the media and published in several articles.¹²⁰ Eventually, the Department tried and convicted James Wolfe, a longtime Democrat staffer on the Senate Select Intelligence Committee, for the unauthorized disclosure of sensitive information.¹²¹ However, the breadth of the Department’s efforts to identify the leaker were not fully realized until 2023, when Google and other telecommunications companies provided notice—after the Department’s repeated nondisclosure orders lapsed—to its users that the Department had subpoenaed for their personal information.¹²²

The Justice Department investigated a swath of Republican and Democrat congressional staffers, including former Chief Investigative Counsel to then-Senate Judiciary Committee Chairman Charles Grassley who, at the time, was conducting vigorous oversight of the Department.¹²³ Google’s notification to this staffer revealed the Justice Department likely also sought the personal records and communications of countless other congressional staffers—both Republicans and Democrats—who engaged in similar oversight during the same period.¹²⁴ This revelation followed reporting that the Department issued subpoenas to obtain the private emails and records of Members of Congress and congressional staffers on the House Permanent Select Committee on Intelligence who were conducting oversight of the Justice Department’s Crossfire

¹¹⁷ See Letter from Mr. Matt Taibbi to H. Comm. on the Judiciary (Mar. 21, 2023); E-mail from taxpayer to H. Comm. on the Judiciary (May 17, 2023, 4:07 PM) (on file with the Committee).

¹¹⁸ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., FIGHTING THE WEAPONIZATION OF THE INTERNAL REVENUE SERVICE: THE END OF ABUSIVE UNANNOUNCED FIELD VISITS at 11-12 (Comm. Print Oct. 27, 2023).

¹¹⁹ Press Release, IRS ends unannounced revenue officer visits to taxpayers; major change to end confusion, enhance safety as part of larger agency transformation efforts, Internal Revenue Serv. (July 24, 2023).

¹²⁰ Press Release, Attorney General Jeff Sessions Delivers Remarks at Briefing on Leaks of Classified Materials Threatening National Security, Off. of Pub. Aff., U.S. Dep’t of Justice (Aug. 4, 2017).

¹²¹ Press Release, Former U.S. Senate Employee Sentenced to Prison Term on False Statements Charge, U.S. Att’y Off., D.D.C. (Dec. 18, 2018).

¹²² See, e.g., Press Release, Chairman Jordan Launches Inquiry into the DOJ’s Attempts to Spy on Congress, H. Comm. on the Judiciary (Oct. 31, 2023).

¹²³ Press Release, Empower Oversight Seeks Information from Justice Department on Subpoenas of Congressional Staff Phone and Email Records, Empower Oversight (Oct. 24, 2023).

¹²⁴ See *id.* at 2; Margot Cleveland, *DOJ Subpoenaed Phone And Email Logs Of Hill Staffers Probing Crossfire Hurricane Malfeasance*, The Federalist (Oct. 25, 2023).

Hurricane investigation.¹²⁵ Taken together, these facts strongly suggests that the Justice Department weaponized its law-enforcement authority to spy on the entities seeking to hold it accountable.

The Select Subcommittee’s oversight led the Department to concede that its actions were improper and to adopt bolstered criteria for opening investigations implicating Members of Congress and congressional staff members.¹²⁶ On November 8, 2023, the Justice Department informed the Select Subcommittee of “a change to the Department of Justice’s policies and procedures in criminal investigations involving Members of Congress and their staff” that “impose[s] new requirements to consult with, or receive approval from, the Public Integrity Section.”¹²⁷

During the Biden-Harris Administration, federal law enforcement consistently turned against the American people. Despite federal law enforcement’s task to protect all Americans, the Biden-Harris Administration pursued a two-tiered system of justice. In fact, the Justice Department silenced conservatives, investigated parents at school board meetings, and called pro-life Catholics extremists. Further, as noted above, the ATF failed to follow protocol and execute sound judgement in its deadly raid in Little Rock, Arkansas. Additionally, the IRS conducted unannounced visits to taxpayers’ homes, including a hearing witness while he was testifying before the Subcommittee. As a result of the Select Subcommittee’s oversight, the Administration rolled back some of these abusive policies, but work remains to ensure that law enforcement works for Americans and not against them.

¹²⁵ Cleveland, *supra* note 124.

¹²⁶ See Justice Manual § 9-85.110 Investigations Involving Members of Congress.

¹²⁷ E-mail from Off. of Legis. Affairs, U.S. Dep’t of Justice, to Comm. Staff, H. Comm. on the Judiciary (Nov. 8, 2023); see also Memorandum from the Deputy Attorney General: Policies and Procedures in Criminal Investigations Involving Members of Congress and Staff (Nov. 7, 2023).



**A “MANUFACTURED” ISSUE AND “MISAPPLIED” PRIORITIES:
SUBPOENAED DOCUMENTS SHOW NO LEGITIMATE BASIS FOR THE
ATTORNEY GENERAL’S ANTI-PARENT MEMO**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



March 21, 2023

EXECUTIVE SUMMARY

The Committee on the Judiciary is conducting oversight of the Biden Administration’s use of federal law-enforcement and counterterrorism resources against parents voicing concerns about controversial curricula and education-related policies at local school board meetings. This oversight began in October 2021 following the issuance of a memorandum from Attorney General Merrick Garland directing the Federal Bureau of Investigation and all U.S. Attorney’s Offices—among other Department components—to examine and address threats posed by parents at school board meetings.

Although the Biden Administration declined to cooperate with this oversight in the 117th Congress, whistleblower disclosures and a report commissioned by the National School Boards Association (NSBA) shed some light on how the Biden Administration colluded with the NSBA to create a justification to use federal law-enforcement and counterterrorism resources against parents. There were gaps in the information available to the Committee then, primarily because the Biden administration did not participate in the NSBA’s third-party report. On February 3, 2023, Chairman Jordan subpoenaed the Justice Department, FBI, and Education Department for documents necessary to advance the Committee’s oversight and inform potential legislative reforms.

From the initial set of material produced in response to the subpoenas, it is apparent that the Biden Administration misused federal law-enforcement and counterterrorism resources for political purposes. The Justice Department’s own documents demonstrate that there was no compelling nationwide law-enforcement justification for the Attorney General’s directive or the Department components’ execution thereof.¹ After surveying local law enforcement, U.S. Attorney’s offices around the country reported back to Main Justice that there was no legitimate law-enforcement basis for the Attorney General’s directive to use federal law-enforcement and counterterrorism resources to investigate school board-related threats. For example:

- One U.S. Attorney reported that “this issue was very poorly received” by his local law-enforcement community and “described by some as a manufactured issue.”² He continued: “No one I spoke with in law enforcement seemed to think that there is a serious national threat directed at school boards, which gave the impression that our priorities are misapplied.”³
- Another U.S. Attorney’s Office reported that the local FBI field office in the area “did not see any imminent threats to school boards or their members . . . , nor did they ascertain any worrisome trends in that regard.”⁴

¹ In fact, Attorney General Garland admitted as much in his October 2021 testimony to the Committee, conceding that the National School Boards Association letter was the only basis for the Department’s actions. *See Oversight of the United States Department of Justice: Hearing Before the H. comm. on the Judiciary*, 117th Cong. at 68 (2021) (testimony from Hon. Merrick Garland, Atty Gen., U.S. Dep’t of Justice).

² DOJ-HJC-0000212.

³ *Id.*

⁴ DOJ-HJC-0000127.

- Local law-enforcement officials noted that local officials should properly respond to school board threats. In Montana, several law-enforcement offices rightly advised the Justice Department that “local law enforcement authorities are best suited to address criminal threats against school board administrators.”⁵
- Most threats reported back to Main Justice had little connection to school board matters. For example, the Southern District of Alabama reported that although one of the school board member’s houses was shot at, the incident was the “unfortunate consequence of gun violence in the city” and not related to school board decisions or policies.⁶

The documents received pursuant to the Committee’s subpoena show the absence of a legitimate nationwide basis for the Attorney General’s directive to insert federal law enforcement into local school board matters. The documents also shed light onto how the Administration worked with education special interests to generate the predicate for the Attorney General’s directive. It appears, from these documents and the information received previously, that the Administration’s actions were a political offensive meant to quell swelling discord over controversial education curricula and unpopular school board decisions. The Attorney General’s directive came just weeks before a pivotal gubernatorial election in Virginia, in which education policies were hotly debated and a local school board’s actions were under intense scrutiny.⁷ The inference from the initial tranche of subpoenaed documents is that the Justice Department’s actions were a reaction to these political circumstances rather than a legitimate law-enforcement response to any serious, nationwide threat.

In response to the Committee’s subpoena, the FBI acknowledged for the first time that it opened 25 “Guardian assessments” of school board threats, and that six of these investigations were run by the FBI’s Counterterrorism Division.⁸ These admissions supplement whistleblower disclosures about the FBI’s actions, including disclosures the FBI investigated a mom because she belonged to a “right-wing mom’s group” and “is a gun owner” and a dad because “he rails against the government.” According to the FBI, none of the school board-related investigations have resulted in federal arrests or charges, highlighting the political motives behind the Attorney General’s actions. The Administration’s goal seems to have been silencing the critics of its radical education policies and neutralizing an issue that was threatening Democrat Party prospects in the close gubernatorial race in Virginia.

This weaponization of law-enforcement powers against American parents exercising their First Amendment rights is dangerous. The Justice Department subjected moms and dads to the opening of an FBI investigation about them, the establishment of an FBI case file that includes their political views, and the application of a “threat tag” to their names as a direct result of their exercise of their fundamental constitutional right to speak and advocate for their children. The Committee has called on Attorney General Garland to rescind his memorandum, which he has

⁵ DOJ-HJC-0000082.

⁶ DOJ-HJC-0000219.

⁷ See generally Emily Crane, *Loudoun County school board faces parents again after sexual assault controversy*, N.Y. POST (Dec. 1, 2021).

⁸ Letter from Mr. Christopher Dunham, Acting Assistant Director, Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Mar. 1, 2023).

refused to do. From the documents and information received pursuant to the subpoena, it is crystal clear that Attorney General Garland should rescind his unwise and unsupported directive to insert federal law enforcement into local school board matters.

The House Committee on the Judiciary, through and with its Select Subcommittee on the Weaponization of the Federal Government, is charged with investigating “violations of the civil liberties of citizens of the United States.”⁹ This interim staff report fulfills the ongoing obligation to identify and report on instances of the weaponization of the federal government—here, the misuse of federal law-enforcement and counterterrorism resources against parents exercising their First Amendment rights at school board meetings. While the documents produced to date help to better understand what transpired, they do not tell the whole story. The Committee and the Select Subcommittee will continue to pursue the relevant facts to inform legislative reforms to protect American civil liberties.

⁹ H. Res. 12 § 1(b)(D).

TABLE OF CONTENTS

Executive Summary.....	1
Table of Contents	4
Background.....	5
New Information in the Subpoenaed Documents.....	9
I. Internal Executive Branch communications show that the Biden Administration and NSBA extensively colluded prior to the Attorney General’s memorandum.....	9
II. If the Justice Department performed due diligence before promulgating the Attorney General’s memorandum, the Department would have learned it lacked a legitimate predicate.	13
III. Local officials generally opposed federal intervention at local school board meetings....	17
Conclusion.....	20

BACKGROUND

In October 2021, House Judiciary Committee Republicans opened an investigation into the Biden Administration’s misuse of federal law-enforcement resources to target concerned parents. Since then, Committee Republicans have sent over 100 letters to Department of Justice components requesting documents and information related to this investigation.¹⁰ Additionally, Republicans have sent four letters to the Department of Education.

With help from brave whistleblowers and the NSBA-commissioned report, the Committee uncovered initial information in the 117th Congress about the Biden Administration’s misuse of its authorities. From the information available then, the Committee learned the following:

- The NSBA collaborated with the Biden White House to develop the language of the NSBA’s September 29, 2021 letter to President Biden urging the use of federal law-enforcement and counterterrorism tools, including the Patriot Act, against parents.¹¹
- The NSBA shared the draft language of its letter with the White House, which apparently raised no concerns with the reference to counterterrorism tools or the inclusion of the Patriot Act in the letter.¹²
- Five days after the NSBA letter to President Biden, on October 4, Attorney General Garland issued a memorandum that inserted federal law enforcement into local school board meetings.¹³
- Attorney General Garland established a task force—including the Department’s National Security Division, with responsibility for enforcing federal counterterrorism statutes—to examine school board-related threats and highlighted the FBI’s National Threat

¹⁰ See Letter from Rep. Mike Johnson *et al.*, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (Oct. 13, 2021); Letter from Rep. Jim Jordan *et al.*, Ranking Member, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (Oct. 25, 2021); Letter from Rep. Jim Jordan *et al.*, Ranking Member, H. Comm. on the Judiciary, to Mr. E. Bryan Wilson *et al.*, Acting U.S. Att’y, Dist. of Alaska (Nov. 1, 2021); Letter from Rep. Jim Jordan *et al.*, Ranking Member, H. Comm. on the Judiciary, to Mr. Mark Lesko, Acting Assistant Att’y Gen., Nat’l Sec. Div., U.S. Dep’t of Just. (Nov. 2, 2021); Letter from Rep. Jim Jordan *et al.*, Ranking Member, H. Comm. on the Judiciary, to Hon. Christopher Wray, Dir., Fed. Bureau of Investigation (Nov. 3, 2021); Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (Nov. 16, 2021); Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Christopher Wray, Dir., Fed. Bureau of Investigation (Nov. 18, 2021); Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Christopher Wray, Dir., Fed. Bureau of Investigation (Feb. 10, 2022); Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (May 11, 2022); Letter from Rep. Jim Jordan *et al.*, Ranking Member, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (Jun. 14, 2022).

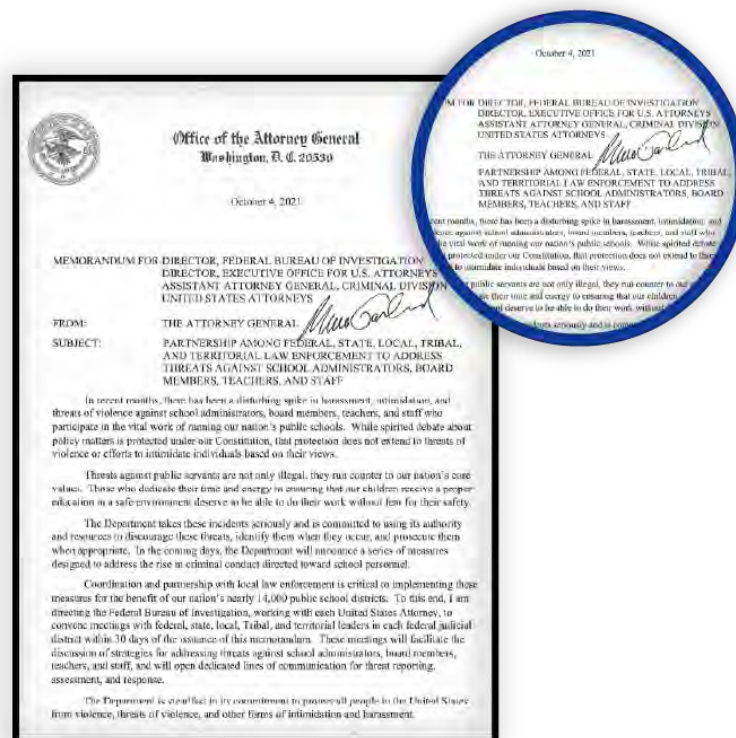
¹¹ Callie Patteson, *WH ‘actively engaged’ with NSBA before ‘domestic terror’ letter: memo* N.Y. POST (Nov. 11, 2021).

¹² *Final Report On the Events Surrounding the National School Boards Association’s September 29, 2021, Letter to the President*, NAT’L SCHOOL BOARDS ASSOC. (May 20, 2022).

¹³ Memorandum from Att’y Gen. Merrick Garland, U.S. Dep’t of Justice, Partnership Among Federal, State, Local, Tribal, and Territorial Law Enforcement to Address Threats Against School Administrators, Board Members, Teachers, and Staff (Oct. 4, 2021).

Operations Center to serve as a snitch-line for tips about parents at school board meetings.¹⁴

- In testimony to the Committee, Attorney General Garland admitted that the sole basis of his memorandum was the NSBA letter sent to President Biden.¹⁵
- On October 20, 2021, the FBI’s Counterterrorism and Criminal Divisions operationalized the Attorney General’s directive, announcing to all FBI special agents in charge the creation of a new threat tag—EDUOFFICIALS—to track school board-related threats.¹⁶



The FBI later opened dozens of investigations into parents’ conduct at school board meetings, using the EDUOFFICIALS threat tag, in almost every region of the country and relating to all types of educational settings.¹⁷ Whistleblower disclosures to the Committee showed how, as a direct result of Attorney General Garland’s October 4 directive, federal law enforcement is using counterterrorism resources to investigate protected First Amendment activity. For example:

¹⁴ Press Release, U.S. Dep’t of Justice, Justice Department Addresses Violent Threats Against School Officials and Teachers (Oct. 4, 2021).

¹⁵ *Oversight of the United States Department of Justice: Hearing Before the H. Comm. on the Judiciary*, 117th Cong. At 92 (2021) (testimony from Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Justice).

¹⁶ See Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (May 11, 2022).

¹⁷ *Id.*

- In one investigation, an FBI field office interviewed a mom for allegedly telling a local school board “we are coming for you.” The complaint, which came into the FBI through the National Threat Operations Center snitch-line, alleged that the mom was a threat because she belonged to a “right wing mom’s group” known as “Moms for Liberty” and because she “is a gun owner.” When the FBI interviewed the mom, she told the agent that she was upset about the school board’s mask mandates and that her statement was a warning that her organization would seek to replace the school board with new members through the electoral process.
- An FBI field office opened an investigation into a dad opposed to mask mandates. The complaint came in through the National Threat Operations Center snitch-line and alleged that the dad “fit the profile of an insurrectionist” because he “rails against the government,” “believes all conspiracy theories,” and “has a lot of guns and threatens to use them.” When an FBI agent interviewed the complainant, the complainant admitted they had “no specific information or observations of . . . any crimes or threats,” but they contacted the FBI after learning the Justice Department had a website “to submit tips to the FBI in regards to any concerning behavior directed toward school boards.”
- In another case, an FBI field office opened an investigation into Republican state elected officials after a state Democrat party official accused them of making an “online terroristic threat by politicians against school board members.” This complaint also came into the FBI through the National Threat Operations Center snitch-line. It alleged that one Republican official “incited violence” against school board members by expressing displeasure with school districts’ vaccine mandates.

These investigations into concerned parents were the direct result of Attorney General Garland’s October 4 directive. Each of the cases was initiated following the directive and the complaints came into the FBI through the same snitch-line—the National Threat Operations Center—highlighted in the press release accompanying the October 4 memorandum. One complainant even told an FBI agent that they reported the tip to the FBI because of the snitch-line, despite having “no specific information” about any actual threat.

The FBI later disclosed—only after Chairman Jordan’s subpoena to Director Wray—that it had opened 25 “Guardian assessments” with the EDUOFFICIALS threat tag.¹⁸ The FBI assigned seventeen of the investigations to the Criminal Investigative Division, six to the Counterterrorism Division, and two to the Weapons of Mass Destruction Directorate.¹⁹ The FBI acknowledged that it “has not observed an uptick of threats directed at school officials since it began tracking the data.”²⁰ Of the 25 investigations, the FBI determined that only one warranted opening a “Full Investigation,” and referred the majority of the remaining cases to state and local authorities.²¹ There have still been no federal prosecutions.

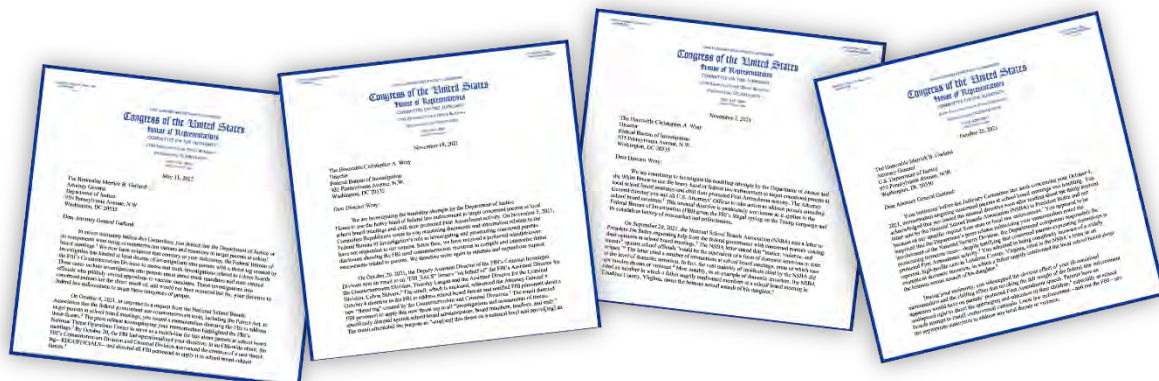
¹⁸ Letter from Mr. Christopher Dunham, Acting Assistant Director, Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Mar. 1, 2023).

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

The Administration did not comply fully with the Committee’s oversight in the 117th Congress. Early in the 118th Congress, Chairman Jordan renewed the outstanding requests to the Justice Department, FBI, Education Department, and White House.²² Still, the Administration declined to comply fully and on February 3, 2023, the Committee issued a subpoena to compel the production of documents. On February 28, 2023—the day before the Justice Department was required to comply with the Committee’s subpoena—the Department produced 448 pages of documents. On the same day, the Education Department produced 1,004 pages of heavily redacted documents. Both departments indicated that they would continue to produce responsive material going forwards.²³



²² See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Miguel Cardona, Sec’y, U.S. Dep’t of Edu. (Jan. 17, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (Jan. 17, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Ronald Klain, Ass’t to the President and Chief of Staff (Jan. 17, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Christopher Wray, Dir., Fed. Bureau of Investigation (Jan. 17, 2023).

²³ Letter from Hon. Carlos Uriarte, Assistant Att’y Gen., U.S. Dep’t of Just., to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 28, 2023); Letter from Hon. Gwen Graham, Assistant Sec’y, U.S. Dep’t of Educ., to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Feb. 28, 2023).

NEW INFORMATION IN THE SUBPOENAED DOCUMENTS

The Committee’s subpoenas have returned new information that demonstrates how the Biden Administration misused its federal law-enforcement and counterterrorism resources on school board-related threats. The documents shed new light on the Administration’s coordination with education special interests to generate the predicate for the Justice Department’s actions. The subpoenaed documents show there was no legitimate nationwide basis for the Attorney General’s directive to insert federal law enforcement into local school board matters. In fact, almost universally, local law enforcement rejected the directive and expressed strong preference that local authorities handle local matters.

I. Internal Executive Branch communications show that the Biden Administration and NSBA extensively colluded prior to the Attorney General’s memorandum.

As the radical left continued to push a woke agenda on America’s children, parents across the country started to speak out at school board meetings against critical race theory, mask mandates, and controversial curricula. As more parents spoke out, the NSBA and the Biden Administration colluded to create a justification, articulated in an October 4 memorandum from Attorney General Garland, to use federal law-enforcement tools to silence parents. The initial documents produced in response to the Committee’s subpoena provide more details on the extent of that coordination.

A. Prior to the October 4 memorandum, the Department of Education and White House worked with a left-leaning group to promote calls for federal law-enforcement intervention.

On September 16, 2021, CEO of the National Association of Secondary School Principals (NASSP) Ronn Nozoe emailed Mary C. Wall, of the White House COVID-19 Response Team, about NASSP’s September 16, 2021, press release calling for the “federal government to protect school leaders from threats and violence.”²⁴ Mr. Nozoe asked Ms. Wall to share it with her networks.²⁵ That same day, employees at the Department of Education set a meeting to discuss the NASSP’s press release.²⁶ The Education Department redacted much of these internal communications among its employees, preventing the Committee from fully understanding the nature and circumstances of these discussions.²⁷

On September 20, 2021, Dr. Aaliyah Samuel, Deputy Assistant Secretary, Local, State and National Engagement in the Office of Communications and Outreach at the Department of Education, emailed Mr. Nozoe requesting a time to talk.²⁸ Mr. Nozoe sent an email with the

²⁴ HJC-118-0000337; HJC-118-0000338. In the press release, Mr. Nozoe called for the “full authority of the federal government to help us remove or ban threatening individuals from our schools who are determined to do nothing more than disrupt learning or potentially harm us or our staff” and for the Department of Education to issue specific guidance on the authority school leaders possess to oust concerned parents.

²⁵ HJC-118-0000338.

²⁶ See HJC-118-0000352; HJC-118-00003363; HJC-118-0000364.

²⁷ The Department of Education did not provide justifications for its redactions throughout the document production, in its cover letter, or in the document production itself.

²⁸ See HJC-118-0000793.

following three requests:

- “Build safe zones around schools – similar to drug free zones. Make it a federal crime to threaten any educator/school staff on school property.”²⁹
- “Set up a 911 Network to report physical and social threats. Establish an ombudsman at the federal level with a direct line to the FBI/Justice Department. Do not leave it solely up to local authorities to determine the severity of the threats.”³⁰
- “Provide legal protections for all educators by creating a legal defense fund so school leaders who have been maligned in their community can get legal assistance to protect/repair their reputations. . . . [W]e are asking for a fund to be set up so school leaders who have had their reputations smeared in public/social media/local media because of mask/no mask vax/no vax mandates do not have to dig into their personal savings to hire attorneys for defamation of character/slander legal action necessary to clear their names.”³¹

Dr. Samuel forwarded the chain to other employees at the Department of Education, but the Department redacted the majority of the content of these communications. Additionally, Dr. Samuel added Ms. Wall to an email thread among Department of Education officials discussing the NASSP’s requests, but Ms. Wall’s message back to the group was also redacted.³²

B. The NSBA sent the Department of Education its letter before it was public.

On September 29, 2021, Chip Slaven, the Interim Director and CEO of the NSBA, emailed the NSBA’s letter to President Biden regarding threats against school officials to Julie Rodriguez at the White House and copied Dr. Samuel at the Department of Education.³³ Dr. Samuel forwarded the NSBA’s letter to several other Department of Education officials.³⁴ In the email, Mr. Slaven thanked the Department of Education for “the recent opportunity to discuss these issues with the White House and Administration officials.”³⁵ Mr. Slaven further explained that the NSBA’s letter to President Biden requests that “federal law enforcement and relevant agencies work with state and local authorities and public schools to address these ongoing threats.”³⁶ Mr. Slaven did well to ensure that the Department of Education received the NSBA’s letter one day before its public release.³⁷ On October 1, 2021, there are emails involving several

²⁹ HJC-118-0000792; HJC-118-0000793.

³⁰ The reference to social threats here indicates the NASSP desired, and the Department of Justice and/or Department of Education may have considered, silencing parents for merely criticizing school board officials. Furthermore, the NASSP’s proposal of creating a reporting phone line mirrors the hotline created by the Justice Department just two weeks later. *See* Press Release, U.S. Dep’t of Just., Justice Department Addresses Violent Threats Against School Officials and Teachers (Oct. 4, 2021).

³¹ HJC-118-0000792; HJC-118-0000793.

³² HJC-118-0000073.

³³ *See* HJC-118-0000508.

³⁴ *See* HJC-118-0000526.

³⁵ HJC-118-0000508.

³⁶ *Id.*

³⁷ *Id.* The NSBA sent the letter to the Biden Administration and its members on Sept. 29, 2021; however, the letter was “embargoed” until Sept. 30, 2021, when it was made available to the media. *See id.*

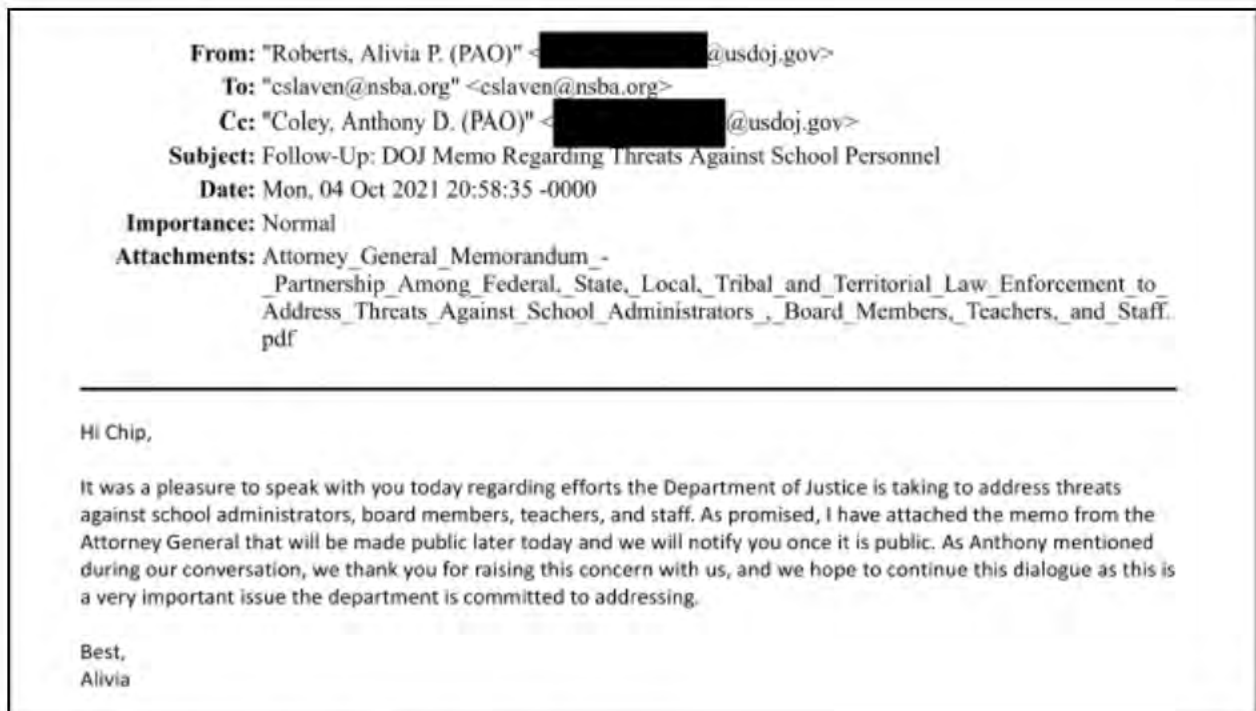
Department of Education officials—Sheila Nix, Chief of Staff; Suzanne Goldberg, Deputy Assistant Secretary for Strategic Operations and Outreach, Office of the Assistant Secretary for Civil Rights at the Department of Education; Dr. Aaliyah Samuel; Scott Sargrad, Deputy Chief of Staff for Policy and Programs; and Emma Leheny, formerly Principal Deputy General Counsel and Acting General Counsel—asking if anyone had “any more thoughts” on the NSBA letter, but the Department redacted the content of those conversations as well.³⁸

C. The Justice Department and the NSBA coordinated prior to the release of Attorney General Garland’s October 4, 2021 memorandum.

On October 4, 2021, Alivia Roberts, from the Justice Department’s Public Affairs Office, sent an email to NSBA Interim Executive Director and CEO Chip Slaven attaching the Attorney General’s memorandum before it was publicly released, writing:

It was a pleasure to speak with you today regarding efforts the Department of Justice is taking to address threats against school administrators, board members, teachers, and staff. . . . [W]e thank you for raising this concern with us, and we hope to continue this dialogue as this is a very important issue the department is committed to addressing.³⁹

Mr. Slaven responded by writing, “[NSBA] stand[s] ready to work with you on efforts going forward. Please let us [know] how we can support your efforts.”⁴⁰



³⁸ HJC-118-0000823; 0000825; 0000833; 0000835; 0000843.

³⁹ DOJ-HJC-0000441.

⁴⁰ DOJ-HJC-0000446.

On October 6, 2021, Mr. Slaven reached out to Anthony Coley, also from the Justice Department’s Public Affairs Office, notifying him that calls and emails to NSBA were increasing and saying they had reported several to the Alexandria Police Department.⁴¹ He also asked for a contact at the FBI with whom the NSBA could communicate. Mr. Coley responded that threats of violence should be reported to the local FBI office or the FBI’s National Threat Operations Center tip line.⁴²

D. There was collaboration between the Justice Department and the Department of Education.

Three days prior to Attorney General Garland issuing his October 4, 2021 memorandum, Shaylyn Cochran, Chief of Staff in the Office of the Assistant Attorney General for the Civil Rights Division, connected Myesha Brayden, a Justice Department employee, to Suzanne Goldberg, Deputy Assistant Secretary for Strategic Operations and Outreach, at the Department of Education, because both were “looking into” the issue of alleged threats directed at school board officials.⁴³ Ms. Cochran suggested that the two “may benefit from connecting to determine any joint equities between DOJ and ED-OCR.”⁴⁴

A week later, Ms. Goldberg’s assistant scheduled time for her to speak with another Associate Deputy Attorney General, Kevin Chambers, who was also involved in the issue.⁴⁵ Whether or not they eventually spoke—and what about—is not clear. On October 5, 2021, Emma Leheny at the Department of Education shared the October 4 Justice Department press release on addressing threats against school officials with Ms. Goldberg, who indicated she “never heard back from the point-person there.”⁴⁶

Officials at the Department of Education responded with approval to the NSBA’s successful attempt to involve federal law enforcement at local school board meetings.⁴⁷ After the release of the Attorney General’s October 4, 2021 memorandum, officials at the Department of Education praised the move, calling it “noteworthy.”⁴⁸ In fact, Ms. Goldberg wrote to Associate Deputy Attorney General Kevin Chambers that she was “very glad to see the memo.”⁴⁹

⁴¹ DOJ-HJC-0000447.

⁴² *See id.*

⁴³ HJC-118-0000821.

⁴⁴ *Id.*

⁴⁵ HJC-118-0000089.

⁴⁶ HJC-118-0000850.

⁴⁷ *See* HJC-118-0000520; HJC-118-0000570.

⁴⁸ HJC-118-0000655.

⁴⁹ HJC-118-000570.

From:	Goldberg, Suzanne
Subject:	Re: [EXTERNAL] RE: DOJ-ED connection, school board meeting disruptions
To:	
Cc:	Chambers, Kevin (ODAG); Zinsner, Addie
Sent:	October 6, 2021 7:32 AM (UTC-04:00)

Kevin, Thanks for your voicemail on Monday. I am not sure why but it only just popped up on my phone this morning.

I was very glad to see the memo, and it would be great to talk in the coming day or two. My schedule is quite cramped as I imagine yours is as well so I am copying Addie Zinsner here to help us find time.

Looking forward to talking soon.

Best,
Suzanne

II. If the Justice Department performed due diligence before promulgating the Attorney General’s memorandum, the Department would have learned it lacked a legitimate predicate.

The documents produced indicate that Attorney General Garland’s October 4, 2021 memorandum—inserting federal law enforcement into local school board meetings—was a misuse of federal authority. Internal Justice Department communications show that had Attorney General Garland performed a modicum of due diligence prior to issuing his memorandum, he would have learned that there was no “disturbing spike” in alleged threats and violence at school board meetings, as he alleged in his memorandum.⁵⁰ The documents show that beyond the NSBA’s letter—which it has since retracted—the evidence does not support any legitimate, nationwide predicate for deploying federal law-enforcement resources against America’s parents.

A. In the days following the issuance of the October 4, 2021 memorandum, Justice Department officials expressed confusion as to how to implement the Attorney General’s directive.

On October 7, 2021, the Deputy Director of the Justice Department’s Office of Public Affairs⁵¹ sent an email to “USAEO-Public Affairs Officers”⁵² list recipients clarifying the Attorney General’s October 4 memorandum and addressing “a rash of misinformation about this memo suggesting it somehow limits parental free speech or label[s] parents as ‘domestic terrorists.’”⁵³ The email included a “set of facts/talking points for use by [U.S. Attorney Offices] in meeting with law enforcement partners, community stakeholders, and the press to keep the record straight as this process plays out.”⁵⁴ The email also included sections of the Attorney General’s memorandum in bold type to emphasize how it should be interpreted and portrayed to stakeholders.⁵⁵

⁵⁰ Memorandum from Hon. Merrick Garland, Atty Gen., U.S. Dep’t of Justice, Partnership Among Federal, State, Local, Tribal, And Territorial Law Enforcement to Address Threats Against School Administrators, Board Members, Teachers, and Staff (Oct. 4, 2021).

⁵¹ The Justice Department redacted this federal employee’s name from its production to the Committee.

⁵² “USAEO” likely refers to the Executive Office for the United States Attorneys.

⁵³ DOJ-HJC-0000409.

⁵⁴ *Id.*

⁵⁵ *See id.*

On October 21, 2021, a person, whose name is redacted, from the U.S. Attorney’s Office for the Southern District of Indiana sent an email to a redacted list of recipients, including the Justice Department’s Public Affairs Office, asking if they had any guidance other than the October 7, 2021 talking points, as they were getting questions about what actions their office was taking concerning threats or disruptions to local school boards.⁵⁶ After some back and forth, the Southern District of Indiana employee explained that their response was “[t]he U.S. Attorney’s Office will comply with the Attorney General’s request as set forth in his memo of October 4, 2021,” to which the Public Affairs Office replied, “That seems fine.”⁵⁷

In addition, employees from different U.S. Attorney’s Offices reached out to each other to learn of other Districts’ plans in response to the Attorney General’s memo. An email from the U.S. Attorney’s Office for the District of Oregon to the USAEO-LEC listserv group asked what plans the Districts have made in response to the Attorney General’s memorandum.⁵⁸ An employee in the U.S. Attorney’s Office for the District of Alaska responded by stating their office was “proposing a joint virtual training with state [law enforcement] agency heads” and “hoping to include [the] state Director of Law in the training.”⁵⁹ The employee stated the USAO and FBI were “awaiting additional guidance and more information regarding the ‘series of measures designed to address the rise in criminal conduct directed towards school personnel’ as referenced in the AG’s memo.”⁶⁰

B. Reported instances of school board officials being threatened were almost nonexistent.

On October 20, 2021, Monty Wilkinson, Director of the Executive Office for United States Attorneys, sent a memorandum to all U.S. Attorneys’ Offices with guidance for implementing the Attorney General’s October 4, 2021 memorandum.⁶¹ Director Wilkinson’s memorandum directed U.S. Attorneys’ Offices to convene a meeting by November 3, 2021, with appropriate district law enforcement leaders and to notify the Executive Office that they had held the meeting, identify which agencies participated, and note any significant issues for the Deputy Attorney General’s attention.⁶² The memorandum specified that the “purpose of these meetings is to address violations of criminal law regarding harassment, intimidation, threats of violence, and actual violence against school officials, teachers, and employees”⁶³

The overwhelming majority of judicial districts reported not having heard of any instances of threats or violence being levied at school board officials.⁶⁴ One U.S. Attorney

⁵⁶ See DOJ-HJC-0000403; 0000404; 0000405.

⁵⁷ DOJ-HJC-0000403.

⁵⁸ DOJ-HJC-0000408.

⁵⁹ DOJ-HJC-0000429.

⁶⁰ *Id.*

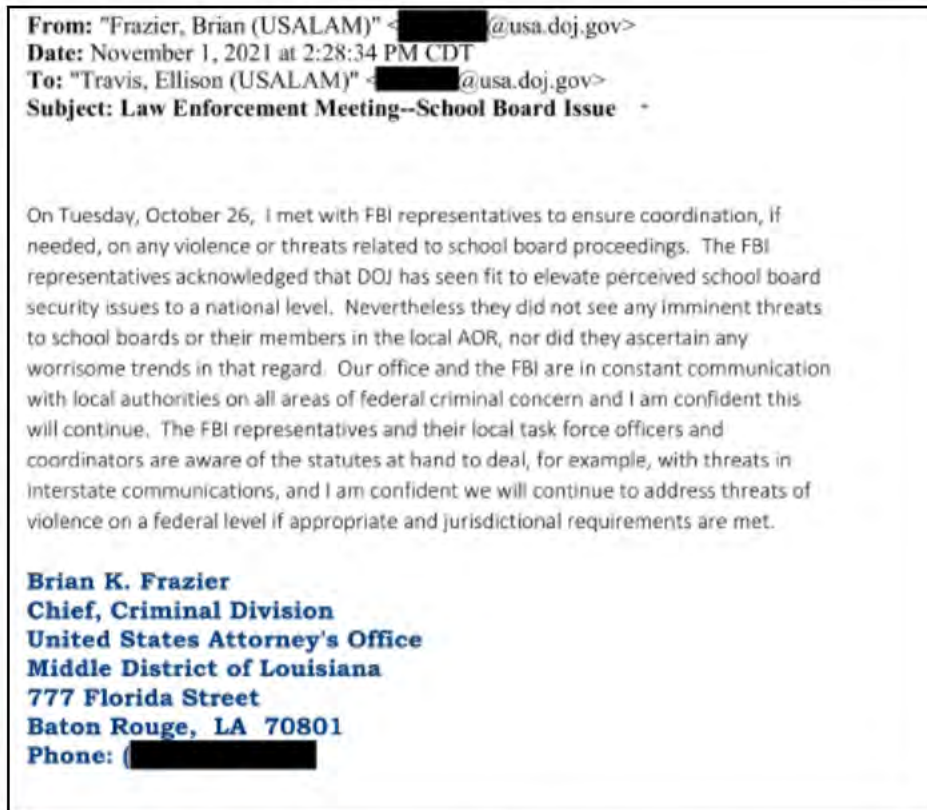
⁶¹ See DOJ-HJC-0000304; 0000305; 0000306; 0000307; 0000308.

⁶² See DOJ-HJC-0000304; 0000305; 0000306; 0000307; 0000308.

⁶³ DOJ-HJC-0000307.

⁶⁴ See, e.g., DOJ-HJC-0000016 (“During the meeting, it was established that there had not yet been a single reported incident concerning a threat of violence directed toward any school board or school board members in Arkansas.”); DOJ-HJC-0000186 (“I can report that none of the elected sheriffs or representatives from the Florida Department of Law Enforcement have encountered any threats directed toward school administrative officials, board members, teachers, or staff . . . there have been no disruptions to any school board meetings in their respective counties or

reported that threats against school officials was “described by some as a manufactured issue.”⁶⁵ In the Middle District of Louisiana, Brian Frazier, the U.S. Attorney Office’s Criminal Division Chief stated, “[t]he FBI representatives acknowledged that DOJ has seen fit to elevate perceived school board security issues to a national level. Nevertheless, they did not see any imminent threats to school boards or their members in the local [area of responsibility], nor did they ascertain any worrisome trends in that regard.”⁶⁶



Other reported threats were too vague to be independently substantiated or so innocuous as to not be of any real concern.⁶⁷ For instance, Acting U.S. Attorney for the District of South Dakota Dennis Holmes reported that “[o]fficials could remember only [one] incident” to report.⁶⁸ In that case, “an irate parent, who was upset about mask mandate[s], had to be removed from a school board meeting by the school resource officer,” but, Mr. Holmes clarified, “[n]o threats were made to board members or school staff.”⁶⁹ In another case, Acting U.S. Attorney for the

areas of responsibility.”); DOJ-HJC-0000204 (“It does not appear that threats against School Administrators, Board Members, Teachers, and Staff is a significant issue within the District of Alaska.”); DOJ-HJC-0000206 (“[S]uch threats have not been a problem here in the District of Columbia.”); DOJ-HJC-0000209 (“[T]here have been no known complaints regarding these types of issues in the Northern District of Mississippi.”).

⁶⁵ DOJ-HJC-0000210-13.

⁶⁶ DOJ-HJC-0000127.

⁶⁷ See, e.g., DOJ-HJC-0000043 (“[R]eceived from PIO--pursuant to my request to follow media coverage of both the Florida Governor's conference and the AG's letter--media report of potential threats against school board official.”)

⁶⁸ DOJ-HJC-0000133.

⁶⁹ *Id.*

Middle District of Tennessee Mary Jane Stewart reported only that “one school district has experienced heated board meetings with the public, which resulted in threats of violence and received national exposure in the news.”⁷⁰ Ms. Stewart provided no other details of the incident.

In these meetings, local law enforcement expressed concerns about other, more pressing issues. For example, the few law enforcement agencies that actually attended the meeting held by the Middle District of Alabama reported no issues with threats against school officials and instead “voiced more concern over the safety of students from other threats, such as gang and gun violence.”⁷¹

In general, participating agencies voiced more concern over the safety of students from other threats, such as gang and gun violence. ATF reported on their program to identify and remove guns from schools. The Auburn Police Chief was very interested in this program and wanted to follow up with the ATF representative on their efforts in his schools.

Similarly, U.S. Attorney Sean Costello of the Southern District of Alabama reported that one of the school board member’s houses was shot at, but the incident was unrelated to the school board member’s service on the school board and instead an “unfortunate consequence of gun violence in the city.”⁷²

On October 26, I traveled to the Northern Division of our district and met with the district attorney, the Dallas County Sheriff, and the Selma police chief to have the same discussion with them. They did not identify any significant issues, though they did note that the home of a city school board member was shot into recently. This incident does not appear to be related to service on the school board, and is believed to be merely an unfortunate consequence of the gun violence in the city.

C. The U.S. Attorney for the Northern District of Georgia deployed domestic terrorism resources against parents after finding only one alleged threat of violence within the district.

The U.S. Attorney’s Office for the Northern District of Georgia was an exception among U.S. Attorney’s Offices, doubling down on the Attorney General’s directive to use domestic terrorism resources against parents.⁷³ When that office reported back to Main Justice, the correspondence noted how Ryan Buchanan, in his former role as Assistant U.S. Attorney and Anti-terrorism Advisory Council Coordinator, had proactively contacted FBI officials in the Atlanta Field Office “to discuss the new guidance and FBI’s plans for contacting and engaging with other federal, as well as, local law enforcement partners” about the Attorney General’s directive.⁷⁴ Specifically, Mr. Buchanan reported that “the FBI’s [domestic terrorism] Squad would take the lead in acting as point-of-contact for referrals concerning school violence threats

⁷⁰ DOJ-HJC-0000075.

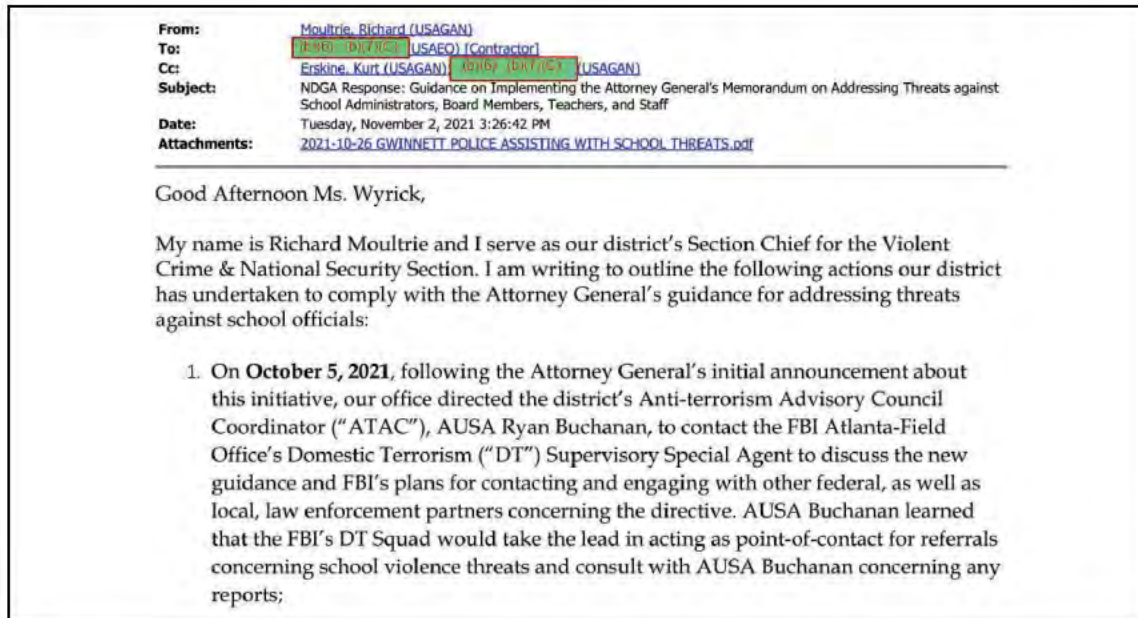
⁷¹ DOJ-HJC-0000169; 170.

⁷² DOJ-HJC-0000219.

⁷³ E-mail from Mr. Richard S. Moutrie, Jr., Chief, Violent Crime & Nat’l Sec. Section, U.S. Atty’s Off., N.D. Ga., to Exec. Off. for U.S. Attys (Nov. 2, 2021); *see also* DOJ-HJC-0000099. Note: The Department of Justice provided the cited email in a less redacted form under the *Freedom of Information Act* to an outside group that is available online.

⁷⁴ *Id.*

and consult with AUSA Buchanan concerning any reports.”⁷⁵ Just days afterward, President Biden nominated Buchanan to be the U.S. Attorney for the Northern District of Georgia.⁷⁶



Notably, in the same report to Main Justice in which the Northern District of Georgia reported that it was activating the FBI's Domestic Terrorism Squad to be the "lead" against school board-related threats, the office cited only one "threat of violence" in the district that was "circulated on social media."⁷⁷ Although the specific nature of this threat is not discussed in the document production, publicly available information suggests that the office was likely referencing a social media post, later determined to be a hoax,⁷⁸ from a student threatening to perpetrate a school shooting in revenge for being bullied.⁷⁹ This incident appears to be unrelated to the Justice Department's ostensible goal of protecting school officials from parent-related threats.

III. Local officials generally opposed federal intervention at local school board meetings.

In reports back to Main Justice, many of the U.S. Attorneys' Offices noted that their local law-enforcement partners opposed federal intervention at local school board meetings. Assistant U.S. Attorney for the District of Montana Joe Thaggard wrote that "[redacted] as well as the Cascade County Attorney, Cascade County Sheriff, and the Great Falls Chief of Police have all . . . written to [Acting U.S. Attorney Leif] Johnson advising that the local law enforcement authorities are best suited to address criminal threats against school administrators and other

⁷⁵ *Id.*

⁷⁶ See U.S. Dep't of Just., U.S. Atty's Off. N.D. of Ga., Meet the U.S. Attorney, <https://www.justice.gov/usao-ndga/meet-us-attorney> (last visited Mar. 6, 2023).

⁷⁷ DOJ-HJC-000099.

⁷⁸ See WSBTV.com News Staff, *5 teens arrested in connection to social media threats to Gwinnett schools*, WSB-TV (Oct. 28, 2021).

⁷⁹ Thom Chandler, *Gwinnett County Police are investigating threats against schools*, GA. SUN (Oct. 26, 2021).

school officials.”⁸⁰ Additionally, Mr. Thaggard noted, “Mr. Johnson has received telephone calls from a concerned citizen, a county attorney, and the press. Most, but not all, of those people have indicated a desire for the local authorities to handle any investigations and prosecutions.”⁸¹

The U.S. Attorney for the Northern District of West Virginia, William Ihlenfeld, II, reported that “[Redacted], Superintendent of the West Virginia State Police, explained his belief that most situations involving threats or harassment of school officials can be handled by state and local officials.”⁸² He continued:

[Redacted], Chief of the Martinsburg (W.Va.) Police Department, said that there have been a handful of situations in Berkeley County in which attendees at board of education meetings have been boisterous and disruptive. However, he said these incidents were able to be handled at the local level without the need for federal assistance.⁸³

Perhaps the most striking response to the Attorney General’s directive and the Justice Department’s guidance was described by Steven D. Weinhoft, the United States Attorney for the Southern District of Illinois.⁸⁴ Mr. Weinhoft explained that “this issue was very poorly received” among the participants to the meetings in that District and was “described by some as a manufactured issue.”⁸⁵ Mr. Weinhoft offered the following summary of his experiences at the meetings:

No one I spoke with in law enforcement seemed to think that there is a serious national threat directed at school boards, which gave the impression that our priorities are misapplied. Some expressed concerns that the federal government was meddling in an area where it does not belong. I heard concerns over the federal government inserting itself into issues of local politics and local choices on education. But more frequently, I heard unease over the [F]irst [A]mendment implications.⁸⁶

Due to the strong negative reactions from local law enforcement, Mr. Weinhoft “advise[d] against further national action on this matter.”⁸⁷

In addition to receiving pushback from local officials regarding federal intervention at school board meetings, U.S. Attorneys’ Offices noted a lack of enthusiasm and participation in their meetings mandated by Main Justice. For example:

⁸⁰ DOJ-HJC-0000082.

⁸¹ *Id.*

⁸² DOJ-HJC-0000007.

⁸³ *Id.*

⁸⁴ *See* DOJ-HJC-0000210.

⁸⁵ DOJ-HJC-0000212.

⁸⁶ DOJ-HJC-0000212; 0000213.

⁸⁷ DOJ-HJC-0000213.

- In her report to Main Justice, Acting U.S. Attorney Sandra J. Stewart of the Middle District of Alabama explained how the office invited 30 organizations and paired the meeting with another quarterly meeting to drive attendance, but only four organizations showed up.⁸⁸ Ms. Stewart noted how the attendance was “remarkably low” compared to the typical 75 to 80 percent attendance at the quarterly meeting.⁸⁹ Ms. Stewart explained that “some invitees decided not to participate because of the subject matter of the meeting,” referring to school board threats.⁹⁰
- U.S. Attorney Clifford D. Johnson explained that the Northern District of Illinois office invited 630 entities, but only 18 attended the meeting.⁹¹
- Acting U.S. Attorney for the Middle District of Florida Karin Hoppmann canceled her scheduled meeting “[i]n light of the paucity of responses received” and instead opted to meet individually with the five agencies that had responded from among the 50 that were invited.⁹²
- The U.S. Attorney’s Office for the District of Oregon highlighted the office’s already strained relationship between local law enforcement and local school boards due to “ideological differences.”⁹³

⁸⁸ DOJ-HJC-0000169; 0000170.

⁸⁹ DOJ-HJC-0000170.

⁹⁰ *Id.*

⁹¹ DOJ-HJC-0000221.

⁹² DOJ-HJC-0000044.

⁹³ DOJ-HJC-0000164.

CONCLUSION

Internal Executive Branch documents indicate that the Biden Administration’s use of federal law-enforcement and counterterrorism resources is an example of government weaponization against American parents. If the Justice Department performed any due diligence prior to the issuance of the Attorney General’s memorandum, it would have understood clearly and forcefully that federal intervention was unwarranted. Because that due diligence did not occur—and the Administration acted out of political motivations rather than for law-enforcement reasons—parents around the country had FBI “assessments” opened into them.⁹⁴

Ensuring the effective and even-handed use of federal law-enforcement authority should be a noncontroversial priority. Americans deserve to have confidence that the enormous power and reach of federal law enforcement will be used fairly and free of any indication of politicization. Committee Republicans have repeatedly called on Attorney General Garland to rescind his memorandum. He has declined to do so to date. The use of these resources chills protected First Amendment activity as parents rightfully fear that their passionate advocacy for their children could result in a visit from federal law enforcement.

The Committee’s and the Select Subcommittee’s work is not complete. This oversight will continue as the Justice Department and the Education Department continue to produce responsive documents. In addition, the FBI has produced only fourteen pages of documents to date in response to the Committee’s subpoena—a flagrant disregard of the serious concerns about the Bureau’s misuse of its authorities against parents.⁹⁵ There remain open questions about the development and issuance of Attorney General Garland’s memorandum—issued only five days after receipt of the NSBA’s letter to President Biden—and the coordination between the Justice Department and White House on that point. There remain open questions about how the FBI quickly operationalized the Attorney General’s directive, and whether the Bureau objected to the civil liberty concerns inherent in the Attorney General’s memorandum. The Committee has outstanding subpoenas for testimony from Chip Slaven and Viola Garcia, senior NSBA officials who signed the letter to President Biden. Until all responsive documents are produced and interviews with the necessary parties take place, the Committee and the Select Subcommittee will continue its oversight to uncover facts that will inform potential legislative reforms.

⁹⁴ See Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Just. (May 11, 2021); Letter from Christopher Dunham, Acting Assistant Director, Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Mar. 1, 2023).

⁹⁵ The FBI has provided *in camera* access to an additional 346 pages of documents, but it did not physically produce that material to the Committee. See Letter from Christopher Dunham, Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Mar. 8, 2023).



**FBI WHISTLEBLOWER TESTIMONY HIGHLIGHTS GOVERNMENT
ABUSE, MISALLOCATION OF RESOURCES, AND RETALIATION**

Interim Staff Report of
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



May 18, 2023

ATTENTION:

All Justice Department and FBI Employees

You have a right to speak with Congress

Every federal employee of the Department of Justice and FBI has an unfettered right to communicate with Congress, without the approval, consent, or awareness of the Department or the FBI. Federal law protects these disclosures.

Whistleblowers are an invaluable source for Congress in identifying, understanding, and remedying waste, fraud, abuse, and mismanagement. The Committee on the Judiciary is charged with conducting constitutional oversight of the Department of Justice and FBI.

Any Justice Department or FBI personnel with information are encouraged to contact the Republican staff of the Judiciary Committee at (202) 225-6906.



Executive Summary

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government are charged by the House of Representatives with conducting oversight of the Federal Bureau of Investigation (FBI). Whistleblower testimony from rank-and-file FBI employees is an essential part of this oversight. From accounts provided by these brave and dedicated law-enforcement officers, Congress can better understand, and ultimately address, the serious problems infesting the senior leadership ranks of the FBI. It is clear from these disclosures, and especially in wake of Special Counsel John Durham's report, that the FBI has become politically weaponized.

To date, the Committee and Select Subcommittee have received whistleblower testimony from several current and former FBI employees who chose to risk their careers to expose abuses and misconduct in the FBI. Some of these employees—Special Agents Garret O'Boyle and Stephen Friend, Supervisory Intelligence Analyst George Hill, and Staff Operations Specialist Marcus Allen—have chosen to speak on the record about their experiences.¹ The disclosures from these FBI employees highlight egregious abuse, misallocation of law-enforcement resources, and misconduct with the leadership ranks of the FBI. Among other disclosures:

- The FBI's Washington Field Office (WFO) pressured a field office in Boston, Massachusetts, to open investigations on 138 individuals who traveled to Washington, D.C., to exercise their First Amendment rights on January 6, 2021, with no specific indication that these people were involved in any way in criminal activity. The only basis for investigating these people was that they shared buses to Washington with two individuals who entered restricted areas of the Capitol that day. Rather than limiting the investigation to just the two people who entered restricted areas, the WFO instructed the Boston Field Office to open investigations on *all* 140 individuals who attended the political rally.
- In response to the WFO's pressure to open investigations into all 140 individuals, the Boston Field Office asked the WFO for more evidence, including video from the Capitol, to properly predicate the investigations. The WFO provided pictures of the two individuals inside the Capitol; however, the WFO refused to provide video evidence from the Capitol out of fear it would disclose undercover officers or confidential human sources inside the Capitol.
- Shortly after the events of January 6, 2021, Bank of America (BoA) provided the FBI with confidential customer data—voluntarily and without any legal process. BoA gave WFO a list of individuals who had made transactions in the Washington, D.C. area using a BoA product between January 5 and January 7, 2021. Individuals who had previously purchased a firearm with a BoA product were reportedly elevated to the top of the list.

¹ Because of the false and defamatory attacks that Democrats on the Committee and Select Subcommittee perpetrated against Friend, O'Boyle, and Hill, Allen initially only consented to speaking with the Committee's majority.

- FBI leadership pressured agents to reclassify cases as domestic violent extremism (DVE), and even manufactured DVE cases where they may not otherwise exist, while manipulating its case categorization system to create the perception that DVE is organically rising around the country.
- The FBI dispenses cash bonuses to local field office leadership for meeting certain arbitrary metrics and performance goals. This bonus structure creates perverse incentives for the FBI to utilize law-enforcement tools and resources where they may not be needed or appropriate in order for FBI leadership to benefit financially.

These FBI employees have come forward to blow the whistle at great personal and professional risk. Each of these whistleblowers described retaliatory conduct that they have faced after making protected disclosures about what they believed in good faith to be wrong conduct. A recurring theme is that the FBI has violated federal whistleblower protection laws and abused its security clearance review process to hamstring the brave agents who exercise their right to make protected disclosures to Congress or who dared to question agency leadership. For example:

- Special Agent O’Boyle made protected disclosures to his Supervisory Special Agent about potentially illegal activity, and the FBI transferred him to a new unit that required him to move his family across-country. When O’Boyle arrived for his first day, the FBI placed him on unpaid, indefinite suspension, effectively rendering his “family homeless” and leaving them without any personal effects—including his young children’s clothing—because these items were in FBI storage.
- Likewise, in Special Agent Friend’s case, the FBI suspended his security clearance after making protected disclosures. This suspension rendered Friend unable to fulfill his duties as a special agent—thus, the FBI suspended him indefinitely. While on suspension, the FBI refused to allow Friend to obtain outside employment, leaving his family without income.
- In Staff Operations Specialist Allen’s case, the FBI suspended his security clearance for simply performing duties of his job—conducting case-related research using open-source news articles and videos and sending his search results to his task force colleagues.

The FBI leadership’s trend toward political partisanship in recent years has disturbed the ranks of front-line FBI agents like O’Boyle, Friend, and Hill. In the words of one whistleblower, the current state of the FBI is “cancerous” as the Bureau has “let itself become enveloped in this politicization and weaponization.” This testimony supplements earlier disclosures from whistleblowers, highlighted in the Committee’s November 2022 report, in which whistleblowers described the FBI’s Washington leadership as “rotted at its core” and having a “systemic culture of unaccountability.”²

² H. COMM. ON THE JUDICIARY, FBI WHISTLEBLOWERS: WHAT THEIR DISCLOSURES INDICATE ABOUT THE POLITICIZATION OF THE FBI AND JUSTICE DEPARTMENT (Nov. 4, 2022).

The whistleblowers who have come to the Committee and Select Subcommittee expressed sincere concern about the state of the FBI, but they remained optimistic that the Bureau could improve with “tough love.” That concern and hope for the FBI’s future is fundamentally what motivates these brave whistleblowers: the belief that speaking truth to power, through the right channels, can help to restore the Bureau to what it once was. This report builds on the disclosures of these whistleblowers to assist the Committee and Select Subcommittee in understanding the problems so that Congress may consider potential legislative reforms to America’s preeminent law enforcement agency.

Table of Contents

Executive Summary	1
Table of Contents	4
I. FBI Whistleblower Disclosures Show Serious Abuses and Misallocation of Law- Enforcement Resources	5
A. The FBI’s Cash Bonus System Creates Perverse Incentives to Use Law Enforcement Tools for Leadership’s Financial Benefit and Not Legitimate Law Enforcement Needs... 5	
B. The FBI Is Reclassifying and Manufacturing Domestic Violent Extremism Cases to Advance a Political Narrative that These Cases Are on the Rise.	10
C. The FBI’s Washington Field Office Pressured the Boston Field Office to Investigate Americans Solely for Traveling to Washington, D.C. on January 6.	23
D. The FBI Gathered Conservatives’ Financial Records from Bank of America Without Any Legal Process Following January 6.	30
E. Line Agents Opposed Attorney General Garland’s Memorandum Directing Federal Law Enforcement Resources Against Parents	34
II. FBI Leaders Weaponized the Security Clearance Adjudication Process Against Whistleblowers in Retaliation for Blowing the Whistle.	42
A. Stephen Friend Was Suspended Without Pay After Questioning the FBI’s Handling of DVE Cases and Expressing Concern about January 6 Tactics.	42
A. Garret O’Boyle Was Suspended Without Pay After Moving His Young Family Across the Country	51
B. Marcus Allen Was Suspended for Merely Forwarding Open-Source News Articles to His Colleagues.	59
C. Whistleblowers Have Described How the FBI’s Politicization Has Crowded Out its Traditional Law Enforcement Function.	63
III. Committee Democrats Attacked and Defamed FBI Whistleblowers to Advance a Political Agenda.....	67
A. The Democrat Report Erroneously Claims that the FBI Whistleblowers Who Have Appeared Before the Committee Are Not <i>Real</i> Whistleblowers.	67
B. The Democrat Report Slandered the Integrity of Veteran Federal Law Enforcement Officers in the Service of Partisan Politics.	71
C. Democrats Deployed the Same Abusive Tactics to Attempt to Discredit Journalists Matt Taibbi and Michael Shellenberger.	74
Conclusion	78

I. FBI Whistleblower Disclosures Show Serious Abuses and Misallocation of Law-Enforcement Resources.

American citizens rightfully expect law enforcement agencies at every level to judiciously exercise its powerful authorities and to properly allocate resources—employees, funds, time, and other finite resources—to tackle the most-pressing issues facing the public. This is especially true regarding the law-enforcement apparatus of the United States Department of Justice.³ However, whistleblower testimony revealed to the Committee and Select Subcommittee that the FBI has abused its authority and egregiously misallocated the resources entrusted to it by American taxpayers.

Particularly, several whistleblowers have described a perverse incentive structure that promises FBI officials financial reward if they can justify opening more cases and meet other investigative metrics as set by officials in Washington. Such an incentive structure is dangerous because the FBI is a powerful law-enforcement agency engaged in the “often competitive enterprise of ferreting out crime.”⁴ It is axiomatic that the FBI should pursue its mission without fear, favor, or expectation of financial profit. The public record is replete, however, with instances of the FBI failing to meet this standard.⁵ Meanwhile, whistleblower testimony has also uncovered that the agency is engaging in the practice of ordering its agents to classify, and in a number of cases, reclassify, particular investigations as involving “domestic violent extremism” in efforts to merely support political talking points that the number of such cases is “on the rise.” These whistleblower allegations are disturbing, and this section details specific whistleblower testimony about these serious matters.

A. The FBI’s Cash Bonus System Creates Perverse Incentives to Use Law Enforcement Tools for Leadership’s Financial Benefit and Not Legitimate Law Enforcement Needs.

Whistleblowers have described a “disconcerting aspect of the FBI”—that is, Special Agents-in-Charge (SACs) around the country are eligible to “get a monetary bonus at the end of the year if they meet metrics.”⁶ Indeed, according to testimony, SACs often keep computer spreadsheets that list performance metrics that the FBI then relies upon to dispense bonuses to these SACs.⁷ These metrics appear to be arbitrarily assigned, and in some cases self-determined by the SAC. This reward structure creates perverse incentives in which law-enforcement tools and resources are expended for the financial enrichment of FBI leadership instead of a legitimate law-enforcement basis.

³ *Principles of Federal Prosecution*, U.S. DEPT. OF JUSTICE, 6 Fed. Sent. R. 317, 317 (1994) (Federal law enforcement’s “priorities are designed to focus federal law enforcement efforts on those matters within federal jurisdiction that are *most deserving of federal attention* and are *most likely to be handled effectively at the federal level.*” (emphasis added)).

⁴ *Johnson v. United States*, 333 U.S. 10, 14 (1948).

⁵ See generally H. COMM. ON THE JUDICIARY, FBI WHISTLEBLOWERS: WHAT THEIR DISCLOSURES INDICATE ABOUT THE POLITICIZATION OF THE FBI AND JUSTICE DEPARTMENT [hereinafter “FBI WHISTLEBLOWER REPORT”].

⁶ Transcribed Interview of Mr. Garret O’Boyle at 120 (Feb. 10, 2023) (hereinafter “O’Boyle Interview”).

⁷ *Id.*

Special Agent Garret O'Boyle explained to the Committee and Select Subcommittee that he had concerns about the potential for abuse in this incentive structure, particularly as they apply to surveillance techniques. He testified:

Q. And are you aware of these self-created performance metrics?

A. So to some degree, I am. . . . And I think a large driving factor in the FBI is to meet those metrics. And I think that raises grave constitutional concerns to be saying to law enforcement officers, you have to go and do X, Y, and Z so the boss gets his bonus. Nobody comes out and says it that way, but when you get the spreadsheet where—or the SAC Excel spreadsheet is red in these categories, we've got to fix it, we've got to do this and that to get it back up to green and then to gold so he gets his bonus. Nobody is saying it that way, but that certainly is what is implied.

Q. And what are the metrics?

A. There's a wide range of them. . . . [O]ne that I do have personal experience with is . . . Title III wiretaps, or FISAs, or other sophisticated—sophisticated techniques. That's what they're called. . . . [A]t the beginning of the year the SAC's metric might be, get three Title IIIs. And it's like, how do you know you're going to get three? And what if you don't get three? Well, then you're not marked gold in that category. So I think that that leads to a pervasive culture of not letting the case dictate where the investigation goes, but it's the manager or the agent pushing for a certain avenue of where a case goes.⁸

Indeed, O'Boyle recalled a specific instance in his career in which he and a co-case agent were not-so-subtly impressed into the profit-seeking service of their then-SAC. He testified:

And me and my co-case agent, a [Task Force Officer] who had been there for years, we had a meeting with my boss. It was Sonia Garcia at the time. And we were talking about this Title III affidavit that I'm writing—or that me and [Task Force Officer] are writing. And we wrap up the meeting, and she says, you guys, I really need this Title III. And it struck me as odd. So we walked out of the office. And I was like, [Task Force Officer], can we go to the conference room? And so we went in there and talked. And I was like, what did she mean, like, I really need this Title III? And he started laughing. And he's like, you'll see. . . . And he told me, like, there are metrics

⁸ *Id.* at 121.

that need to be met, and then your boss or their boss can write to that, oh, while I was the supervisory resident or supervisory special agent, I had a Title III on this case. And they can write to that on what's called an FD-954, which is . . . your internal resume that you have to submit when you want to get promoted. And it's like, oh, she really needed that because it helps her get promoted. And then it also helps the SAC because then he's got a Title III for his Excel spreadsheet. So he's one Title III closer to being gold in that way and then getting his bonus. And I would say, like, by and large—I mean, a Title III, you listen to people's phone calls. . . . [T]hat's an extreme measure to take. And now with the FBI saying, get this arbitrary number of Title IIIs because then the big boss gets his bonus? Like, that's not how law enforcement should be working.⁹

O'Boyle testified that although that is “not how law enforcement should be working,” it was commonly understood in the FBI that special agents did well to meet these metrics so that their bosses could receive a financial bonus.¹⁰ The bonus structure was not only “common knowledge,” but a source of humor and speculation within the Bureau.¹¹ George Hill, a former FBI Supervisory Intelligence Analyst, testified to the Committee and Select Subcommittee that SACs would joke about the bonus while FBI personnel would speculate about how much money the SAC would receive as a bonus.¹² But as O'Boyle made clear, there is nothing funny about an incentive structure that “leads to a pervasive culture of not letting the case dictate where the investigation goes,” but allowing arbitrary metrics to guide the allocation of law-enforcement assets and resources.¹³

The pressure felt by field agents to hit metrics for their SACs even affected real-world law enforcement operations in the field. Special Agent Stephen Friend testified that he once was asked to “space out” arrests on different days so that the arrests would count as nine separate data points. He explained:

- Q. And as a special agent, when you were asked to either make an arrest or push an arrest off for a couple months, would you describe it as an environment of pressure to hit the metrics?
- A. Yes. I was told on one instance where there were nine subjects on a case that if I arrested them all in the same day it would count as one disruption statistic. But if I arrested one each day for nine straight days, it would count as nine statistics, so I should space out those arrests.

⁹ *Id.* at 121-22.

¹⁰ *Id.* at 124.

¹¹ Transcribed Interview of Mr. George Hill at 56 (Feb. 7, 2023) (hereinafter “Hill Interview”).

¹² *Id.*

¹³ O'Boyle Interview at 121.

Q. So would you say that the pressure to hit the metrics, did it cause you to make changes to how you were doing your law enforcement duties?

A. Yes.¹⁴

It is concerning—to the say the least—that these perverse financial incentives affect the way in which FBI agents undertake their law enforcement duties. However, testimony from another whistleblower, Staff Operations Specialist Marcus Allen, also highlighted the disturbing practical effects of these incentives, which leads to unethical and inaccurate FBI documentation. Specifically, Allen explained how the FBI management will demand that employees manipulate time-keeping records to create the perception that a particular office is working more than it is on a particular matter. As he explained:

A. So I've observed in the workplace, like, on more than one year where it's like, someone from management will come down and they'll say, "Everybody, TURK¹⁵ this." And so all the investigators will be like, no matter what case it is, it's like, "Well, I guess we're TURKING this now," and they'll just literally all TURK that number, like, regardless of what they may have really worked on. It seems to me they're trying to meet whatever the number that's desired is, you know, and if they're short of that, then it's like, "Everybody, from this point forward, TURK this"¹⁶

O'Boyle's testimony further supported Allen's assertion about manipulating time-keeping records to hit certain metrics, particularly in the context of domestic terrorism cases. In his transcribed interview, O'Boyle explained:

Q. Given your experience with domestic terrorism cases, I want to ask you about some information that the committee has learned regarding domestic terrorism cases and domestic violent extremism. So we have learned that the Biden administration's narrative about the FBI's work on domestic violent extremism — abbreviated as DVE — cases may be misleading. We have received accusations that FBI agents are bolstering the number of cases of DVEs to satisfy their superiors. For example, one whistleblower claimed that, because agents are not finding enough DVE cases, they are

¹⁴ Transcribed Interview of Mr. Stephen Friend at 126 (Feb. 15, 2023) (hereinafter "Friend Interview").

¹⁵ "The FBI uses the Time Utilization and Recordkeeping (TURK) system to record time spent by most FBI field office personnel on various types of investigative matters." *The Internal Effects of the Federal Bureau of Investigation's Reprioritization, Chapter 3: Resource Utilization and Casework*, OFFICE OF THE INSPECTOR GEN. (Sept. 2004), <https://oig.justice.gov/reports/FBI/a0439/ch3.htm#:~:text=The%20FBI%20uses%20the%20Time,various%20types%20of%20investigative%20matters.>

¹⁶ Transcribed Interview of Mr. Marcus Allen at 63 (May 8, 2023) (hereinafter "Allen Interview").

encouraged and incentivized to reclassify cases as DVE cases, even though there's minimal circumstantial evidence to support the reclassification. Do you have any information regarding the reclassification of cases as DVEs?

- A. I would have to think about that further because I don't remember exactly where I heard this from. But in the FBI, we classify our cases—we call it a TURK code. TURK is, like, time, utilization, and record keeping. So there's, like, an alphanumeric code for every type of case, every type of investigation you work . . . I can't recall exactly, but I learned at some point that FBI agents were being directed to reclassify 170—I think it was 176 cases, so that would be domestic cooperation with police—to reclassify any of those into some type of domestic terrorism case. But, again, I don't remember if I heard that secondhand or if that was something I learned at work. I guess along that same line, as a DT agent, I encountered similar stat padding or case bolstering, in that I had a case—and I'll try not to get into too many details because I think it might still be open, but I don't know. It's a case I was trying to wrap up before my transfer. And truth be told, it was one case. But the FBI had me open up four different cases because they had me open a case for every individual that I had an articulable, factual basis that there may have been potential federal law being violated. And when I first got these cases, I'm like because I initially—they were transferred to me from another agent. And I think it was, like, two at the time. And I asked my boss, I was like, why do I have—these are the same. Like, everything I wrote, . . . everything I did, I started putting into all four cases because they were really just one case. Where, like, on a criminal case, say you were working, like, a gang, which this case was, I guess, like, a militia, if you're working, like, a gang, you have a case open on the gang, and you have a subfile for each person in it. Like, John Doe one, two, and three, they would all have their own subfile. Where in my case, John Doe one, two, three, and four all had their own separate case because then the FBI can—from my perspective—the FBI can come back to Congress and say, look at all the domestic terrorism we've investigated. Where, really, I was working one case. But the FBI can then say, well, he actually had four, and so we need you to give us more money because look at how big of a threat all this domestic terrorism is. So that's just my personal experience with that.

- Q. So it was the usual practice that if there were multiple individuals involved with one case, you may open a subfile for each individual? Is that correct?
- A. If you're working traditional criminal matters, yes. But I believe it's policy on the CTD side to open up all these separate cases, when in reality then that's just—they're just obscuring the truth and the facts. Like, all my guys that I was working on were related. They should have just been in one case. But they weren't because—
- Q. Who gave you the directions, Mr. O'Boyle, to open four cases in that matter rather than categorize all that conduct in one case?
- A. So, sir, I don't know if anybody even gave me a specific direction. It was more like, this is the policy¹⁷

American citizens deserve to know that their tax dollars are being spent on necessary investigations pervasive to their local communities. As this whistleblower testimony demonstrates, the FBI is rife with unnecessary and potentially unethical enticements that direct agents to not only lie about the types of cases on which they work but reward such FBI leadership for such deception.

B. The FBI Is Reclassifying and Manufacturing Domestic Violent Extremism Cases to Advance a Political Narrative that These Cases Are on the Rise.

Whistleblowers assert that the FBI pressured agents to reclassify cases as domestic violent extremism (DVE), and even manufactured DVE cases where they may not otherwise exist, while manipulating its case categorization system to feign a national problem. At a time when the Biden Administration maintains that DVE is the “greatest threat” facing the United States,¹⁸ the FBI appears to be complicit in artificially supporting the Administration's political narrative.

The FBI defines a DVE as “an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals wholly or in part through unlawful acts of force or violence.”¹⁹ According to the Biden Administration, investigations into DVEs have increased “significantly” in recent years.²⁰ In August 2022, FBI Director Wray testified

¹⁷ O'Boyle Interview at 91-93.

¹⁸ *The Way Forward on Homeland Security: Hearing Before the H. Comm. on Homeland Sec.*, 117th Cong. (2021) (statement of Hon. Alejandro Mayorkas, Sec'y, U.S. Dep't of Homeland Sec.).

¹⁹ FED. BUREAU OF INVESTIGATION AND DEP'T OF HOMELAND SEC., STRATEGIC INTELLIGENCE ASSESSMENT ON DATA AND DOMESTIC TERRORISM AT 2, NOTE 3 (MAY 2021) [hereinafter “FBI STRATEGIC INTELLIGENCE ASSESSMENT”].

²⁰ *Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Hon. Christopher A. Wray, Dir., Fed.

before the Senate Judiciary Committee that “[t]he number of FBI investigations of suspected DVEs has more than doubled since the spring of 2020.”²¹

According to Hill, however, the pressure on FBI agents to meet metrics also contributed to the manipulation of DVE data. Hill explained how then-Washington Field Office ASAC Timothy Thibault and the FBI’s former Assistant Director of the Counterterrorism Division Jill Sanborn pressured agents to move cases into the DVE category to hit self-created performance metrics.²² Indeed, according to Hill, Director Wray and Assistant Director Sanborn set a “tone” to encourage agents “to identify opportunities where cases could be tagged as domestic terrorism threats.”²³ In a transcribed interview with the Committee, however, Sanborn denied this environment of pressure, testifying:

Q. And during your time at the FBI, are you aware of any instances where an agent has been told to reclassify a case?

A. Not that I can recall, no.

Q. Any instance where an FBI agent was pressured to reclassify a case?

A. Not that I can recall.

Q. During your time at the FBI, do you know if there is an—was an initiative to prioritize DVE cases?

A. . . . But there is a process for prioritizing threats, and I think it’s a yearly if not biyearly process, very mindful process, that takes into account a lot of different things. And it’s very intelligence based. It’s something that I believe is done well on the heels of the lessons we learned from 9/11 to not base prioritization just on volume of cases. So when I came in that’s how priorities got set in field offices, was the squad that had the most cases. And so I think this process that’s rooted in intelligence then gives you how the cases should be ranked—I mean, how the cases—how the threats should be ranked. And going through that process definitely during my time as [Assistant Director], and I believe I saw some of this as [Executive Assistant Director], made the DVE threat

Bureau of Investigation); Hon. Merrick B. Garland, Atty Gen., Domestic Terrorism Policy Address at U.S. Dep’t of Justice (June 15, 2021).

²¹ *Oversight of the Federal Bureau of Investigation, Hearing Before S. Comm. on the Judiciary*, 117th Cong. at 2 (2022) (statement of Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation).

²² Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation (July 27, 2022); *see also* Letter from Reps. Jim Jordan & Mike Johnson, H. Comm. on the Judiciary, to Ms. Jill Sanborn, Senior Dir. Of Geopolitical Strategy & Risk Analysis, Roku Inc. (Aug. 10, 2022).

²³ Hill Interview at 18.

fall more elevated on that continuum than it maybe would've been 5 years ago.²⁴

Still, Hill recalled that ASAC Thibault's "level of excitement" at the prospect of targeting a "growing segment of our population" as domestic terrorists was, in his words, near "hysterical."²⁵

According to whistleblower information, the FBI has manipulated the manner in which it categorized January 6-related investigations to create a misleading narrative that domestic terrorism is organically surging around the country. Ordinarily, the FBI characterizes and labels cases according to the originating field office, with leads "cut" to other field offices for specific assistance in that geographic location.²⁶ With January 6 cases, however, the FBI has not followed its ordinary procedure, which would have resulted in the WFO leading the investigation and categorizing the investigations as WFO cases.²⁷ In particular, Friend disclosed that:

Q. So, per policy in the DIOG, or the Domestic Investigations and Operations Guide, is it correct that FBI agents ordinarily label full investigations case files according to the originating field office?

A. Yes.²⁸

Q. So, if the field office is cut a lead or sent a lead, is that field office then referred to as the lead office under the DIOG?

A. Yes.

Q. So, for example, if a Federal crime occurs in Texas, would the originating field office be in Texas?

A. Yes.²⁹

²⁴ Transcribed Interview of Ms. Jill Sanborn at 25-6 (Feb. 1, 2023) (hereinafter "Sanborn Interview").

²⁵ *Id.* at 34-37, 99. Notably, Thibault resigned from the FBI in disgrace after credible allegations surfaced that he attempted "to thwart a criminal investigation into Hunter Biden." Caroline Downey, *Top FBI Agent Resigns after Allegedly Thwarting Hunter Biden Investigation: Report*, NAT'L REV. (Aug. 30, 2022). He "was escorted out of the Washington field office by at least two 'headquarters-looking types.'" *Id.*

²⁶ Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on the Judiciary, to Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation (Sept. 19, 2022).

²⁷ FBI WHISTLEBLOWER REPORT at 10.

²⁸ Friend Interview at 12.

²⁹ *Id.*

Q. And for full investigations opened into the events that occurred at the Capitol on January 6, 2021, would the originating field office for those investigations be the Washington Field Office?

A. Yes.

Q. And if investigative actions outside of D.C. are required, would or should the WFO case agent then cut a lead to the appropriate FBI field offices?

A. Yes.

Q. And, following January 6th, to your knowledge, did the FBI set up any kind of task force within headquarters or the WFO to work on January 6th investigations?

A. Yes.

Q. Can you describe that task force? Was it in headquarters or the WFO?

A. The WFO. And it was staffed by employees who worked in WFO as well as TDY, temporary duty agents, from around the Bureau.

Q. Do you know who was in charge of the task force?

A. I don't.

Q. Okay. And since the events occurred in Washington, D.C., it is natural that the WFO would handle the investigations?

A. Yes.

Q. During your tenure at the Daytona Beach Resident Agency, were you ever assigned January 6th cases?

A. Yes.

Q. And during your tenure at the FBI, did the FBI follow this regular procedure with regards to January 6th investigations for labeling cases?

A. No.

- Q. How did the handling of January 6th investigations deviate from the regular procedure?
- A. We received leads from headquarters, from the task force working out of Washington, D.C., with directives to carry out certain investigative actions, in assumption that we were going to be opening cases from our office as the originating office. Then we would perform tasks and send that information back to Washington, D.C., for their approval or for their request for more work to be done and then ultimately for their decision on how to pursue a case, whether or not to prosecute it.³⁰

Friend also explained that although the field offices are carrying out the directives from WFO, the agents in WFO are actually determining and approving the investigative tactics. He explained this manner of running investigations was a deviation from standard practice. He testified:

- Q. . . . So, instead of following the regular case file management procedure, the WFO is directing other field offices to open full investigations, and then the WFO is performing and approving the investigative work. Is that an accurate characterization?
- A. Yes.
- Q. So, if January 6th cases are handled in this manner, does it appear on paper that local field offices instead of the WFO are the originating field offices?
- A. Yes.
- Q. And that deviates from the standard practice?
- A. Yes.
- Q. And, to your knowledge, is this only happening with January 6th cases?
- A. Yes.
- Q. How were your assigned January 6th cases handled? Were they handled in this similar way, where the WFO would tell you what to do and open cases?

³⁰ *Id.* at 12-13.

A. Yes.

Q. Were you told or pressured by the WFO to open full investigations?

A. We were told to open full investigations and that they would populate them with paperwork or case file work that was pertinent to that particular case.

Q. So, if you completed investigative steps, would you have to report back to the WFO on what you had done?

A. Yes.

Q. And would they tell you if you needed to do more investigating?

A. Yes.

Q. And what if you didn't believe that there was enough of a predicate to continue to investigate? Did you still have to investigate?

A. I was told that we could push back as much as we wanted but they would continue to send us additional requests to perform more work.

Q. And "they" meaning agents at the WFO?

A. Yes.

Q. Were you ever provided any insight as to why January 6th cases were handled in this manner?

A. Yes.

Q. And what was that insight that you received?

A. I was told that there was a coordination call very early on after January 6th, during which there was representatives from all around the country, and the question was posed as to why this protocol was being followed, and that they were told that it was to get buy in from the field.³¹

³¹ *Id.* at 15-16.

- Q. Do you know when this coordination call happened?
- A. I was told it was in the immediate aftermath, so I was under the belief that it was probably within a week or two.
- Q. Did you get an understanding of who was on this coordination call?
- A. Yes. I was told that it was people from all around the Bureau who were going to be charged with primarily investigating the cases.
- Q. Okay. So it included WFO people and agents from across the country in different field offices?
- A. Yes.
- Q. And do you know what the substance — what was discussed on that call?
- A. That's the only fact that I know that was discussed on that particular call. But in my inquiries, I was told that these coordination calls were going on quite frequently in the aftermath of January 6th.³²

Friend explained that the FBI's manner of handling January 6-related investigations in a way that deviated from standard practice created a false impression with respect to the threat of DVE nationwide. He testified:

- Q. And, to your knowledge, does managing or labeling case files in this way create a false and misleading narrative that domestic violent extremism is increasing around the country?
- A. Yes.
- Q. Does this, in turn, give the impression that the threat of DVE is present in jurisdictions around the Nation even though the cases all stem from the same related investigation?
- A. Yes.³³

³² *Id.* at 16-17.

³³ *Id.* at 17.

Worse yet, the FBI prioritized DVE cases over other criminal investigations such as those involving child exploitation. As Friend testified:

- Q. And you said that you became a member of the Joint Terrorism Task Force at the Daytona Beach Resident Agency in October of 2021. Is that correct?
- A. Yes.
- Q. Is it correct to say that you were reassigned from investigating child exploitation cases to work on domestic terrorism cases?
- A. Yes.
- Q. Were those cases specifically related to January 6th?
- A. Yes.
- Q. And how was that communicated to you?
- A. There was a phone call from the assistant special agent in charge to my supervisor at the time, and he said that the new fiscal year approaching, that they were going to be resourcing manpower differently and that I was going to be reassigned from my current assignment to the JTTF. My supervisor asked about the investigations that I was working, and the ASAC said that those are to be considered a local issue going forward.³⁴

From Friend's testimony it is clear that although the local field offices appear to be running the cases on paper, the WFO was directing the field office special agents to "open the case" in their geographic area.³⁵ Meanwhile, the WFO was performing and approving "all of the investigative work and paperwork for the casefile."³⁶ Friend described how "there are active criminal investigations of January 6th subjects in which I am listed as the 'Case Agent,' but have not done any investigative work" and his supervisor "has not approved any paperwork within" those investigative files.³⁷ This deviation from established practice has an obvious motive: it allows the FBI to support the Biden Administration's narrative that domestic terrorism is on the rise by claiming that "[t]he FBI is a field-based law enforcement organization, and the vast

³⁴ *Id.* at 8-9.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

majority of our investigations should continue to be worked by our field offices,” while, in reality, running the investigation from Washington.³⁸

By deviating from standard practice, the FBI has given itself a pretext to claim the DVE threat is rising nationwide.³⁹ Friend disclosed:

The manipulative casefile practice creates false and misleading crime statistics. Instead of hundreds of investigations stemming from a single, black swan incident at the Capitol, FBI and DOJ officials point to significant increases in domestic violent extremism and terrorism around the United States.⁴⁰

In other words, the FBI’s case categorization creates the illusion that FBI field offices around the country are investigating a groundswell of domestic terrorism cases, giving the impression that the threat of DVE is present in jurisdictions across the nation. The reality is simpler: the cases all stem from the same related investigation concerning the actions at the Capitol on January 6. This scheme permits the FBI leadership to misleadingly point to “significant” increases in DVE threats nationwide.⁴¹

According to O’Boyle, the FBI classified “every single January 6th case . . . as a domestic terrorism case.”⁴² And yet hundreds of those cases were resolved as “petty crimes,” such as “trespassing and disorderly conduct.”⁴³ O’Boyle testified:

[T]he FBI holds [the January 6th investigation] up as the biggest investigation that it’s ever had. So if you’re categorizing all of them as domestic terrorism cases, yeah, they would double. But I think it’s kind of a misnomer to say that because the vast majority of those, at least in my experience, we would get leads related to those, and we’d work the leads and then send back to [WFO], who was running—kind of running everything, like, hey, this lead, you know, it’s unfounded or it is founded.⁴⁴

³⁸ Letter from Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation, to Hon. Michael Horowitz, Inspector Gen., U.S. Dep’t of Justice (Dec. 6, 2019).

³⁹ Hill Interview at 23 (noting that FBI leaders “need to create the perception that these cases are all over the country and in numbers that the [Threat Review and Prioritization process] needs to reflect some sort of mitigation plan attached to it”).

⁴⁰ FBI WHISTLEBLOWER REPORT at 10-11.

⁴¹ See, e.g., *Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation); see also *Oversight of the Federal Bureau of Investigation: Hearing Before H. Comm. on the Judiciary*, 117th Cong. (2021) (statement of Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation); Hon. Merrick B. Garland, Atty Gen., Domestic Terrorism Policy Address at U.S. Dep’t of Justice (June 15, 2021). (“The number of open FBI domestic terrorism investigations this year has increased significantly.”).

⁴² O’Boyle Interview at 124-25.

⁴³ Alan Feuer, *Prosecutors Move Quickly on Jan. 6 Cases, but One Big Question Remains*, N.Y. TIMES (Jan. 5, 2022).

⁴⁴ O’Boyle Interview at 104.

O'Boyle further recalled one example in which he was pressured to pursue an unreliable and uncorroborated tip related to January 6 that normally would not have been pursued. He explained:

- Q. Do you know, did the WFO pressure other field offices to keep January 6th cases open or open cases?
- A. I would say they pressured us to open cases to some degree. One example that I have personally But I received a lead about someone based on an anonymous tip, and in law enforcement anonymous tips don't hold very much weight, especially without evidence that you can corroborate pretty easily. I wasn't able to corroborate anything they said, even after speaking with the person they alleged potential criminal behavior of. While I'm trying to figure all that out, I get another lead from the same agent who sent me that lead. And they essentially tried to get me to violate policy or law.⁴⁵

And after talking to her, my mind was blown that she was still trying to get me to do some legal process on the guy that I got the anonymous tip on. Because there was no rational explanation that anybody could come up with, especially with the additional information I had found, that would have permitted me to do legal process even if I wanted to. And so I ended up writing that all up and denying it. But that was a personal example for me where it was like, okay, this has gone way off the rails here.⁴⁶

Similarly, Friend testified:

- Q. . . . I want to go back to the treatment of these January 6 cases. You talked about information packets that the Washington Field Office would send out around the country. Could you give me a sense of the categories of evidence that would be included in those packets?
- A. It would have information with photographs of surveillance footage tied to social media, facial recognition, to ensure that it matched with the individual's, say, their Facebook profile. It would be GPS information for the person's phone. And that information was provided by the phone providers to the FBI. And they were able to geolocate geo fence if that

⁴⁵ *Id.* at 102-03.

⁴⁶ *Id.*

phone was in the area. It included tips that came in through the public at large. In the aftermath of January 6th, there was a large push to get that information, so many, many people made phone calls or provided electronic communications to turn in who they thought were subjects. It could be anything from—confidential human sources might be able to provide some information. So that would all be assembled into a packet and disseminated to the field to pursue investigative—logical investigative action.⁴⁷

Q. And just so I understand this, in these packets, you observed information regarding confidential human sources?

A. Yes.

Q. Can you explain what happened when you went and spoke to that individual who there was no facial recognition indicating they were in the Capitol?

A. Yes. It was an anonymous tip from Rhode Island. Facial recognition was negative. The phone was negative. At that point, I said, it's probably it's not worth resourcing because we can't pursue an investigation, even if the person confesses to being there, because we don't have a complainant on this case. And I was told that, yeah, we got those all the time, especially right after January 6, and you have to go talk to them; otherwise, Washington is going to keep kicking it back to us. So I went and talked to him and knocked on his door, identified myself, and asked him if he was at the Capitol, and he told me that he wasn't because that was the day of his son's funeral. So I gave him my business card and I left.⁴⁸

Likewise, with respect to manipulating the data on the January 6 investigation, Friend testified:

A. By opening a separate case for each individual as opposed to one case with however many subjects are involved, they've turned one case into a thousand cases. And by spreading them to the field they've given the impression that those domestic terror cases are around the country when, in fact, the subjects, if they committed any sort of violation or

⁴⁷ Friend Interview at 107-08.

⁴⁸ *Id.* at 108-09.

infraction, they committed a crime at the Capitol on one day as opposed to being a cell that's operating in El Paso or Cleveland.⁴⁹

Q. And, to your knowledge, does managing or labeling case files in this way create a false and misleading narrative that domestic violent extremism is increasing around the country?

A. Yes.

Q. Does this, in turn, give the impression that the threat of DVE is present in jurisdictions around the Nation even though the cases all stem from the same related investigation?

A. Yes.⁵⁰

Q. Do you agree that manipulating the case file system in this way allows the FBI to support Director Wray's December 2019 assertion that the FBI is a, quote, "field-based law enforcement organization," end quote?

A. Yes.⁵¹

By manipulating the classification of January 6 investigations, according to Hill, Director Wray and FBI leadership "encourage[d] the use of DVE tags" and "create[d] the perception that [DVE] cases are [on the rise] all over the country. . . ." ⁵² O'Boyle put a finer point on the FBI's manipulation of case files. When asked about the FBI's deviation from practice related to the January 6 investigation, he testified:

Q. And is this how cases are normally handled?

A. No. I've never seen that before.

Q. Why do you think the FBI is handling the cases in this manner given your experience?

A. I think it goes back to making that threat appear larger than

⁴⁹ *Id.* at 131.

⁵⁰ *Id.* at 17.

⁵¹ *Id.* at 18.

⁵² Hill Interview at 23, 36.

it actually is, and then WFO kind of . . . being at the head of everything to try to ensure, as best they can, how the direction of a particular case will go.

- Q. And so if the main event occurred in Washington, D.C., and then now there's cases opening across the country, would it then look like there are domestic terrorism cases popping up across the country if this is how the FBI is handling?
- A. Yes, that is how it would look.⁵³

The nature of this manipulation has not been lost on the rank and file of the FBI. As Friend testified:

- Q. [W]hy did it concern you that the FBI was padding the stats on the [January 6] cases with this practice you've testified to of keeping matters open without any real law enforcement utility?
- A. For two reasons. I was worried that we were violating our rules and individuals' rights, and that could contribute to us essentially losing righteous prosecution against an individual, as well as being violative of their civil liberties. And, secondly, I believe . . . that the FBI is supposed to exist for maintaining law and order, and if we are creating the illusion that domestic terrorism is on the rise around the country, it's going to make people nervous, and it's going to contribute to a very toxic environment where we might be shifting the Overton window to the extent that half the country might be cut out of a constructive dialogue.⁵⁴

This testimony from these FBI whistleblowers is concerning. The FBI is pressuring agents to classify cases as DVE matters and manipulating data to advance a political narrative that domestic extremism is on the rise—and that everyday Americans in neighborhoods around the country are part of that growing threat. The FBI has diverted resources from investigating violent criminal enterprises, major drug traffickers, and international sexual predators and human traffickers to prioritize “domestic extremists”—roughly translated, according to the President's own words, as the half of the country that does not support his political views and policies.⁵⁵ This misallocation of law-enforcement priorities should concern all Americans.

⁵³ O'Boyle Interview at 181.

⁵⁴ Friend Interview at 47-48.

⁵⁵ Remarks, The White House, Remarks by President Biden on the Continued Battle for the Soul of the Nation (Sept. 1, 2022).

C. The FBI's Washington Field Office Pressured the Boston Field Office to Investigate Americans Solely for Traveling to Washington, D.C. on January 6.

The Committee has obtained information suggesting the FBI's push to advance an artificial narrative that domestic terrorism is on the rise is infringing on Americans' constitutional liberties. From whistleblower disclosures to publicly available information, it appears that with the newfound emphasis on fighting domestic violent extremism, the FBI sees signs of domestic terrorism wherever it looks.

Retired Supervisory Intelligence Analyst Hill provided one insightful example. According to Hill, two individuals organized a bus trip from Massachusetts to Washington, D.C., to attend a political rally in support of President Trump on January 6, 2021.⁵⁶ The group included a total of 140 people on two buses.⁵⁷ The two organizers of the trip entered restricted areas in the United States Capitol that day and, as a result, the FBI's Boston Field Office (BFO) opened cases against them for potentially violating federal law.⁵⁸ Rather than limiting the investigation to just the two people who entered restricted areas of the Capitol, however, the WFO instructed the BFO to open cases on *all* 140 individuals who attended the political rally.⁵⁹ As Hill testified to the Committee:

WFO wanted us to open up a case on each and every one of those 140 individuals, to which the [Supervisory Special Agent] in Boston said, "They were going to a political rally, which is First Amendment-protected activity. No, we're not starting cases on these people." To which they said, "Well, we're going to call your SAC." And the SSA said, "Go right ahead." . . . [T]o his credit, [the SSA] said, no, we're not opening up cases on people who went to a rally⁶⁰

Hill further recounted that when the Boston office asked the WFO for video evidence that the other 138 individuals were in the Capitol, the WFO informed the Boston agents that it could not share the video out of fear it would disclose the identities of undercover officers in the Capitol.⁶¹ Hill elaborated:

And I forgot a key part. The SSA for CT2 said, "Happy to do it. Show us where they were inside the Capitol, and we'll look into it." To which WFO said, "We can't show you those videos unless you can tell us the exact time and place those individuals were inside the Capitol."

To which the SSA responded back – and I was privy to these

⁵⁶ Hill Interview at 82.

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Id.* at 82-83.

conversations firsthand – “Why can’t you show us – why can’t you just send us the – give us access to the 11,000 hours of video that’s available?” “Because there may be” – may be – “UCs,” undercover officers, “or CHSes,” confidential human sources, “on those videos whose identity we need to protect.”⁶²

In a subsequent exchange with Chairman Jordan, Hill detailed the sequence of events. He testified:

Q. So Washington Field Office contacts you and says, we want to open up investigations on the two people who organized these two buses –

A. And we did.

Q. – who were inside the Capitol.

A. Yes.

Q. And you said, fine, because they were inside the Capitol.

A. Because they were able to show us pictures of them inside the Capitol.

Q. Definitive proof they were inside the Capitol.

A. Yes.

Q. So you open up investigations on them. And then Washington Field Office asked you, we want you to look at everyone who was on the bus who came to the rally?

A. Correct.

Q. You said, show us why –

A. Show us proof they were in the Capitol.

Q. – and you’d be happy to do it.

A. Yes.

Q. And then they said, we can’t show you proof.

A. Correct.

⁶² *Id.* at 82.

- Q. And you asked, “Why can’t you show us proof?” Is that correct? “Why can’t you show us proof?”
- A. Either show us pictures or give us access to the videos, the 11,000 hours of video.
- Q. Back up a second. The two who you opened cases up on the initial two –
- A. Those came through with pictures.
- Q. So they had pictures of them –
- A. Yeah.
- Q. – inside the Capitol.
- A. In the Capitol, yeah.
- Q. Got it.
- A. It was clear cut violation of the law.
- Q. Got it. The other 140, they had no evidence, no proof that they had actually violated the law and were inside the Capitol.
- A. They may have, but they refused to share it with us.
- Q. Refused to share it with you. And then you said, we're not going to open up an investigation –
- A. Right, because all we had was they –
- Q. Before you said that, you said, show us the proof, show us the video or pictures, whatever you have. And they said, we can’t.
- A. Correct.
- Q. And the reason they gave you was?
- A. There may be UCs, undercovers, or CHSes, confidential human sources, and we need to protect their identities.⁶³

⁶³ *Id.* at 83-84.

Hill's supervisor, Special Agent-in-Charge Joseph Bonavolonta, confirmed Hill's account about WFO asking Boston to open investigations on all 140 individuals. In a transcribed interview with the Committee, Bonavolonta testified:

- Q. . . . I'm going to read to you some testimony that we received from Mr. Hill . . . only for the purpose of potentially refreshing your recollection, to see if it, you know, jogs your memory. Mr. Hill testified—and this is on page 81 of his transcript—two individuals in Massachusetts organized buses to go down to the rally, and Boston opened up cases on those two individuals because we were shown definitive evidence from WFO of them entering restricted areas of the Capitol. On to page 82 of the transcript, [b]ut those two individuals organized these buses, and there were 140 people on the buses, on the two buses. And WFO wanted us to open up a case on each and every one of those 140 individuals, to which the SSA in Boston said, They were going to a political rally, which is a First Amendment protected activity, no, we're not starting cases on these people. To which they said, meaning WFO, Well, we're going to call your SAC, or your S A C, and the SSA said, Go right ahead. Does that vignette, was that briefed to you?
- A. So once again, the exact verbiage that came from George Hill there, like, I, that I can't recall if that's exactly how it went down. But, yes, the—the—when my team briefed me on that one issue, one of the things they did communicate to me was that because of that initial pushback about not wanting to immediately conduct blanket interviews of all of the 150 some odd passengers, absent [the two individuals who entered restricted space], then, you know, that a comment was made by somebody either out of headquarters or WFO, I don't know which one, that your SAC may be getting a call.
- Q. Okay.
- A. But as we spoke about earlier, I never received any such call or outreach.
- Q. Okay. And do you know who in the WFO would've been making that type of statement?
- A. So it would have been somebody somewhat commensurate to the line supervisor up in Boston. I just don't know who.

- Q. Okay. Hill's testimony goes on, on page 82, Because when you're pushing back, you know, you want to make sure that you have your six covered—I'm not sure what that means, but—so the SAC and the ASAC were intimately aware of these kinds of exchanges that were going on. And again, to his credit, Joe Bonavolonta said, No, we're not opening up cases on people who went to a rally. And I forgot a key part, the SSA for CT2 said, happy to do it . . . Does that jive with your recollection?
- A. Not—once again, just not the—not the verbiage that's being used or the quotes that are being attributed, but in totality, as I've said before all along, the methodology used by the line supervisor to either headquarters or WFO was simply, if you have additional evidence or information that would — that would justify us conducting interviews on certain individuals, then provide it to us, and we will do it.⁶⁴

Bonavolonta also testified that while he was not briefed to “that level of specificity” regarding Hill's disclosure that the presence of undercover officers in the Capitol was the reason the WFO withheld information from the Boston agents, he was aware “we were requesting additional information to see if we could . . . if we in fact had enough of a predication” for investigating.⁶⁵

Bonavolonta further testified:

- Q. And are you aware of whether agents or analysts within the Boston Field Office were asked to work on investigations related to the events that occurred at the U.S. Capitol on January 6th, 2021?
- A. Yes.
- Q. And about how many cases?
- A. I really can't give you a number in terms of the overall number of cases.
- Q. And was it your understanding that the agents within the Boston Field Office were running the investigations?
- A. No. The actual cases relative to January 6th were all program managed and generated out of our Washington

⁶⁴ Transcribed Interview of Mr. Joseph Bonavolonta at 71-2 (May 4, 2023) (hereinafter “Bonavolonta Interview”).

⁶⁵ *Id.* at 74-75.

Field Office. And so, where our involvement would come into play would be if a—you know, a package with the requisite evidence in it that may have risen to the level of an individual being charged with a certain crime related to January 6th would be sent up to us and then worked in conjunction with an agent in my office, as well as with a AUSA within the district of Massachusetts. But then once whether it was if it was for instance, an arrest warrant, that arrest would be executed, and then the case would be—you know, the subject would go down for an appearance in Washington, and then that's where it would be worked from there, whether there was a guilty plea or a trial, it would all be done down in Washington, D.C., not up in Boston.

Q. And, when you say program managed out of the Washington Field Office or the WFO, did that mean the WFO was giving your agents direction on what to do?

A. I wouldn't necessarily say "direction." It was just more—it was more a package that would be sent up with the requisite evidence to execute in most cases an arrest warrant, and that was it. It was pretty—it was very basic.⁶⁶

Q. And you said or one of your colleagues in the Boston Field Office said that if you have additional evidence, we will take it, and if it meets the DIOG, we'll go out and interview these people. Is that correct?

A. That's correct.

Q. And subsequent to that, somebody from Washington came back with some additional evidence on a specific finite number of individuals and then you proceeded to do investigative work on that finite group?

A. Correct.⁶⁷

O'Boyle similarly testified that the combination of financial incentives and political considerations led the FBI's January 6 investigation to go, in his words, "way off the rails."⁶⁸ When asked to clarify this statement, O'Boyle indicated he was pressured by at least one agent

⁶⁶ *Id.* at 10.

⁶⁷ *Id.* at 22-23.

⁶⁸ O'Boyle Interview at 127.

from the WFO to “violate policy [and] law” by initiating legal processes against at least one citizen who was simply the subject of an anonymous tip.⁶⁹ O’Boyle testified:

Q. And when you say “legal process,” what are you referring to?

A. So they were trying to get me to do the grand jury subpoenas, when there was no rational way to conclude that the legal process she wanted was in any way associated with the anonymous tip⁷⁰

Q. . . . Could you explain?

A. So the initial tip I received from [the WFO] I did investigate and did due diligence.

Q. Right.

A. And then the second tip, where then [the WFO is] asking me to get legal process, when there wasn’t a rational link between what [the WFO] wanted me to get the legal process for from the one tip and associating it with the previous tip [the WFO] had sent me the day or maybe 2 days prior.

Q. Okay. And so you declined, you didn’t seek legal process, right?

A. Correct.

Q. Okay. Were there any punitive actions against you for declining to take that step?

A. No, but I think that’s only because I think I was very meticulous in how I wrote it up, and after my boss read it, he was like, “Huh.”

Q. Okay. So, at the end of the day, you exercised your judgment, and you weren’t—there were no consequences for that.

A. As far as I know.⁷¹

⁶⁹ *Id.* at 102-04.

⁷⁰ *Id.* at 105.

⁷¹ *Id.* at 120-21.

Although O’Boyle did not face any punitive actions from the FBI relating to his refusal to unlawfully seek legal process following a tip, his testimony is still shocking. Such testimony confirms that the FBI was pressuring its agents to violate federal law to investigate American citizens without adequate legal process. It is undoubtedly also concerning that O’Boyle feels he avoided any punitive or adverse action from the FBI in this case only because he “was very meticulous” in assessing the case and creating a paper trail to justify his refusal to follow a directive from the WFO.

D. The FBI Gathered Conservatives’ Financial Records from Bank of America Without Any Legal Process Following January 6.

Just like FBI whistleblowers O’Boyle and Friend, retired FBI Supervisory Intelligence Analyst George Hill provided the Committee with detailed allegations of FBI civil liberties abuses. Specifically, he testified that following the events at the Capitol on January 6, 2021, Bank of America (BoA) gave the FBI’s Washington Field Office a list of individuals who had made transactions in the D.C., Maryland, Virginia area with a BoA credit or debit card between January 5 and January 7, 2021.⁷² He also testified that individuals who had previously purchased a firearm with a BoA product were elevated to the top of the list provided by BoA.⁷³ Specifically, Hill testified:

A. . . . The Bank of America, with no directive from the FBI, data-mined its customer base. And they data-mined a date range of 5 to 7 January [of 2021] any BOA customer who used a BOA product. And by “BOA product,” I mean a debit card or a credit card. They compiled that list. And then, on top of that list, they put anyone who had purchased a firearm during any date. So it was a huge list⁷⁴

Q. Was the list that Bank of America provided targeted just to the D.C. area for those—

A. Yes.

Q. —dates?

A. Just the District and surrounding area, so, like, the NOVA area.

Q. And the surrounding area.

⁷² Hill Interview at 74-75.

⁷³ *Id.*

⁷⁴ *Id.* at 74.

- A. Yeah.
- Q. And it's anyone who used a Bank of America either debit or credit card—
- A. Right.
- Q. —to conduct a transaction.
- A. Any transaction. To buy a hotdog. Doesn't matter.
- Q. Okay. And then my understanding is that they created a second list where that first list was prioritized based on individuals that had purchased a firearm?
- A. They just basically just built on top of it, anybody who committed a—you know—
- Q. A firearm purchase?
- A. [T]hese are your priorities, these are your number one individuals that you need to go after. Not only did they use a BOA product in the District, but they've also purchased a firearm at some point in time, any time.
- Q. This list was provided then without any legal process to the FBI?
- A. Correct. So my understanding of the DIOG and amateur assessment based on law is that, you know, if a citizen sees a crime in commission, there's nothing wrong with injecting that and opening up a case. But, to my knowledge, you know, using a debit card or a credit card in the District does not provide adequate predication for the investigation of a crime. So there was no legal process either asking for it or — you know, from the Bureau or from DOJ or anybody.⁷⁵

Hill further testified:

- Q. Mr. Hill, you described the process by which this Bank of America data pull is lashed to data regarding firearm purchases. What was the geographic envelope for those firearm purchases?

⁷⁵ *Id.* at 75-76.

- A. They would had to have met both criteria: used a BOA product in the District—but there was no geographic framework if they had ever, ever bought a firearm.
- Q. What about the firearm purchase as a feature of time? Did—
- A. No, there was no time—there was no—
- Q. So that—
- A. That was not in the data range, date . . . But the gun purchase could be anywhere—
- Q. Anywhere, anytime. You could live—you could be a resident of Iowa, be a BOA customer, purchased a shotgun in 1999, go to the District, use your credit card to pay for a hotel on January 5th and check out. You're going to rise to the top of that list . . . [w]ere there any other criteria, other than the BOA transaction and the firearm purchase, that were prerequisites?
- A. No.⁷⁶

Hill's testimony was corroborated by the testimony of Boston's Special Agent-in-Charge Joseph Bonavolonta, who testified that Boston's JTTF Squad Supervisor, Chief Division Counsel, and Special Agent-in-Charge of Counterterrorism brought the BoA data to his attention. He further testified to the Committee and Select Subcommittee:

- Q. . . . And are you aware of information coming from Bank of America that was sent to the FBI?
- A. I am, yes.
- Q. [A]re you aware of the existence of that information on the FBI systems?
- A. I can't tell you where it is housed on FBI systems or what the current status is, but I am aware of information that was forwarded to us related to a Bank of America lead, yes.⁷⁷

- Q. And why did they bring this information to your attention?

⁷⁶ *Id.* at 76-77.

⁷⁷ Bonavolonta Interview at 11.

- A. So they brought the information to my attention, first and foremost, to make me aware that a lead had been sent to our office from a unit within FBI Headquarters that fell under the Office of Private Sector. And the lead, the lead itself, was for informational purposes only. There was no directive in the lead to do anything . . . from an investigation standpoint. However, in the body of the lead, there was an information that was provided by Bank of America following a certain number of criteria that in essence aggregated a list of individuals that were supposedly living up in the New England area who . . . either had potentially made . . . certain credit card purchases . . . for hotel reservations or plane tickets, or potential purchases at certain gun stores in and around . . . January 6th or planned for the inauguration date, like around January 20th, like in that timeframe. I'm speaking in generalities just because simply I can't recall the exact nature of the criteria, but it was something to that effect. And so my team brought that to my attention just to make me aware of it and to . . . just to see if there was going to be any request to actually . . . do something from an investigative measure on these individuals. So I reviewed the lead, and it was very clear in the lead that there was not a request to engage with anybody. Or we weren't being directed to do anything. But what I did on my own was . . . at the time, I was a co-chair of the SAC Advisory Committee, and I reached out to my colleague who was the SAC out of Springfield, Illinois, who was the chair of the SAC Advisory Committee. So we worked together on that just to see if he had been aware of this. And then we wound up together proactively communicating with the assistant director of the Counterterrorism Division [Jill Sanborn] at headquarters at the time just . . . to see if they were aware that this lead had at least been sent to two field offices. And the only knowledge I had at the time, obviously, was that it was sent to Boston, and it had been sent to Springfield. And we just wanted to make Counterterrorism Division aware of that just to let them know that we, based on the information provided in the lead, . . . we were not planning on doing anything with that information . . . and just so that Counterterrorism Division could be aware as well if in the event that it had been sent to other field offices . . . for awareness. And that was really my level of involvement with that particular lead.⁷⁸

⁷⁸ *Id.* at 13.

- Q. And it was also represented to us that individuals were prioritized on that list if they had a firearms purchase. Does that match your recollection?
- A. So . . . I don't have any knowledge of anybody being prioritized over a firearm purchase, but in one of the criteria that was in there in terms of Bank of America's data, it was related to purchases that had been made at either gun shops or, you know, stores that would sell firearms, but I can't speak to in terms of if any individual on that list was actually prioritized, or at least that wasn't conveyed to me.
- Q. And did the gun purchases have to be recent, or could it have been at any time in the past?
- A. That I just don't know.
- Q. And how many individuals were included on that list that were in the jurisdiction of the Boston Division?
- A. Approximately 6 or 7, or around that number.⁷⁹

This testimony is highly alarming. The FBI seemingly worked with a major financial institution to receive, without legal process, financial records about Americans who used credit or debit card to purchase hotels, flights, or firearms in close proximity to January 6, 2021. This invasion of the privacy of American citizens in this manner is decidedly concerning.

E. Line Agents Opposed Attorney General Garland's Memorandum Directing Federal Law Enforcement Resources Against Parents.

As the radical left pushed its woke agenda on America's children, parents across the country started speaking out at school board meetings against critical race theory, unscientific mask mandates, transgender ideology in the classroom and bathroom, and anti-America curricula. Concerned parents were vocal and unafraid in their opposition to this indoctrination. The National School Boards Association (NSBA) and the Biden Administration, however, could not abide this growing parental rights revolution and colluded to create a pretext—articulated in an October 4 memorandum from Attorney General Garland—to use the federal law-enforcement apparatus to silence parents.⁸⁰

The FBI was a witting participant in the Administration's anti-parent endeavor. A press release accompanying the Attorney General's memorandum highlighted the FBI's National

⁷⁹ *Id.* at 17.

⁸⁰ Memorandum from Hon. Merrick Garland, Atty Gen., U.S. Dep't of Justice, Partnership Among Federal, State, Local, Tribal, And Territorial Law Enforcement to Address Threats Against School Administrators, Board Members, Teachers, and Staff (Oct. 4, 2021).

Threat Operations Center for tips about parents at school board meetings.⁸¹ On October 20, 2021, the FBI operationalized Attorney General Garland’s directives. The FBI’s Assistant Director for the Counterterrorism Division and the Assistant Director for the Criminal Division sent an email to SACs around the country referencing the Attorney General’s October 4 directive and notifying FBI personnel about a new “threat tag” created to apply to school board investigations.⁸² The FBI then began to open investigations with the EDUOFFICIALS threat tag across the nation and established case files on dozens of parents with information that included their political views and the application of this “threat tag” simply because they exercised their fundamental constitutional right to speak.⁸³

The FBI informed the Committee that, between October 14, 2021, and the end of January 2023, the FBI applied the EDUOFFICIALS threat tag to “approximately 25” cases—only one of which “subsequently resulted in the opening of a Full Investigation.”⁸⁴ Additionally, the FBI stated that the majority of these 25 cases “were referred to state and local law enforcement, and the vast majority—all but one—have been closed at the FBI level.”⁸⁵ The FBI also provided that 17 of the 25 cases “were assigned to the [FBI’s] Criminal Investigative Division; six were assigned to the Counterterrorism Division; and the remaining two were assigned to the Weapons of Mass Destruction Directorate”⁸⁶ In other words, the FBI’s disclosure confirmed whistleblower allegations that the FBI had misused criminal and counterterrorism resources against parents attending school board meetings.

Despite the inexplicable willingness of FBI leadership to use federal law enforcement and counterterrorism resources to investigate parents, it is clear that some brave FBI agents in local field offices saw this memorandum for what it was—weaponization of the federal law enforcement community against moms and dads speaking up about their children’s education.⁸⁷ Whistleblower testimony from O’Boyle and Friend details the “shock and surprise” that line agents had when learning of the memorandum and the Attorney General’s directive to target parents.⁸⁸

1. Special Agent O’Boyle Was “Stunned” to Learn that Attorney General Garland Intended to Pursue Concerned Parents for Investigation.

On October 4, 2021, Attorney General Garland issued a memorandum that directed the FBI and U.S. Attorneys’ Offices to address the “disturbing spike in harassment, intimidation, and

⁸¹ Press Release, U.S. Dep’t of Justice, Justice Department Addresses Violent Threats Against School Officials and Teachers (Oct. 4, 2021).

⁸² E-mail from Mr. Carlton Peeples, Deputy Assistant Dir., Criminal Investigative Div., Fed. Bureau of Investigation, to FBI_SACS (Oct. 20, 2021).

⁸³ See Letter from Rep. Jim Jordan and Rep. Mike Johnson, H. Comm. on the Judiciary, to Hon. Merrick Garland, Atty Gen., U.S. Dep’t of Justice (May 11, 2022).

⁸⁴ Letter from Mr. Christopher Dunham, Acting Asst. Dir., Office of Cong. Affairs, Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Jud. (Mar. 1, 2023).

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ See O’Boyle Interview at 78, 85.

⁸⁸ *Id.* at 81.

threats of violence” at school board meetings.⁸⁹ O’Boyle testified to the Committee about his reaction to the memorandum and that of his colleagues. O’Boyle recalled that he was “stunned” to learn “that the highest-ranking law enforcement official in the country would publish something like that to the workforce.”⁹⁰ He viewed “the content and overall direction” of the memorandum to be “leading towards targeting parents for speaking up about their children’s education.”⁹¹ As a former police officer, he found it “most striking at first” that “such a high-ranking federal official” would use “federal law enforcement to hone in on” an area that is typically addressed by local law enforcement.⁹²

O’Boyle also shared the reaction of Supervisory Special Agent (SSA) at the Wichita Resident Agency, Sean Fitzgerald. O’Boyle recalled SSA Fitzgerald, whom O’Boyle reported to, stating “we will not be going to school board meetings in this office.”⁹³ Fitzgerald’s reaction to the memorandum is not surprising to O’Boyle. As O’Boyle put it, “There’s nothing that I know of, based on my training and experience in the FBI, that brings this to a level of federal concern.”⁹⁴

On October 20, 2021, in response to the Attorney General’s October 4 directive, FBI Counterterrorism and Criminal leadership in Washington created the EDUOFFICIALS threat tag to track and monitor school board-related investigations.⁹⁵ O’Boyle testified that the creation of the EDUOFFICIALS threat tag was “troubling” in that both the Criminal Investigative Division and Counterterrorism Division had signed off on the threat tag.⁹⁶ Particularly, O’Boyle questioned why federal law enforcement would be involved in local law enforcement matters, and stated that federal law enforcement involvement would “[a]bsolutely . . . chill parents from exercising their First Amendment right.”⁹⁷ O’Boyle testified:

- Q. And what was your reaction to seeing this EDUOFFICIALS threat tag on the news?
- A. Again, it was shock and surprise, especially—so Carlton Peeples was in charge of the Criminal Investigative Division, but also as part of that email was, I believe, Timothy Langan, who was from the Counterterrorism Division. And it was already surprising that the FBI’s CID would be involved in something like this, but then to have

⁸⁹ Memorandum from Hon. Merrick Garland, Atty Gen., U.S. Dep’t of Justice, Partnership Among Federal, State, Local, Tribal, And Territorial Law Enforcement to Address Threats Against School Administrators, Board Members, Teachers, and Staff (Oct. 4, 2021).

⁹⁰ O’Boyle Interview at 78-79.

⁹¹ *Id.*

⁹² *Id.* at 78-79.

⁹³ *Id.* at 79.

⁹⁴ *Id.* at 86.

⁹⁵ E-mail from Mr. Carlton Peeples, Deputy Assistant Dir., Criminal Investigative Div., Fed. Bureau of Investigation, to FBI_SACS (Oct. 20, 2021).

⁹⁶ O’Boyle Interview at 81.

⁹⁷ *Id.* at 82.

both CID and CTD, the Counterterrorism Division, sign off on a threat tag like that was troubling to say the least.

Q. And just like the memorandum, did agents and employees within your office discuss their reaction to hearing the news of the EDUOFFICIALS threat tag?

A. It is something we discussed just at the squad level, [task force officers] and agents, which I would say, in my experience, everybody I talked to about it was—had a similar reaction as me, like, why are we inserting ourself into this type of matter?

Q. Were you involved with any official conversations or correspondence about the creation of the EDUOFFICIALS threat tag?

A. No.

Q. And given your law enforcement background and your work at the FBI — or I guess when you were at the FBI—did you have any knowledge of or participate in any investigations that were labeled with the EDUOFFICIALS threat tag?

A. No.

Q. Are you generally aware that the FBI did in fact use that threat tag?

A. I am.

Q. And are you aware that several parents were investigated by the FBI for protected First Amendment activity?

A. I am.

Q. Given your law enforcement background and your work in the FBI, does this concern you?

A. It does.

Q. And do you think, given your background, does knowing that you could be investigated by the FBI for speaking up at your child's school board meeting, do you think that would chill parents from exercising their First Amendment right?

- A. Absolutely.
- Q. Given your law enforcement background and your work at the FBI, does the EDUOFFICIALS threat tag have any law enforcement utility? Is there any reason to have it?
- A. I don't believe so.⁹⁸

Significantly, none of the veteran FBI employees interviewed by the Committee to date could articulate a law enforcement utility for the threat tag.⁹⁹

2. Field Agents Viewed Attorney General Garland's Pursuit of Concerned Parents as a Chill on Parents' Protected First Amendment Activity.

This infringement upon parents' constitutionally protected activity was evident to special agents in the field. In his transcribed interview with the Committee, Friend described how he was directed to surveil parents at an anticipated "contentious" school board meeting in an effort to connect January 6 subjects to the EDUOFFICIALS threat tag.¹⁰⁰ As Friend recounted, his supervisor at the time ordered Friend and another agent to go to the location of a local school board meeting.¹⁰¹ As Friend testified:

- Q. So part of the pressure campaign, as you've testified, were these phone calls. Other than phone calls, was there any other medium in which that pressure campaign manifested? Emails? Directives? Other information?
- A. I didn't receive emails. I know that there was probably Instant Message within the FBI, because [a senior agent in our office] was corresponding with [the WFO] that way a lot. And there were communications, I know, for one group that they said they wanted surveillance done on them because they had been talking in online forums, so I know they were being monitored. And they wanted us to surveil them to a school board meeting.
- Q. What more can you tell us about that?
- A. There was an anticipated very—going to be a very contentious school board meeting in Flagler County, because there had been some disturbing books that had been found in the library, and a lot of parents were displeased, and some of these individuals were going to go attend the

⁹⁸ *Id.* at 81-82.

⁹⁹ *Id.* at 82; *see also* Sanborn Interview at 91.

¹⁰⁰ Friend Interview at 111, 127.

¹⁰¹ *Id.*

meeting. And we were asked to surveil them to the meeting. And then, once we arrived, we kind of looked around and said, this looks bad. It was right after the EDU threat tag had emerged. They told us to get out before we were identified as Federal agents.¹⁰²

In his interview, Friend noted that he had concerns about surveilling parents at school board meetings, believing this could chill parents' exercise of their First Amendment rights.¹⁰³ In fact, Friend testified that "I appeared at a school board meeting in September, so I was a little bit humored by the fact that I might be investigating myself."¹⁰⁴ He noted that his colleagues even teased him about this fact when they discussed the Attorney General's memorandum.¹⁰⁵ Friend stated that local law enforcement agencies were capable of handling any issues that might arise at school board meetings, and local law enforcement should properly handle those matters.¹⁰⁶ He testified that his colleagues had a similar dismissive reaction to the memorandum, stating, "We didn't take it seriously to the point where we were going to pursue investigations."¹⁰⁷

This position was not just held by whistleblowers and their colleagues. It was apparently shared by the field and local law enforcement. In an initial set of documents produced to the Committee pursuant to a subpoena, the Justice Department's own documents demonstrate that there was no compelling nationwide law-enforcement justification for the Attorney General's directive or the Department components' execution thereof.¹⁰⁸ After surveying local law enforcement, U.S. Attorney's offices around the country reported back to Main Justice that there was no legitimate law-enforcement basis for the Attorney General's directive to use federal law-enforcement and counterterrorism resources to investigate school board-related threats.¹⁰⁹ In addition, in reports back to Main Justice, many of the U.S. Attorneys' Offices noted that their local law-enforcement partners opposed federal intervention at local school board meetings.¹¹⁰ Similarly, Allen testified:

Q. Do you recall, subject to this memorandum, an email sent by Carlton Peeples, who was the Deputy Assistant Director of the Criminal Investigative Division, also in October of 2021, to announce the creation of an "EDUOFFICIALS" threat tag?

¹⁰² *Id.* at 110-11.

¹⁰³ *Id.* at 128.

¹⁰⁴ *Id.* at 121.

¹⁰⁵ *Id.* at 128.

¹⁰⁶ *Id.* at 121-22.

¹⁰⁷ *Id.* at 122.

¹⁰⁸ In fact, Attorney General Garland admitted as much in his October 2021 testimony to the Committee, conceding that the National School Boards Association letter was the only basis for the Department's actions. *See Oversight of the United States Department of Justice: Hearing Before the H. comm. on the Judiciary*, 117th Cong. at 68 (2021) (testimony from Hon. Merrick Garland, Atty Gen., U.S. Dep't of Justice).

¹⁰⁹ Interim Staff Report, H. Comm. on the Judiciary & Select Subcomm. on the Weaponization of the Fed. Gov't, A "Manufactured" Issue and "Misapplied" Priorities: Subpoenaed Documents show No Legitimate Basis for the Attorney General's Anti-Parent Memo (Mar. 21, 2023) (hereinafter "School Board Report").

¹¹⁰ *Id.*

A. I do remember seeing an email about a threat tag having to do with schools. I can't recall if that was the specific threat tag that I saw on the email, but I do remember there being a creation of a threat tag and some people having ire about it in the squad area.

Q. When you say some people had ire about it, what do you mean?

A. I mean, like, verbal responses like, "What, are we going after, like, people at school like, parents at school board meetings now?" Statements to that effect.¹¹¹

Q. And when you talked about, you know, individuals expressing ire within the JTTF squad area . . . were those individuals special agents . . . ?

A. Yes . . . [i]t was a combination of both. People were like, "Like, what is this? Like, this is ridiculous."

Q. Did they think it was a waste of FBI resources?

A. Yes.

Q. Was it your understanding and the understanding that you could tell from the individuals of the JTTF squad were they under the impression that this was a local law enforcement issue?

A. I don't know what their official, you know, motivation was. I just know that they had ire with the threat tag and comments of the nature of, "What are we doing, going after parents now?" You know, almost like a ridiculousness, you know?

Q. Would you say that the reaction among the JTTF squad to the "EDUOFFICIALS" threat tag, was it negative?

A. I would say yes.

Q. Did you share that ire that your colleagues expressed?

¹¹¹ Allen Interview at 58.

A I thought it was concerning. You know, I thought it was very concerning.

Q And did you believe that the FBI should be using counterterrorism resources on this issue?

A No.¹¹²

According to Friend, the school board memorandum and the directives he had to surveil parents were consistent with the demand to show that DVE cases are on the rise around the country.¹¹³ Friend testified to his belief that he and his fellow agents were told to surveil parents “in order to meet the metrics that we have in order to show that we’re a successful agency.”¹¹⁴ Friend recognized, rightly, that they were overstepping their bounds and infringing on parents’ constitutional rights.¹¹⁵

¹¹² *Id.* at 59-60.

¹¹³ School Board Report, *supra* note 1099, at 123.

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 128.

II. FBI Leaders Weaponized the Security Clearance Adjudication Process Against Whistleblowers in Retaliation for Blowing the Whistle.

Whistleblower testimony makes clear that the FBI rid itself of employees who dared to speak out against FBI leadership or to raise good-faith concerns about FBI operations. The FBI has taken personnel actions against whistleblowers who raised concerns within the Bureau and, later, to Congress. In several instances—Friend, O’Boyle, and Allen—the FBI weaponized the security clearance adjudication process to silence employees who fight against the politicized “rot” within the FBI leadership. Because a security clearance is necessary to work at the FBI, revoking or suspending an agent’s security clearance effectively indefinitely suspends the agent and leaves the agent to languish in an unpaid purgatory.

This section details whistleblower testimony about the retaliation they have faced at the hands of the FBI. Despite FBI statements that it is “committed to addressing misconduct head-on” and that it is “taking considerable steps to ensure that employees are aware of whistleblower protections,” the reality is otherwise.¹¹⁶ As Friend explained, the FBI does all this in a way that “creates an impression that [whistleblowing] is frowned upon.”¹¹⁷ The FBI’s actions against whistleblower employees, rather than its words, reveal how the FBI leadership truly views whistleblowing.

A. Stephen Friend Was Suspended Without Pay After Questioning the FBI’s Handling of DVE Cases and Expressing Concern about January 6 Tactics.

The FBI retaliated against Friend after he expressed concerns about how DVE cases were being labeled and managed, the excessive force used in apprehending January 6 subjects, and for making protected disclosures to Congress.¹¹⁸ Friend testified:

Q. And were you ever told or notified that the FBI SWAT team would be used during search and arrest warrants for January 6th subjects?

A. Yes.

Q. Did that concern you?

A. Yes.

Q. Why did the plans for the execution of these warrants concern you?

A. Because the subject of the arrest warrant had been in communication with the FBI at that point and had expressed a willingness to cooperate with the FBI. And, in my

¹¹⁶ *Id.* at 106.

¹¹⁷ *Id.*

¹¹⁸ Friend interview at 20, 22, 26-27, 30.

experience in dealing with subjects of crimes and bringing them into custody, the FBI tends to use the least amount of force necessary to do that safely, and I felt that the use of SWAT, and coming from my background of being a SWAT team member, I felt that that was an unnecessary tool to use for that particular individual.

Q. So the subject of the warrant that the SWAT team was going to be used for was cooperating with the FBI. Is that your understanding?

A. Yes.

Q. And had mentioned a willingness to come in voluntarily . . . ?

A. Yes.

Q. . . . And in your experience working on criminal cases and SWAT teams, you said that the FBI normally uses the least intrusive methods. Is that correct?

A. Yes.

Q. And is that per FBI or DOJ policy?

A. I don't know what policy. I just know that that is the general approach that we always used.

Q. Can you explain some of the less intrusive methods that might be used for a subject who is cooperating with the FBI and has said that they're willing to come in?

A. You can call the individual and ask them to surrender. You can issue a summons. You can contact their attorney, if they're represented, and ask them to surrender. You can ask for local law enforcement to execute an arrest warrant. You can use surveillance resources to interdict an individual while they're traveling and away from their home base of operations.

Q. And, to your knowledge, none of these were used for the January 6th subjects that you were tasked with executing search and arrest warrants for?

A. Not on the individual SWAT was going to be used for, no.

Q. Did you raise these concerns to your direct supervisor?

A. Yes.¹¹⁹

Q. And what did you disclose to [your direct supervisor]?

A. I raised my concerns about the use of the SWAT team for the arrest. I also raised my concerns about the departures from the DIOG with regards to how the cases were being managed and told him that I believed that it was to manipulate the crime statistics. And I also said that I believed that we were infringing on individuals' Sixth Amendment rights.¹²⁰

Q. Okay. And how did [he] respond to your concerns?

A. He said that—he agreed that there was not a lot of work to be done on JTTF and that he was actually going to lobby to move me back into working child pornography investigations in the next fiscal year. He told me that he was concerned that he was doing file reviews on cases that none of his people in his—none of his subordinates were actually doing work on. And he then suggested that I might want to speak to the employee assistance program for counseling; and then asked me, if he brought my concerns up the chain of command, how they thought—how I believed that they would respond to that, and said that I had a good reputation and that my career could be in jeopardy if I wanted to beg out of participating in the upcoming arrest and searches.¹²¹

Q. And so is it fair to say that you had two kind of tranches of concerns: You had one about the DIOG violations stemming from how the investigations were being labeled, and then a separate concern about the use of SWAT team for one of the January 6th subjects who had been cooperating with the FBI? Is that correct?

¹¹⁹ *Id.* at 18-20.

¹²⁰ *Id.* at 20.

¹²¹ *Id.* at 20-21.

A. Yes.

Q. And you raised both of those concerns to [your direct supervisor]?

A. Yes.

Q. Who did you raise your concerns to next?

A. I was contacted by one of the assistant special agents in charge of my office . . . and asked to attend a meeting with him and another [assistant special agent in charge]. And [he contacted me] on August 22nd in the evening, and I went and attended that meeting the following day, on the 23rd.¹²²

Q. And how did [the two assistant special agents in charge] respond to your concerns?

A. They pushed back on my concerns. They said that I had the right to raise my concerns, but I had to follow through on the orders that I was given to do.

Q. During your conversation with [the two assistant special agents in charge], did you ever refuse to participate in the warrants?

A. I told them that I didn't want to and that, if assigned to, I would have to consider not going, but I would call ahead if that was going to be the case.

Q. And did you raise both your concerns about the labeling of the January 6th investigations as well as the use of the SWAT team?

A. Yes.

Q. And did you ever participate in any of the operations for the executions of the warrants on the January 6th subjects?

A. I didn't have the opportunity to.

Q. Why didn't you have the opportunity to?

¹²² *Id.* at 22.

A. Following my meeting, I received an email from ASAC Markovski telling me that I was ordered to not come to work the following day and that I was going to be considered absent without leave.

Q. So they ordered you to be on AWOL status? Is that correct?

A. Yes.

Q. How long were you on AWOL status?

A. One day, August 24th.

Q. And they never gave you the opportunity to come into the office on that day?

A. No.

Q. When did you go back into the office?

A. August 25th. I emailed my supervisor, Greg Federico, in the evening on the 24th and asked him if I could come back the following day, and he said I could.

Q. Okay. And so, following your AWOL status, did you raise your concerns with anyone else?

A. Yes.

Q. And who was that?

A. I spoke to the special agent in charge of the Jacksonville Field Office, Sherri Onks.

Q. And what did you tell Special Agent in Charge Onks?

A. The same concerns that I had that I had raised with Greg Federico, Sean Ryan, and Coult Markovski . . . [m]y conversation with her was not as lengthy as it was with the ASACs. I essentially told her that my feelings on the matter were not changed after being placed AWOL and that I had concerns about the constitutionality of what we were doing.

Q. And how did she respond to those concerns?

- A. She told me that I represented a very fringe belief within the FBI and that I needed to question whether or not I wanted to have a future with the agency.¹²³

Shortly thereafter, as Friend recounted, when he arrived at work on September 19, 2022, four officials from his office, including the chief security officer, met him and took his badge, credentials, firearms, and all FBI property.¹²⁴ Friend testified:

They said that—they issued me a letter from Human Resources Division, signed by Executive Assistant Director Jen Moore, detailing the rationale for suspending my security clearance. And without a security clearance, I can't work in an FBI space and I can't fulfill my duties as a special agent, so I was suspended indefinitely. I was allowed to exhaust my accrued leave time. And they gave me a mechanism to—if I wanted to use sick time, it would need justification from a doctor. And I was given paperwork to seek outside employment if I wanted to, and escorted from the building.¹²⁵

When asked about his reaction to the suspension, Friend testified:

- Q. What was your reaction when you were suspended?
- A. In the immediate aftermath, I called my wife to come pick me up, and that was pretty disturbing for her. She had a tumor removed from her spine a few weeks before that, and she was not actually supposed to be driving. So she had to come and drive me with a back brace on home. And then, at that point, I started to communicate with my attorneys about, you know, what to do as far as bringing my concerns to the OIG and to the Office of Special Counsel and to Congress. So we drafted a formal complaint and submitted that to all three.
- Q. And have you had any communication with your colleagues from the Daytona Beach Resident Agency since your suspension?
- A. I have one friend who is now a former task force officer. He was not assigned to the JTTF. He was assigned to the Safe Streets Task Force. And he and I are friends, and we go to the gun range together . . . [a]nd the secretary of the office,

¹²³ *Id.* at 22-24.

¹²⁴ *Id.* at 27.

¹²⁵ *Id.*

she sends me text messages just of greetings and hello. But nobody else from the office.

Q. What was the reaction of your colleagues when they learned that you had been suspended?

A. I can only say what my task force friend said, and he said that everybody just kind of went along with whatever the proceedings were but that, in the aftermath, the office has been extremely reticent to do anything. They don't want to draw attention to the office. So the SSRA Federico is sort of nixing anything operational at this point.

Q. And when you say that people are hesitant to take actions, what do you mean by that?

A. Nobody ever got fired for doing nothing . . . [s]o it's pretty easy to extend an investigation out long, as opposed to being more aggressive in your investigative tactics that you use, and it's better to let the dust clear and settle around my situation before you draw a spotlight to yourself.

Q. And do you believe that you were retaliated against by the FBI for making protected disclosures to Congress?

A. Yes.

Q. And do you believe some of your colleagues, some of their hesitation is that they're nervous that they will be retaliated against for speaking up?

A. Yes.¹²⁶

The retaliation did not end with Friend's indefinite suspension. Despite informing Friend that he could seek outside employment, the FBI refused to sign off on his requests to obtain it or to provide him with the documents necessary for other employment. He testified:

Q. Did you take any steps to seek outside employment?

A. I submitted two FD-331s requesting outside employment. The first one was rejected. And the second one I submitted with also a caveat that I requested my training records, which the FBI has yet to furnish me.

Q. So the first form that was rejected, who rejected that?

¹²⁶ *Id.* at 29-30.

A. I was told that it was rejected by the executive management of the Jacksonville Field Office.

Q. Did you get a reason for why it was rejected?

A. No.

Q. And then you submitted a second form for outside employment and asked for records. What records did you request?

A. I'm seeking my firearms training records as well as my training records in general to prove my employment. Both of those are necessary to gain employment from the second outside entity. That's not the first request of those records that I've made either.

Q. . . . And have they given you the requested records?

A. No.

Q. Do you know why they have not given you the records?

A. No, I don't.

Q. Who has been denying your request to obtain your records?

A. I made a request to the firearms training unit and sent an email to their general counsel. And I sent the second request for outside employment to the chief security officer of Jacksonville Division.

Q. . . . And do you think this is just another episode of retaliation, by not giving you your records?

A. Yes.¹²⁷

Coincidentally, Jennifer Moore, who serves as the Executive Assistant Director of the FBI's Human Resources Branch, testified that the agency's failure to give Mr. Friend his records was a "mistake" that she "owned."¹²⁸ Ms. Moore specifically testified:

¹²⁷ *Id* at 32-33.

¹²⁸ Transcribed Interview of Ms. Jennifer Leigh Moore at 119-20 (Apr. 24, 2023) (hereinafter "Moore Interview").

Q. That wasn't done intentionally. What happened to Mr. Friend wasn't done intentionally. These are just all coincidences?

A. I'm not sure what you're referring to that happened to Mr. Friend.

Q Mr. Friend, where you denied his firearms training documents

A We did, and I owned that. That was a mistake . . . [m]istakes happen when you have a 37,000 employee organization.¹²⁹

Q. So it was a mistake not to give Mr. Friend his training records that he requested[?]

A. Yes, sir.¹³⁰

Nevertheless, the FBI knew exactly what it was doing when it suspended Friend's security clearance. The Bureau suspended it as retaliation for Friend making protected whistleblower disclosures to Congress.¹³¹ Without an active security clearance, he could no longer work as an FBI agent. As a husband and father, Friend needed to work to earn income. When asked how his suspension affected his family, Friend testified:

Q. And how has the FBI's retaliation against you affected you and your family?

A. Well, it's very unusual. My household, I have two young children, and they have asked, you know, why I'm not going to work and why my FBI vehicle is not in the driveway anymore, and that's sort of complicated to explain to grammar school children . . . [m]y wife lost her career shortly after my suspension, and she had to sign a nondisclosure about that, but it was under very suspicious circumstances, and I firmly believe that is related to my situation . . . [s]o neither one of us are gainfully employed, and that's been a financial burden on us as well as just a stressor, because we lost our health insurance, as well, with her employment termination.

¹²⁹ *Id.*

¹³⁰ *Id.* at 122.

¹³¹ Friend Interview at 105.

- Q. And if you had to put an estimate on it, how much has this ordeal cost you both in time and financially?
- A. Well, I would say, it's difficult to calculate because she received a severance from her prior employer. But myself, you know, being out of work for about 20 weeks, 13 of which unpaid—you'd have to go back and calculate what my, you know, salary would've been for that time period. But I don't think you can put a price tag on the stress that it's put on our family. I voiced to my supervisors that working for the FBI was my dream job and that's all I ever wanted to do. So having that opportunity taken away from me earlier than I was expecting has been very disappointing. And the way that the Bureau has conducted itself against me in the aftermath—as opposed to actually considering and investigating the righteousness of my complaint, they've chosen to circle the wagons and go after me—I think is very disappointing and soured me greatly enough that I actually resigned today.¹³²

In addition to his family's struggles, and to ensure maximum pressure—and, no doubt, to deter other potential whistleblowers—the FBI denied Friend's requests for outside employment and failed to provide him with records to obtain relevant employment. This ultimately led Friend to have no other option but to resign from his employment with the agency.

B. Garret O'Boyle Was Suspended Without Pay After Moving His Young Family Across the Country.

Like Friend, O'Boyle was subject to FBI retaliation for making protected disclosures to Congress after expressing his concerns up his chain of command with no action being taken.¹³³ O'Boyle, too, had his security clearance suspended.¹³⁴ In his interview, he testified that the FBI has “weaponized that clearance process.”¹³⁵ He explained:

They know that if they claim national security that they, carte blanche, can do whatever they want. And you have to have a security clearance to work in the FBI. So if they find any reason to strip you of that clearance, they'll do it, and they'll send you packing, and then there's no – hardly any recourse for you to take because the FBI investigates itself.¹³⁶

¹³² *Id.* at 33-34.

¹³³ O'Boyle Interview at 26-31.

¹³⁴ *Id.* at 13.

¹³⁵ *Id.* at 14.

¹³⁶ *Id.* at 15.

In his transcribed interview, O'Boyle shared his firsthand experience with the weaponization of the security clearance process. He described how the FBI suspended him right in the middle of his transfer and two weeks before his wife gave birth to their fourth child, causing their personal belongings—clothes, toys, furniture—to be stuck in an FBI-controlled storage unit for an extended period of time. O'Boyle testified:

A. You know, we're begging and borrowing from family for coats for our kids and warm clothes for our baby because the FBI won't let us have our stuff.

Q. And so I just want to make sure that we have everything, kind of, the facts straight on this. So you're notified in June that you make the new unit and you're going to be transferred from Kansas to Virginia, correct?

A. Correct.¹³⁷

Q. So then in order to retrieve your goods after a month of them being held by the FBI, you had to spend over \$10,000 of your own money, correct, to retrieve those?

A. I would have to do the math, but it's right around ten grand.

Q. And in your opinion, do you believe this whole ordeal with recovering your personal goods and having to cover those costs, was that just another episode of retaliation?

A. I believe it was. I think every step of the way it just—the whole process continues to get weaponized. And people are complicit in it because they claim, well, I'm just doing my job and I was told to tell you that I can't let you come get your stuff, or whatever other excuse they can come up with to justify it in their own minds.¹³⁸

O'Boyle further testified:

Q. And let's talk a bit more about your transfer from Kansas to Virginia. You said that you accepted the position in June and then moved. Your first day was September 26th, I think you said. Is that correct?

A. Correct.

¹³⁷ *Id.* at 20.

¹³⁸ *Id.* at 21-23.

Q. So during that time, you sold your house in Kansas, correct?

A. Correct.

Q. And then were your personal belongings moved or shipped to Virginia at some point?

A. They were. So after we closed on our house in—or I guess right before we closed on our house in Kansas, we had a contract—I mean, they contract through the government to some degree, came to our house, they packed up our stuff, put it in a truck and brought it to Virginia, where it was put in storage. And we were supposed to get that—those belongings delivered to the new house once we closed on it. So I'm trying to think of my dates here. So September 26th I get suspended. So between September 26th and November 3rd we're trying to figure out how we can get our stuff. And for the vast majority of that time, we essentially got the runaround from the FBI and the business they contract with on how to release our goods, on if we can get them shipped or not. And I think I have most of that in email. But essentially we kept being told, oh, they're not going to release your goods, they're not releasing your goods, we can't give you your stuff. And then eventually it was certain criteria for me to come get it myself. And so typically all of this is paid for, it's part of the transfer, and you pay, like, the tax bill on this stuff. But instead, in my case, they said, you can come and get it, you have to inspect all of your stuff at the warehouse that it's being stored, and then sign off on the paperwork, and see ya. So at my own expense, again, I rented moving trucks. A friend of mine came with me from Wisconsin. Honestly, I couldn't have done it without him. He has worked in the moving industry for many years. And without his expertise, I don't think my brother and I, who also — he flew in to help — would've been able to even pack it up correctly, because they essentially just pull it all out and say, here's your stuff, make sure it's all there. So we spent the whole day doing that. And, yeah, it cost about \$10,000 out of my own expenses to handle that. That doesn't even account for the labor costs that would've been associated with it. And then it's interesting that on that same day is when I was told that my pay was suspended¹³⁹

¹³⁹ *Id.* at 18-21.

Q. And so for over a month you weren't able to access your personal goods. And can you describe what that includes furniture wise, what?

A. Everything. I mean, it was, yeah, other than, you know, I think our daughters all had, like, a backpack with, like, a toy and some clothes. And then my wife and I, same, had, like, a backpack of clothes and stuff like that. And we obviously did not anticipate this happening, so when our stuff got packed up in August, we had summer clothes because we thought, oh, by late September, early October, we'll be here, which the climate is much more moderate than in Wisconsin. So in October in Wisconsin it's practically winter and we're—just give me a minute.

Q. Take your time.¹⁴⁰

Q. And so to accommodate this transfer, you put your Kansas City home on the market and sell it, correct?

A. Our Wichita home.

Q. Your Wichita home.

A. Well, we lived in a suburb called Derby—

Q. And during that time, did you look for housing in Virginia?

A. We did. And that's another interesting aspect of it. So as part of the transfer, you're supposed to get a house hunting trip, 10 days. I didn't know at the time, but I found out later, that once you accept orders essentially your job is to focus on that transfer and work on that transfer. Instead, I was directed by my boss to try to finish up some casework that I had. So I didn't even really get to focus on that transfer like I should have. But I was able to come back to Virginia. I was here, I think, for 9 days or so, for training for that new position. So every night after—or just about every night after training was over, I would meet with my realtor, and we'd go look at houses. I think in those evenings over that time span, I think I looked at around 30 or 35 houses. So even though I didn't get the 10 day house hunting trip or

¹⁴⁰ *Id.* at 20.

anything like that, I was able to look for housing while I was at that training, which was in August.

Q. So then did you put an offer on in a house here?

A. We did. My last day of that training, which I think was like either the last day of August or the first day of September, is the last house I looked at, and I was like, oh, this is the one. And once I got back to Kansas, I talked to my wife about it, showed her pictures and stuff. And we put an offer in on it which was accepted and—yeah, so we were, like, okay, that part's done, now let's have this baby and then carry on. But obviously that—it didn't work out as planned.

Q. And so you packed up all your belongings in August, and then the FBI moved those belongings to Virginia, correct?

A. Correct.

Q. So you're now in Virginia, your Kansas City—or your Wichita house is sold, and your belongings are in Virginia, and then on the first day at your new job in Virginia, you're walked out, correct?

A. Correct.

Q. So then you have to wait over a month to retrieve your belongings because, as you've said, the FBI was giving you the runaround, correct?

A. Correct.

Q. Did you have access to those belongings during that period of time?

A. I did not.

Q. And did you ask the FBI for access to those belongings?

A. We did. We asked if we could come get them and because there was really no other way than—that's when it was just back and forth, back and forth, or then not hearing from them, and then them saying, oh, we're trying to figure out the best way to get you your stuff. And then at one point, were, like, well, can you ship them here? Because we're not living in Virginia now. And then I think at one point they

were, like, oh, we might be able to do that, but it's going to cost you \$17,000. And we were, like, whoa, no, we—I'm suspended. Like, we knew my pay was going to get suspended. It hadn't been suspended yet. But we were, like, no, we're not paying you \$17,000 for you to send us our stuff that you took to Virginia. So then we were able—they eventually they agreed to let me go and get it. That still cost, like I said, about ten grand, but I guess that beats 17.

Q. And the FBI wouldn't—in the normal course of things, if you're transferred, the FBI pays for those expenses, and then, as you said, you're in charge of the tax bill. Is that correct?

A. Correct.¹⁴¹

“Nearly 180 days” after his suspension, O’Boyle testified that he had not heard from the FBI regarding the status of his security clearance.¹⁴² Ms. Moore, who signed O’Boyle’s notice that his security clearance was suspended, testified that O’Boyle’s situation was a mere “coincidence.”¹⁴³ Ms. Moore specifically stated:

Q. The date that's on Mr. O'Boyle's letter? That was . . . October 22nd[?]

A. Yeah. And what day did Mr. O'Boyle execute his actual move?

Q. His first day was on September 23, 2022.

A. And so what was the date of the letter?

Q. September 23, 2022.

A. Okay.

Q. So that's just some big coincidence, that it was his first day [in Virginia]?

A. Absolutely.¹⁴⁴

¹⁴¹ *Id.* at 21-23.

¹⁴² *Id.*

¹⁴³ Moore Interview at 121-23.

¹⁴⁴ *Id.* at 121.

Pointedly, however, O’Boyle believes that the agency was intentionally weaponized against him.¹⁴⁵ As O’Boyle testified:

- Q. Culture wise, is the current FBI the same FBI you signed up to work for?
- A. Not at all.
- Q. Why?
- A. I think the biggest reason is how they have become weaponized against anyone who doesn’t just toe the line that they want them to toe. I think I’m a primary example of that. I start shedding light on things, on wrongdoing that is happening in the FBI; I get suspended. And I know I’m not alone. There are a number of other whistleblowers out there who are in a similar situation after being suspended. Some of them, after—it said—they claim they don’t retaliate for First Amendment protected activity. I know for a fact that they do, because one of my protected disclosures was about that, about the FBI retaliating against employees for engaging in First Amendment protected activity, and those employees got suspended.¹⁴⁶

Many other FBI whistleblowers told O’Boyle that they believe his experience is perhaps the most severe exhibition of the FBI’s weaponization.¹⁴⁷ As O’Boyle told the Committee and Select Subcommittee:

- Q. The retaliation that you’ve testified to today seems to have an enhanced feature of cruelty to it.
- A. I agree. I agree.
- Q. You know, are you and the other whistleblowers, the cases that you’re aware of, are there features of such acute cruelty?
- A. Not like this. My situation is one that all the other whistleblowers I’ve talked to are like, “I just can’t believe” — I mean, and they’re in a similar situation, they’re suspended without pay, and they say, “I can’t believe what has happened to you.” You know, earlier, I alluded I went to Iraq and Afghanistan, a year each, as an infantryman. I received the Combat Infantryman Badge for—I mean, that

¹⁴⁵ O’Boyle Interview at 37-38.

¹⁴⁶ *Id.*

¹⁴⁷ *Id.* at 108-09.

is awarded to infantrymen who fight the enemy. So I've been shot at. I've had rockets shot at me, IEDs. And it's different, but this, what I'm going through right now, is harder than those deployments. When I got home from Afghanistan, I knew I was getting out of the Army. I had 10, 11 months left. And I was like—I had just turned 25, and I was like, "I'm done. The hardest thing I will do in my life, I've done it, and now I can move on." And then this happened. And it's not war, but it's very war like, in what it has done to me mentally, what it's doing to me and my family. And I didn't have a family then. You know, I just had my wife. And, you know, yeah, it's just—it's hard to believe.

- Q. Yeah . . . In these other suspensions, there doesn't seem to be this purposeful manifestation of cruelty to someone's family, to someone's living situation, to someone's ability to secure future employment. Why do you think the acuity of the cruelty is so much higher with you?
- A. I wish I knew. I think it probably just goes back to the pervasiveness of how the FBI has deemed—they've decided they're going to do what they want, on their agenda, on their terms, that they're the law, and they're not going to have someone internally shining a light in the darkness on the bad things that they are doing. And I think they realized, we have him in the perfect position to completely flip his life upside down and cause torment to him. Because then they can come back and say, well, look at his mental status, or, you know, he's clearly unstable, he hasn't had a job, or whatever they might try to drum up in the future, which I wouldn't be surprised at anything they try to drum up. But—
- Q. Do you believe they're making an example out of you?
- A. I do, yeah. I think it's clear. I mean, and I think that also has a cooling effect on speech, because any FBI employee who hears my story I'm sure would be stunned.
- Q. So you believe that you and your family are being . . . tortured so that the FBI can send a message to any future whistleblowers that this is what life will be like for you?
- A. I do.¹⁴⁸

¹⁴⁸ *Id.*

C. Marcus Allen Was Suspended for Merely Forwarding Open-Source News Articles to His Colleagues.

The FBI retaliated against Marcus Allen, a decorated Marine and former FBI Staff Operations Specialist in the Charlotte Field Office, for simply performing the duties of his job.¹⁴⁹ Like other whistleblowers, Allen was suspended without pay.

Allen, who held a top-secret security clearance for approximately two decades, had worked as part of FBI Charlotte's Joint Terrorism Task Force (JTTF) while employed by the Bureau.¹⁵⁰ In addition to the JTTF, Allen's duties included "respond[ing] to the intelligence program."¹⁵¹ In order to meet the requirements of the intelligence program, Allen testified he was required to perform "all-source analysis" in which he would "research publicly available information [and] anything on the open web . . . to help out with our assessments and cases that the FBI has."¹⁵² While reading open-source news articles and watching open-source opinion videos concerning the events at the U.S. Capitol on January 6, 2021, Allen testified that he sent around links to these articles for his squad's "situational awareness" related to the FBI's investigation.¹⁵³ Because these open-source articles questioned the FBI's handling of the violence at the Capitol, the FBI suspended Allen for "conspiratorial views in regards to the events of January 6th"¹⁵⁴ However, Allen testified that passing along such articles was "part of [his] job."¹⁵⁵ Allen particularly stated:

Q. And why exactly did you send th[e] email[s]?

A. I sent [the emails] just for awareness because the[y] . . . indicated potential problems with the investigation as far as informants were concerned, and our organization's potential forthrightness about the utilization of informants there on that day. That might have some impact on our cases and the subjects that we're looking up, and just a general awareness overall for the investigation as a whole, that there might have been some kind of potential Federal involvement with the activities on January 6th, and I thought it was important enough that it like warranted our attention, you know.

Q. Is it safe to say that you sending th[ose] email[s] was part of your job at the time?

A. Yes.

¹⁴⁹ Allen Interview at 49.

¹⁵⁰ *Id.* at 10.

¹⁵¹ *Id.*

¹⁵² *Id.*

¹⁵³ *Id.* at 25.

¹⁵⁴ *Id.* at 19.

¹⁵⁵ *Id.* at 30.

Q. Did you direct any of your colleagues to take any action regarding [these emails]?

A. No.¹⁵⁶

Worse yet, the FBI did not even give Allen the opportunity to rebut the allegations or to meet with agency leadership in his office.¹⁵⁷ Instead, Allen testified:

Q. So I want to talk more about the actual day of your suspension. I know that might be tough. So can you walk us through what happened that day?

A. Yes. So on the actual day of my suspension, I met with the chief security officer . . . , as well as [the] assistant special agent in charge The assistant special agents in charge are like the top three or four agents in the office right underneath the special agent in charge who's the chief essentially. And I met with them in a parking lot at a Cracker Barrel off of Carowinds Boulevard in Charlotte. They met me, and they read off a letter in the parking lot that I was being suspended for conspiratorial views in regards to the events of January 6th, and that my suspension—the date of the start was January 10th. The day of the meeting was January 19th, and it would be without pay as well.¹⁵⁸

However, the retaliation did not end with Allen's suspension. During his suspension, Allen testified that he sought the FBI's permission to seek outside employment, but the FBI has refused to acknowledge his requests or provide him with the documentation necessary for other employment. Allen specifically testified:

Q. Have you ever sought [the FBI's] approval for outside employment?

A. Yes.

Q. Can you expand upon that and tell us when you sought outside employment?

A. Yes. I sought outside employment within the past month. I went through the process. Because of the nature of the employer, I needed to correspond with an ethics attorney, which I did. I explained to him the announcement and the type of job, and we had a correspondence back and forth.

¹⁵⁶ *Id.* at 30-31.

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

And he relayed to me to go ahead and submit the outside employment form, the 331B, to the chief security officer at the Charlotte Field Office, . . . , which I did. I reached out to her. I submitted it, and she said she put it within the [Enterprise Process Automation System].¹⁵⁹ That employment approval—there’s a 15 business day response time, and that 15 day response time has been expired for several days, and I’ve received no correspondence back from the Bureau in its regard.¹⁶⁰

Allen additionally testified:

Q. And so you have received no answer as of today about your outside employment request?

A. No.

Q. And before that, did you submit to the FBI a prayer journal for prepublication review?

A. Yes.

Q. And when, about, was that?

A. Let’s see. That would’ve been October of 2022.

Q. And why did you submit it to the FBI for prepublication review?

A. I just wanted to make sure that it was okay; that, you know, I had their okay to go ahead and do it. Because of the nature of the situation, I conveyed, you know, there is nothing in here referencing my time as an employee for the FBI. You know, there’s nothing in reference to the FBI like, basically conveying to them that there’s nothing there that I’m trying to profit off of my association with the FBI. And I just want to make sure that I’ve got the, “Hey, we’re good to go. You can go ahead and do whatever you want with your prayer journal.” There was a correspondence back and forth, and then the correspondence dropped off, and I got no response after that.

¹⁵⁹ *Privacy Impact Assessment for the Enterprise Process Automation System (EPAS)*, FED. BUREAU OF INVESTIGATION (July 15, 2011), <https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/departments-of-justice-fbi-privacy-impact-assessments/enterprise-process-automation-system>.

¹⁶⁰ Allen Interview at 66-67.

Q. So your goal was to publish the prayer journal. Is that correct?

A. Yes.

Q. And maybe gain some income, since you weren't earning any income at that point in time?

A. Yes.

Q. So you're suspended from the FBI February of 2022. Is that correct?

A. Yes.

Q. And then you get a month of pay due to your service to the country. Is that correct?

A. Yes.

Q. And then you are without pay from February until today, correct?

A. Correct.

Q. So you sought prepublication of your prayer journal in October of 2022 to earn some income, and then you never heard back from the FBI as to whether or not you could go ahead and publish it?

A. Correct.

Q. And then, just this month, you requested outside employment approval. Is that correct?

A. Yes.

Q. And you have never heard back from the FBI?

A. No.

Q. So you've been languishing now for over a year on unpaid suspension. Is that correct?

A. Correct.

Q. And, during that time, you have earned no income. Is that correct?

A. Correct.¹⁶¹

Allen further testified about the financial hardship that the FBI's decision to suspend him without pay has had on his family. He explained:

My family and I have been surviving on early withdrawals from our retirement accounts while the FBI has ignored my request for approval to obtain outside employment during the review of my security clearance.¹⁶²

The FBI officially revoked Mr. Allen's security clearance one day after his transcribed interview to this Committee.

D. Whistleblowers Have Described How the FBI's Politicization Has Crowded Out its Traditional Law Enforcement Function.

Whistleblowers have told the Committee that the FBI's Washington hierarchy is "rotted at its core" and maintains a "systemic culture of unaccountability." The FBI and the Department of Justice have been deeply politicized by its current partisan leadership. This politicized behavior has adversely affected front-line FBI agents.

According to O'Boyle, the FBI has allowed itself to be "enveloped in this politicization and weaponization" so much so that it is "a cancerous point."¹⁶³ O'Boyle testified:

Q. Are you aware of allegations that the FBI is using security clearance revocations as a tool to purge conservatives from its ranks?

A. I am.

Q. Do you believe that's occurring?

A. I do.

Q. Do you believe that the FBI has become political?

A. I do.

Q. Do you think the extent of the politicization at the FBI is a

¹⁶¹ *Id.* at 68-70.

¹⁶² *Id.* at 6.

¹⁶³ O'Boyle Interview at 154.

problem that festers within its hierarchy, or is it nationwide, enterprise-wide?

- A. I think it's encompassed in the hierarchy and then it trickles down throughout the rest of the Bureau. And those who are especially geared towards promoting will adhere themselves to whatever they need to promote. I think most people out in the field try to avoid that politicization of the agency, which is good. But it's gotten to a point, it seems to me, that it's like a cancerous point where the FBI has let itself become enveloped in this politicization and weaponization that I don't know how to even begin to fix it.¹⁶⁴

When asked about characterizations of the FBI's hierarchy, Friend stated that it was "consistent" with what he has heard from other FBI employees.¹⁶⁵ Friend testified:

- Q. Whistleblowers told committee Republicans that the FBI's Washington hierarchy is, quote, "rotted at its core," end quote, maintains a, quote, "systemic culture of unaccountability," end quote, and is full of, quote, "rampant corruption, manipulation, and abuse," end quote. Do you agree with these statements?

A. Yes.

- Q. And what is your reaction to hearing that this is how people characterize the FBI?

A. It sounds consistent with just about everybody that I've talked to who has never gone to headquarters.

- Q. So it doesn't surprise you that fellow FBI employees and agents are making these characterizations?

A. No.¹⁶⁶

Similarly, Allen testified about the politicization that he has witnessed within the FBI. He explained:

- Q. Mr. Allen, do you feel that you've been treated fairly?

A. No.

¹⁶⁴ *Id.*

¹⁶⁵ Friend Interview at 130-31.

¹⁶⁶ *Id.*

- Q. Do you believe that the FBI has become political?
- A. Yes.
- Q. Given your experience, do you see any other recent actions that we haven't discussed today by the Biden administration, DOJ, and the FBI as problematic?
- A. Problematic? I would say, by appearance, some of the information that's been made available in the public domain about public corruption that on the surface appears to not be being pursued seems problematic, especially in regards of public corruption when it comes from the highest offices in the land.
- Q. Is it fair to say that you've lost confidence in the FBI's leadership?
- A. Yes.
- Q. So the FBI told this committee that it . . . "does not target or take adverse actions against employees for exercising First Amendment rights or for their political views." Do you think that's accurate?
- A. I don't agree with that statement.¹⁶⁷

In Hill's view, similarly, the FBI needs "tough love" to eliminate its highly politicized culture and return to a "highly functioning, apolitical, high-performing FBI."¹⁶⁸

For whistleblowers who have spoken with the Committee and the Select Subcommittee, working for the FBI was their dream job.¹⁶⁹ They came to Congress with the goal of helping to return the FBI to its origins as an effective, apolitical law enforcement agency.¹⁷⁰ The FBI's motto—Fidelity, Bravery, Integrity—has long been used to describe the motivation of the men and women who serve.¹⁷¹ Yet agents like O'Boyle and Friend do not believe the FBI has kept

¹⁶⁷ *Id.*

¹⁶⁸ Hill Interview at 103.

¹⁶⁹ See Friend Interview at 34; see also O'Boyle Interview at 8, 25.

¹⁷⁰ See, e.g., O'Boyle Interview at 26 ("[W]hen we see things that are wrong, that are harmful to people, that are unloving, or that are against the law, it's my duty to speak up."); see also *id.* at 25 ("Every single American deserves the rights that are provided to us in the Constitution. And every single FBI agent should uphold those rights. And every single FBI agent, when they see that the agency they work for are treading over those rights, they have to speak up."); see also *id.* at 30 ("I think in a lot of ways I was, like, oh, the FBI's not actually what I thought it was, where you have people who want to serve this great nation and keep it strong and uphold the Constitution. Rather, you have people who just do what they're told and want to climb that ladder and get that pension.").

¹⁷¹ See *Seal & Motto*, FBI, <https://www.fbi.gov/history/seal-motto> (last visited May 17, 2023).

faith with this motto, stating it “couldn’t be further from the truth.”¹⁷² And when they spoke out against what they reasonably believed were abuses and violations of law, they were silenced and their lives were upended. The efforts to silence whistleblowers, treat them cruelly, and ruin their careers are intended to prevent other agents from speaking out. The first step toward treatment is diagnosing the illness, and these brave whistleblowers have outlined the systemic sickness at the FBI’s core.

¹⁷² O’Boyle Interview at 90; *see also id.* (stating that other agents have supported his whistleblowing but “when they see something that’s wrong, most of them don’t report it, because they’re trying to get to that 20-year mark and get that pension or whatever ... is inhibiting them”).

III. Committee Democrats Attacked and Defamed FBI Whistleblowers to Advance a Political Agenda.

On March 2, 2023, Committee Democrats released a misleading document based on selective, cherry-picked information to attack some of the FBI whistleblowers who bravely testified to the Committee and Select Subcommittee.¹⁷³ Rather than engage in good faith with the substance of the concerns raised by these FBI whistleblowers, the Democrats mischaracterized much of the whistleblowers' testimony, reached conclusions not based in fact or law, and denigrated these Americans with *ad hominem* attacks. The Democrat's report was so egregiously inaccurate that news organizations reporting on it were forced to later correct the record about the whistleblowers.¹⁷⁴

Wildly, the Democrat report asserted that “[n]o law protects witnesses who speak to Congress.”¹⁷⁵ This assertion is plain wrong. But worse, it reveals the Democrats' broader posture toward these brave federal law-enforcement officers: distort, distract, and discredit any effort to expose federal bureaucratic misconduct. The Democrats similarly deployed this strategy during the Select Subcommittee's March 9, 2023, hearing to expose the government-censorship complex. During that hearing, several Democrat Members pressured two independent and highly respected journalists to reveal their sources, and Ranking Member Stacey Plaskett attacked them as “so-called journalists.”¹⁷⁶

A. The Democrat Report Erroneously Claims that the FBI Whistleblowers Who Have Appeared Before the Committee Are Not *Real* Whistleblowers.

During their transcribed interviews, each of the FBI whistleblowers detailed episodes in which they had firsthand knowledge of what they reasonably believed to constitute fraud, waste, abuse, mismanagement, or violations of a law, rule, or regulation at the FBI. Despite the unsupported conclusions in the Democrats' report asserting otherwise, these episodes as detailed by the whistleblowers in their own words are exactly the types of protected disclosures contemplated by whistleblower protection laws.

Federal law—specifically, 5 U.S.C. § 2303—protects federal employees, including FBI employees, from retaliation for disclosing what he or she *reasonably believes* to be evidence of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.¹⁷⁷ Under the law, a whistleblower is protected even if what he or she discloses ends up being wrong or mistaken, so

¹⁷³ Democratic Staff of H. Comm. on the Judiciary, 118th Cong., *GOP Witnesses: What Their Disclosures Indicate About the State of the Republican Investigations 1* (hereinafter “Democrat Report”).

¹⁷⁴ See, e.g., Luke Broadwater and Adam Goldman, *G.O.P. Witnesses, Paid by Trump Ally, Embrace Jan. 6 Conspiracy Theories*, N.Y. TIMES (Mar. 2, 2023); Justine McDaniel, *Democrats Challenge Credibility of GOP Witnesses Who Embrace False Jan. 6 Claims*, WASH. POST (Mar. 3, 2023).

¹⁷⁵ See Democrat Report, *supra* note 173, at 10.

¹⁷⁶ *The Twitter Files Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't*, 118th Cong. 8 (2023) (statement of Rep. Stacey Plaskett, Delegate, United States Virgin Islands).

¹⁷⁷ 5 U.S.C. § 2303 (emphasis added).

long as it is a reasonable, good-faith belief.¹⁷⁸ The law is not overly complicated, yet the Democrats’ report claims without evidence that “[n]one of the three witnesses interviewed to date comes close to meeting that definition” of a whistleblower.¹⁷⁹ Democrats concede, as they must, that an FBI employee is protected from reprisal if a whistleblower makes a disclosure that he or she reasonably believes to evidence such violations.¹⁸⁰ Nevertheless, throughout their report, they ignored the reasonable belief standard and, instead, invented a beyond a reasonable doubt standard that whistleblowers must satisfy.¹⁸¹

The Democrats’ report improperly tries to disqualify the whistleblowers’ numerous meritorious claims by mischaracterizing their disclosures, manipulating their testimony, and making false claims to support the Democrats’ conclusion that Hill, O’Boyle, and Friend are not *real* whistleblowers. Despite the Democrat’s bluster, the record is crystal clear. Each of these whistleblowers had a good-faith basis for believing wrongdoing had occurred.

1. George Hill.

Retired FBI Supervisory Intelligence Analyst George Hill provided the Committee with detailed allegations of FBI abuses. However, instead of engaging with Hill’s allegations, the Democrat report minimized the allegations by trying to discredit Hill. The report claims that “Hill explained that he himself did not handle any cases . . . and, while he viewed an electronic communication referencing the list in the FBI’s case management system, he never opened or viewed the actual list himself.”¹⁸² *Rolling Stone*, in an article based on information leaked from Democrats, assumed this biased framing, asserting that Hill “learned about [the allegations] only through secondhand chatter from colleagues.”¹⁸³ In a response to *Rolling Stone*, Hill’s attorney explained that this assertion was “factually incorrect, misleading, and lacked context.”¹⁸⁴ An examination of Hill’s testimony demonstrates that the *Rolling Stone* article—and the Democrat assertion on which it is based—is wrong.

Hill testified that he observed the FBI Sentinel electronic message bringing the list of Bank of America customers’ transactions purportedly related to January 6th into the FBI’s internal system, and that “the [Supervisory Special Agent] and I had already talked about it, and the SSA had already talked to the [Assistant Special Agent in Charge] about it.”¹⁸⁵ Hill believed the FBI’s receipt of this information was a violation of law, explaining that “there was no legal

¹⁷⁸ See *id.*; see also *Whistleblower Rights and Protections*, U.S. Department of Justice Office of Inspector General, <https://oig.justice.gov/hotline/whistleblower-protection> (last visited May 17, 2023) (explaining the requirements for a disclosure to be protected).

¹⁷⁹ See Democrat Report, *supra* note 173, at 4 (internal quotations omitted).

¹⁸⁰ *Id.*

¹⁸¹ See *id.* at 29 (claiming O’Boyle “did not present any violation of a law, rule, or regulation, or of gross mismanagement, waste of funds, an abuse of authority, or a substantial danger to public health or safety”); see also *id.* at 49-50 (claiming Friend also did not provide any evidence).

¹⁸² Democrat Report, *supra* note 173, at 11.

¹⁸³ Kara Voght, Adam Rawnsley, Asawin Suebaeng, *Inside Jim Jordan’s Disastrous Search for a ‘Deep State’ Whistleblower*, ROLLING STONE (March 2, 2023).

¹⁸⁴ See Jason Foster (@JsnFostr), Twitter (Mar. 3, 2023, 9:45 AM), <https://twitter.com/JsnFostr/status/1631667084512903170>.

¹⁸⁵ Hill Interview at 74.

process . . . asking for it . . . from the Bureau or from DOJ or anybody.”¹⁸⁶ On these facts, it is clear that Hill had a reasonable belief that there was a violation of law.

2. Garret O’Boyle.

The Democrat’s attempt to discredit the disclosures of O’Boyle by creating a procedural strawman around his allegations. They criticized O’Boyle for not providing information in his transcribed interview that was included in his protected disclosures to Congress. The Democrats concede “[t]hat material may well include relevant, probative evidence that would bear on the validity of his claims,” but still wrongly assert that O’Boyle provided no “evidence of a violation of law, rule, or regulation”¹⁸⁷ Here too, the Democrats ignored the substance of O’Boyle’s testimony.

During his transcribed interview, O’Boyle highlighted his numerous firsthand experiences with fraud, waste, and abuse at the FBI.

- In highlighting the FBI’s attempt to inflate DVE numbers, he testified to one instance in which the FBI instructed him to divide one case into four cases, to “open a case for every individual that I had an articulable, factual basis that there may have been potential Federal law being violated.”¹⁸⁸ He said this was done so the FBI could show Congress that DVE cases were on the rise and in turn receive more funding.¹⁸⁹
- In another part of his interview, O’Boyle testified about the EDUOFFICIALS threat tag, used by the FBI to investigate parents who attended school board meetings. O’Boyle testified that investigating parents for First Amendment-protected free speech was “absolutely not” a proper use of FBI resources.¹⁹⁰
- He also testified to the FBI’s use of “arbitrary” metrics to award bonuses to Special Agents in Charge.¹⁹¹ By basing bonuses on arbitrary metrics like how many Title III wiretaps or FISAs were obtained, O’Boyle stated that this focus on metrics “leads to a pervasive culture of not letting the cases dictate where the investigation goes, but it’s the manager or the agent pushing for a certain avenue.”¹⁹²

This testimony establishes that O’Boyle had a reasonable belief that the FBI was violating the law, abusing its authority, or wasting taxpayer funding.

3. Stephen Friend.

The Democrat report also presents a strawman to discount FBI whistleblower Friend’s allegations of FBI abuse. The report asserts that because the Office of Special Counsel (OSC)

¹⁸⁶ *Id.* at 76.

¹⁸⁷ Democrat Report, *supra* note 173, at 29.

¹⁸⁸ O’Boyle Interview at 92.

¹⁸⁹ *Id.* at 92-93.

¹⁹⁰ *Id.* at 85.

¹⁹¹ *Id.* at 98-100.

¹⁹² *Id.* at 99.

and the Department of Justice’s Office of Inspector General (OIG) declined to open an investigation into Friend’s claims, his whistleblower claims are invalid.¹⁹³ Neither the facts nor the law support the Democrats’ anti-whistleblower assertions.

While OSC and OIG did not open investigations into Friend’s whistleblower claims, OIG did *not* reject Friend’s retaliation claim.¹⁹⁴ In response to erroneous media reporting relying on the Democrats’ report in early March 2023, Friend’s attorney explained that “the OIG ’had not investigated Friend’s claims at that point, but did not reject them either—it simply claimed it did not have enough resources and chose not to open an investigation.¹⁹⁵ The OIG asked Friend for his permission to refer the disclosure back to the FBI to investigate itself, which Friend declined to provide.”¹⁹⁶

By obsessing on OSC’s failure to open an investigation, Democrats ignored serious allegations of FBI wrongdoing. Specifically, Friend’s written complaint, which he provided to the Democrats in advance of his transcribed interview, included allegations that the FBI engaged in at least three systemic abuses.¹⁹⁷ Friend testified about matters concerning:

- The manipulation of case management policies to drive a false narrative supporting an FBI priority;¹⁹⁸
- The violation of the DOJ’s Use of Force policy and FBI policy to send a message to disfavored actors; and¹⁹⁹
- Whistleblower retaliation.²⁰⁰

During his transcribed interview, Friend testified about how the FBI’s focus on January 6 cases led to wasted resources and a de-emphasis on child exploitation crimes.²⁰¹ Friend related one example in which the FBI ordered Friend to make a three-hour round-trip to conduct an in-person interview of a January 6 subject, even though other less-intrusive methods had not substantiated the allegations.²⁰² Friend explained that he learned the subject was not in D.C. on January 6 because he was at his son’s funeral in Florida.²⁰³ Friend testified that by confronting the man about his whereabouts on that day, he needlessly forced the man to re-live the worst day of his life.²⁰⁴ As Friend’s attorney explained to the media, “Friend’s disclosures are protected

¹⁹³ Democrat Report, *supra* note 173, at 30-31.

¹⁹⁴ Friend Interview at 92-96.

¹⁹⁵ See Letter from Tristan Leavitt, President, Empower Oversight, to Hon. Michael E. Horowitz, Inspector Gen., U.S. Dep’t of Investigation; See also Letter from Jason Foster, Founder & President, Empower Oversight, to U.S. Dep’t of Justice, Office of Inspector Gen. (Jan. 31, 2023).

¹⁹⁶ Letter from Jason Foster, Founder & President, Empower Oversight, to U.S. Dep’t of Justice, Office of Inspector Gen. (Jan. 31, 2023).

¹⁹⁷ See Democrat Report, *supra* note 173, at 175.

¹⁹⁸ *Id.* at 131.

¹⁹⁹ *Id.* at 19-20, 26.

²⁰⁰ Friend Interview at 21, 23, 32-33.

²⁰¹ *Id.* at 8.

²⁰² *Id.* at 192.

²⁰³ *Id.*

²⁰⁴ *Id.*

whistleblower disclosure about wasted resources²⁰⁵—and Friend testified accordingly²⁰⁶—but the Democrats edited that portion of the transcript out of their one-sided presentation.”²⁰⁷

B. The Democrat Report Slandered the Integrity of Veteran Federal Law Enforcement Officers in the Service of Partisan Politics.

Committee Democrats ignored the substance of O’Boyle’s, Friend’s, and Hill’s allegations of FBI wrongdoing. Instead, they attacked the messengers with *ad hominem* attacks. Throughout their report, Democrats implied and then explicitly accused these former FBI employees of being “insurrectionists” and “conspiracy theorists” who only sought to profit from their whistleblowing activities.

In their report, Democrats asserted that these FBI whistleblowers objected to the arrest of January 6 subjects who had committed crimes. This is wrong and easily contradicted by the actual whistleblower testimony. For example:

- In questioning from Democrat staff, Friend explicitly condemned the individuals who committed violence on January 6th. He testified: “[A] lot of these guys are bad dudes, and they should go to jail. And we didn’t follow our rules, and we set ourselves up to get crushed at trial . . . lose on appeal. I want to win.”²⁰⁸ Friend explained that his concern was with the *process* leading to the arrests, not with the people, especially when certain January 6 subjects were cooperating with investigators.²⁰⁹
- Hill similarly testified: “I don’t support, under any circumstances, attacking police officers, breaking into restricted areas, destroying of government property. . . . Every person that broke the law needs to be identified and prosecuted to the fullest extent. What I take umbrage with is casting in a sea net covering miles and scooping up everything that they can and the erosion of civil liberties surrounding that.”²¹⁰
- When asked whether he believes the government should be prosecuting individuals that were involved on January 6th, O’Boyle testified: “Some of them, yes.”²¹¹

Rather than address the content of the whistleblower allegations, Democrats attacked the whistleblowers for their personal, constitutionally protected views. At each transcribed interview, Democrats spent a majority of their time badgering the witnesses about their personal opinions on public matters. Democrats confronted the witnesses with cherry-picked social media posts, hoping to portray the whistleblowers as holding controversial, disfavored, or unpopular

²⁰⁵ Katelynn Richardson, *DOJ Internal Watchdog Shuts Down House Democrats’ Claims Against FBI Whistleblower Steve Friend*, DAILY CALLER (Mar. 16, 2023), <https://dailycaller.com/2023/03/16/doj-inspector-general-office-whistleblower-corrects-democrat-claims/> (last accessed May 16, 2023).

²⁰⁶ Friend Interview at 30, 135.

²⁰⁷ See generally Democrat Report, *supra* note 173.

²⁰⁸ Friend Interview at 173.

²⁰⁹ *Id.* at 19, 173.

²¹⁰ Hill Interview at 125.

²¹¹ O’Boyle Interview at 65.

personal opinions.²¹² The Democrats used this information in their report to complain that each whistleblower “offered a wide range of personal opinions,” and suggest that the substance of their whistleblower disclosure was therefore discredited.²¹³

Democrats even pried into the private finances of the whistleblowers, hoping to malign them as having pecuniary motivations for disclosing FBI wrongdoing. The Democrats criticized Friend for receiving help from a former Trump Administration official in finding a job *after* the FBI all but forced him to resign.²¹⁴ Because Friend’s new employer supports the important work of the Select Subcommittee,²¹⁵ the Democrat report concluded that “[p]ublicity generated by the Committee’s investigation would benefit Friend in his new role by increasing the visibility of that organization” and, therefore, “Friend has a monetary incentive to continue pursuing his claims.”²¹⁶

Moreover, the Democrat report baselessly chastised Friend for accepting a monetary gift from a friendly organization during his FBI suspension. The Democrats implied that this gift colored the reliability of Friend’s testimony,²¹⁷ but they conveniently omitted that the FBI had denied Friend’s request to seek outside employment, leaving him to exhaust his accrued leave time, expend his personal savings, and eventually go without pay.²¹⁸ The Democrat report also failed to mention that Friend’s wife lost her job and, at the time, was recovering from a serious surgery.²¹⁹ When Friend again asked the FBI to seek outside employment and for his training records—so he could pursue other employment opportunities—he never heard back.²²⁰

In his testimony, Friend denied, clearly and unequivocally, that he was paid to come forward with his allegations against the FBI.²²¹ Friend testified that he never took money from a fundraising account that he promoted for suspended whistleblowers’ living expenses,²²² he denied making money from the articles he wrote,²²³ and he declared that he has not yet made any money off of a book he authored about his experience.²²⁴ Only after the FBI denied Friend’s requests for outside employment and only after Friend and his family survived 150 days of unpaid suspension did Friend take a job as a fellow with a conservative organization to provide for his family and “be a productive citizen.”²²⁵

Like Friend, O’Boyle experienced Democrat slander during and after his transcribed interview. The Democrat report insinuates that O’Boyle had a “financial connection” to a former Trump Administration official and his attorney “appeared to surprise his client with an

²¹² *Id.*

²¹³ *Id.*

²¹⁴ Democrat Report, *supra* note 173, at 7.

²¹⁵ *Id.* at 76.

²¹⁶ *Id.* at 34.

²¹⁷ *Id.* at 72.

²¹⁸ *Id.* at 32.

²¹⁹ Democrat Report, *supra* note 173, at 101.

²²⁰ *Id.* at 32-33.

²²¹ *Id.* at 73-77, 83.

²²² *Id.* at 76-77.

²²³ *Id.* at 82.

²²⁴ Democrat Report, *supra* note 173, at 82-83.

²²⁵ *Id.* at 43.

announcement that he was now representing O’Boyle *pro bono*.”²²⁶ Conveniently, the Democrat report omitted that O’Boyle spent over \$10,000 to retrieve his personal belongings from FBI storage after the FBI gave him the “run around” when it suspended him on his first day after a cross-country transfer.²²⁷

Notably, their attack on Hill’s credibility was so unfair that it prompted an apology from Democrats at the interview for impugning his credibility.²²⁸ Particularly, during Hill’s testimony to this Committee and Subcommittee, counsel for Democrats on the Committee and Subcommittee castigated Hill for some social media posts and podcast appearances in which Hill disseminated his political opinions based on his concerns that were apparent during his time at the FBI. After the Democrats’ counsel ceased the attacks, Hill testified:

Q. So, just before we close, the minority staff spent a lot of time going through various what I would call political opinions that you have posted since leaving the FBI. Is it fair to say that those opinions were based on the concerns that you had about what you saw while you were in the FBI as well as public reporting?

A. Yes. Nothing’s changed. I love the FBI. But, like with any parent, I mean—or if someone calls themselves your friend, if they’re not willing to say, “Hey, you need to adjust yourself,” they’re not your friend. If all they do is just say, “Hey, this is great, this is great, this is great, keep going the way you’re going,” they’re truly not your friend and they’re not a very good parent. Nothing’s changed. I want the FBI to be successful.

Q. So the minority staff also, in the first round of questioning, said that your statements on the podcast went to your claimed that they went to your credibility. I didn’t hear anything that suggested that you were dishonest in any way, in any form, anywhere, anytime. Is everything that you testified to today with regard to the facts accurate and truthful, to the best of your knowledge?

A. Regarding fact testimony, yes. Opinions are opinions, and, unfortunately, I probably gave too many of those.

[Minority Counsel]. And I should clarify. I did say “credibility.” I meant to say “bias.”

A. Huge difference.

²²⁶ *Id.* at 7.

²²⁷ O’Boyle Interview at 23.

²²⁸ Hill Interview at 147-48.

[Minority Counsel]. And I—yeah, I did not mean to impugn your credibility, and I do apologize.

A. I—for the record, I—quite frankly, I found it offensive.

[Minority Counsel]. I apologize.

A. I don't know if you've ever been subject to a full scope lifestyle poly, but it's—yeah. You went there.²²⁹

C. Democrats Deployed the Same Abusive Tactics to Attempt to Discredit Journalists Matt Taibbi and Michael Shellenberger.

The Democrat report exemplifies their tactics of personal destruction. These tactics were on full display during the Select Subcommittee's March 9, 2023, hearing about government censorship revealed by two journalists in the Twitter files. There, as they did when they accused the FBI whistleblowers of not being *real* whistleblowers, Democrats suggested that the journalists covering the Twitter Files—Matt Taibbi and Michael Shellenberger—were not *real* journalists, but merely “so-called journalists.”²³⁰

During her line of questioning at the hearing, Democrat Representative Debbie Wasserman Schultz told Taibbi, “Being a Republican witness today certainly cast[s] a cloud over your objectivity.”²³¹ This is no different from the attack Democrats lodged against the whistleblowers, telling the *New York Times* that by testifying to a Republican-led Committee, the whistleblowers “have engaged in partisan conduct that calls into question their credibility.”²³² Just as the Democrat report accused Friend and O'Boyle of receiving money from a conservative organization in order to shape their testimony, Democrat members asked Taibbi if he benefitted financially from exposing misconduct. During her questioning, Representative Wasserman Schultz admonished Taibbi:

Before the release of the emails . . . in August of last year, you had 661,000 Twitter followers. After the Twitter Files, your followers doubled, and now it's three times what it was last August. I imagine your Substack [r]eadership, which is a subscription, increased significantly because of the work you did for Elon Musk. Now, I'm not asking you to put a dollar figure on it, but it's quite obvious that you've profited from the Twitter Files. You hit the jackpot on that Vegas slot machine to which you referred. That's true, isn't it?²³³

²²⁹ *Id.*

²³⁰ *The Twitter Files Hearing Before the Select Subcomm. On the Weaponization of the Fed. Gov't*, 118th Cong. 8 (2023) (statement of Del. Stacey Plaskett).

²³¹ *Id.* at 33 (questioning from Rep. Debbie Wasserman Schultz).

²³² See Broadwater and Goldman, *supra* note 174.

²³³ *The Twitter Files Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't*, 118th Cong. 34-35 (2023) (questioning from Rep. Debbie Wasserman Schultz).

Taibbi denied the insinuation that his reporting was profit-motivated—calling it “a wash” between income generated and income spent on his reporting—and defended the integrity of his work.²³⁴

The startling Democrat attacks on the First Amendment continued when they pressed the journalists to reveal their sources for the information contained in the Twitter Files. They pressed Taibbi and Shellenberger:

Ms. Plaskett: And then who gave you access to these emails? Who was the individual that gave you permission to access the emails?

Mr. Taibbi: Well, the attribution from my story is sources at Twitter, and that’s what I’m going to refer to.

Ms. Plaskett: Okay. Did Mr. Musk contact you, Mr. Taibbi?

Mr. Taibbi: Again, the attribution from my story is sources at Twitter.

Ms. Plaskett: Mr. Shellenberger, did Mr. Musk contact you?

Mr. Shellenberger: Actually, no. I was brought in by my friend, Bari Weiss.²³⁵

Ms. Garcia: Mr. Taibbi, I want to follow up a little bit on the ranking member’s questions. When was the first time that Mr. Musk approached you about writing The Twitter Files?

Mr. Taibbi: Again, Congresswoman, that would –

Ms. Garcia: I just need a date, sir.

Mr. Taibbi: But I can’t give it to you, unfortunately, because this is a question of sourcing, and I don’t give up – I’m a journalist. I don’t reveal my sources.

Ms. Garcia: It’s not a question of sources. It’s a question of chronology.

²³⁴ *Id.*

²³⁵ *Id.* at 51 (questioning from Del. Stacey Plaskett).

- Mr. Taibbi: No. That's a question of sources.
- Ms. Garcia: Because you earlier said that someone had sent you to the internet, some message about whether or not you would be interested in some information.
- Mr. Taibbi: Yes. And I refer to that person as a source.
- Ms. Garcia: So you're not going to tell us when Musk first approached you?
- Mr. Taibbi: Again, Congresswoman, you're asking me to –
- Ms. Garcia: You can answer yes or no.
- Mr. Taibbi: You're asking a journalist to reveal a source.
- Ms. Garcia: So do you consider Mr. Musk to be the direct source of all of this?
- Mr. Taibbi: No. Now you're trying to get me to say that he is the source. I just can't answer your question about sources.
- Ms. Garcia: Well, he either is or he isn't. If you're telling me you can't answer because it's your source, well, then, the only logical conclusion is that he is, in fact, your source.²³⁶

Committee Democrats have opposed the Committee's critical oversight work since its inception. The conduct of Democrats in attacking brave FBI whistleblowers and intrepid investigative journalists speaks volumes to their motives. Although deeply disappointing, it is consistent with their promises to sabotage the Committee's work. As Leader Jeffries and Ranking Member Nadler promised: Democrats would fight our work "tooth and nail."²³⁷

From the outset of the 118th Congress, Democrats have reached new lows in their obstruction. They released nonpublic copies of the Committee's first subpoenas to the White House, which in turn provided them to *Punchbowl*. Committee Democrats were the source of the leak because only the Committee—and not any subpoena recipients—had possession of the versions of the subpoenas that later appeared in *Punchbowl*.²³⁸ Just weeks later, Democrats

²³⁶ *Id.* at 65-66 (questioning from Rep. Sylvia Garcia).

²³⁷ Rep. Hakeem Jeffries (@RepJeffries), Twitter.com (Jan. 11, 2023, 10:03 AM), <https://twitter.com/RepJeffries/status/1613189897237438467>; Press Release, Rep. Jerrold Nadler, Nadler Blasts Formation of New Partisan Select Subcommittee (Jan. 10, 2023).

²³⁸ See Max Cohen, *Punchbowl News PM: Inside Jordan's Subpoenas*, *Punchbowl News* (Feb. 3, 2023).

provided cherry-picked excerpts of transcripts of whistleblower interviews to *Rolling Stone* and *CNN* to preemptively discredit their testimony. The Democrats' tactics in their subsequent report and the hearing is more of the same.

A. The Actions of Committee Democrats Discourage Whistleblowing and Facilitate Citizens' Fear of Government.

Because the Committee Democrats' report outed FBI whistleblowers' identities and substance of their testimonies to the public, one whistleblower, Allen, approached the Committee on the condition that they could speak initially only in presence of Republicans. Regarding this choice, Allen testified:

While I have agreed to this voluntary transcribed interview to help the committee fulfill its constitutional oversight function, I have concerns about the ability of the committee to protect me from further retaliation and protect confidential information I share during the interview. I have seen news coverage where excerpts of other FBI whistleblower testimony to this committee has been selectively leaked to fuel deceptive political attacks on those who have cooperated and provided voluntary testimony. That naturally makes me reluctant to subject myself to the same abuse, and that is why I was not comfortable agreeing to testify in a private setting with the same staff who are responsible for the previous leak and smear campaign against other whistleblowers. I am comfortable testifying to the chairman's staff based on assurances that confidential information provided during this interview will not be released without my consent and authorization by the chairman.²³⁹

Democrats' behavior regarding their treatment of brave FBI whistleblowers is a disgrace and an affront to the service that these whistleblowers have provided to this country. It is obvious from whistleblowers' testimonies that the Democrats' actions have had their desired chilling effect on whistleblowers who wish to come forward to expose unlawful activities within the FBI.

²³⁹ Allen Interview at 5-6.

Conclusion

The FBI, under Director Christopher Wray and Attorney General Merrick Garland, is broken. The leadership at the FBI and Justice Department have weaponized federal law enforcement against everyday Americans, seeking to silence those who dare to have a different viewpoint. Whistleblowers play a vital role in identifying and rooting out waste, fraud, abuse, and mismanagement in the federal government. When they speak out against such abuses, federal law protects them from retaliation.²⁴⁰ If you are an FBI whistleblower, however, this is not the case. As detailed above, the brave agents who have testified to the Committee and Subcommittee have faced devastating retaliation from the agency for their protected disclosures, with such retaliation taking the form of indefinite suspensions without pay and being left homeless and without income by the country's once-preeminent law enforcement agency.

Meanwhile, whistleblower testimony highlights that the FBI's partisan leadership is currently engaging in a "purge" of agents who hold conservative political beliefs. Particularly, the testimony from Friend demonstrates the agency's blatant targeting and dismissal of conservatives within its ranks. In Friend's case, he was indefinitely suspended and had his security clearance suspended for simply asking why the FBI was unnecessarily using force to arrest individuals suspected of participating in the events at the U.S. Capitol on January 6, 2021. The agency's attacks on bold agents must cease, and this Committee and Select Subcommittee will consider legislation aimed to curb such attacks. Additionally, the matters concerning the FBI's treatment of O'Boyle, Friend, Hill, and Allen will be referred to the U.S. Office of Special Counsel and the Inspector General for further investigation.

The Committee's and Select Subcommittee's investigation into the weaponization of the federal law enforcement apparatus continues. Consistent with the charge to keep the House of Representatives informed of the oversight work, this interim report provides a summary of the whistleblower testimony received so far. The Committee and Select Subcommittee will continue to uncover facts to inform legislative reforms to protect civil liberties and rein in federal law enforcement.

²⁴⁰ 5 U.S.C. § 2303.



**THE FBI'S BREACH OF RELIGIOUS FREEDOM:
THE WEAPONIZATION OF LAW ENFORCEMENT AGAINST CATHOLIC
AMERICANS**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



December 4, 2023

EXECUTIVE SUMMARY

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been investigating the Federal Bureau of Investigation's (FBI) categorization of certain Catholic Americans as potential domestic terrorists. While the FBI claims it “does not categorize investigations as domestic terrorism based on the religious beliefs—to include Catholicism—of the subject involved,” an FBI-wide memorandum originating from the FBI's Richmond Field Office did just that.¹ Under the guise of tackling the threat of domestic terrorism, the memorandum painted certain “radical-traditionalist Catholics” (RTCs) as violent extremists and proposed opportunities for the FBI to infiltrate Catholic churches as a form of “threat mitigation.”² The FBI's Richmond memorandum is a startling reminder that Americans' civil liberties and core Constitutional rights must be vigorously guarded against government overreach, including in this case from an overzealous law enforcement agency.

In February 2023, the Committee began its oversight after whistleblower Kyle Seraphin revealed the existence of the Richmond memorandum in internal FBI systems.³ In April 2023, after the FBI failed to fully cooperate with the oversight, Chairman Jordan issued a subpoena to Director Christopher Wray, requesting documents related to the memorandum.⁴ The Committee and Select Subcommittee's oversight shows that the FBI abused its counterterrorism tools to target Catholic Americans as potential domestic terrorists. The Committee and Select Subcommittee discovered that the FBI relied on at least one undercover agent to develop its assessment and the FBI even proposed developing sources among the Catholic clergy and church leadership.⁵ Not only did the FBI propose to develop sources, but it already interviewed a priest and choir director affiliated with a Catholic church in Richmond, Virginia for the memorandum.⁶ Most concerning of all, without the disclosure of the brave whistleblower, the Richmond memorandum would still be operative in FBI systems, violating the religious liberties of millions of Catholic Americans.

From witness testimony and FBI internal documents, the Committee and Select Subcommittee have learned that there were errors at every step of the drafting, review, approval, and removal process of the memorandum. For example:

¹ Letter from Christopher Dunham, Acting Asst. Dir., Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, and Rep. Mike Johnson, Chairman, Subcomm. on the Const. and Limited Gov't at 1 (Mar. 23, 2023) (on file with the Comm.) [hereinafter March 23 Letter].

² Fed. Bureau of Investigation, U.S. Dep't of Justice, Domain Perspective, Interest of Racially or Ethnically Motivated Violent Extremists in Radical-Traditionalist Catholic Ideology Almost Certainly Presents New Mitigation Opportunities at FBI-HJC118-DP-000282 (Jan. 23, 2023) (on file with the Comm.) [hereinafter Catholic Memorandum].

³ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, and Rep. Mike Johnson, Chairman, Subcomm. on the Const. and Limited Gov't, to Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation (Feb. 16, 2023) [hereinafter February 16 Letter].

⁴ See Subpoena from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation (Apr. 10, 2023) [hereinafter April 10 Subpoena].

⁵ Catholic Memorandum at FBI-HJC118-DP-000282 and FBI-HJC118-DP-000285.

⁶ Whistleblower disclosure to Committee.

- The documents received pursuant to the Committee’s subpoena show there was no legitimate basis for the memorandum to insert federal law enforcement into Catholic houses of worship.
- The basis for the Richmond memorandum relied on a single investigation in the Richmond Field Office’s area of responsibility in which the subject “self-described” as a “radical-traditionalist Catholic” (RTC).⁷ However, FBI employees could not define the meaning of an RTC when preparing, editing, or reviewing the memorandum. Even so, this single investigation became the basis for an FBI-wide memorandum warning about the dangers of “radical” Catholics.
- Whistleblower disclosures reveal that the FBI interviewed a priest and choir director affiliated with a Catholic church in Richmond, Virginia while preparing the memorandum to inform on the parishioner under investigation.⁸
- In addition to the investigation in Virginia, FBI Richmond relied on reporting from other field offices across the country, including FBI Los Angeles, FBI Milwaukee, and FBI Portland in making its assessment.⁹
- The two FBI employees who co-authored the memorandum later told FBI internal investigators that they knew the sources cited in the memorandum had a political bias—sources including the Southern Poverty Law Center, *Salon*, and *The Atlantic*.¹⁰
- The documents received pursuant to the Committee’s subpoena show that the FBI singled out Americans who are pro-life, pro-family, and support the biological basis for sex and gender distinction as potential domestic terrorists. The memorandum recognized “the run-up to the next general election cycle”¹¹ as a key time frame and cited the *Dobbs v. Jackson Women’s Health Organization* decision that overturned *Roe v. Wade* as a flash point.
- Without considerable criticism in the wake of the disclosure of the memorandum, the document would have remained in an FBI-wide system. At the time of the memorandum’s disclosure, FBI officials were discussing turning the memorandum into an external, public-facing document highlighting the threats of “radical” Catholics. Most concerning, FBI Richmond still desires to convey this information to other field offices about “radical-traditionalist Catholics.”¹²

⁷ Inspection Div., Fed. Bureau of Investigation, U.S. Dep’t of Justice, *Strategic Review Report: Richmond Field Office – Domain Perspective Strategic Review* at FBI-HJC118-DP-000294 (2023) (on file with the Comm.) [hereinafter Strategic Review Report].

⁸ Whistleblower disclosure to Committee.

⁹ Strategic Review Report at FBI-HJC118-DP-000297.

¹⁰ *Id.* at FBI-HJC118-DP-000298.

¹¹ Catholic Memorandum at FBI-HJC118-DP-000281 – FBI-HJC118-DP-000282.

¹² Transcribed Interview with Stanley Meador, Special Agent in Charge, Fed. Bureau of Investigation at 115-116 (Aug 24, 2023) (on file with the Comm.) [hereinafter Meador Interview].

- FBI Richmond’s senior leadership saw the memorandum as an opportunity to insert federal law enforcement into places of worship and support outreach efforts to the Diocese of Richmond and other Catholic parishes.¹³
- Following public criticism about the memorandum, FBI Richmond’s Special Agent in Charge Stanley Meador met with members of the clergy, including the Most Reverend Barry Knestout, Bishop of the Diocese of Richmond, and a Cardinal of the Catholic Church to mend the FBI’s relationship with the Catholic community.
- Whistleblower disclosures to the Committee further reveal that the memorandum was accessible to other field offices across the country. However, the FBI still has no idea how many FBI employees accessed the memorandum before its removal and cannot confirm whether any outreach occurred to Catholic parishes as a result of the memorandum.

The Committee on the Judiciary, through and with its Select Subcommittee on the Weaponization of the Federal Government, is charged with investigating “violations of the civil liberties of citizens of the United States.”¹⁴ This interim staff report fulfills the ongoing obligation to identify and report on instances of the weaponization of the federal government—here, the FBI’s mishandling of domestic violent extremism investigations against Catholic Americans exercising their First Amendment rights. While the documents and information received to date help to better understand what transpired, they do not tell the whole story. The Committee and the Select Subcommittee will continue to pursue the relevant facts to inform legislative reforms and to protect American civil liberties from government overreach.

¹³ Catholic Memorandum at FBI-HJC118-DP-000286.

¹⁴ H. Res. 12, 118th Cong. § 1(b)(D) (2023).

TABLE OF CONTENTS

Executive Summary 1

Table of Contents 4

Background 5

New Information about the FBI’s Targeting of Catholic Americans 10

 I. The FBI’s own internal review identified errors at every step of the drafting, review, and approval of Richmond’s Catholic “intelligence product.” 10

 II. Without widespread criticism from other agents and public reporting about the Richmond memorandum, the document would have remained in FBI systems. 19

 III. SAC Meador met with several members of the clergy to mend the FBI’s relationship with the Catholic community. 24

Conclusion 29

BACKGROUND

On January 23, 2023, the FBI's Richmond Field Office published an eleven-page document, known as a domain perspective, that linked “racially or ethnically motivated violent extremists” (RMVEs) with individuals who hold a “radical-traditionalist Catholic” (RTC) ideology.¹⁵ In this memorandum, the FBI purported to distinguish what it called “traditional Catholics” from the RTC adherents, whom the FBI characterized as embracing “anti-Semitic, anti-immigrant, anti-LGBTQ, and white supremacist ideology.”¹⁶ The FBI identified certain public policy issues—such as conservative stances on immigration, affirmative action, and life issues—that it believed would “catalyz[e]” RTC adherents.¹⁷ In addition to attempting to separate and categorize Catholic Americans based on theological distinctions, the FBI underscored the political nature of its actions: “FBI Richmond assesses RMVE interest in RTCs is likely to increase over the next 12 or 24 months in the run-up to the next general election cycle.”¹⁸

The memorandum cited biased and partisan sources, including the Southern Poverty Law Center (SPLC), *Salon*, and *The Atlantic*, to support its assessment.¹⁹ For example, the SPLC misleadingly defines RTCs as “the largest single group of serious antisemites in America” and claims to have identified nine RTC “hate groups” across the United States.²⁰ The SPLC also identifies the broad term “Christian identity” as a hate group—a term that could arguably encompass millions of Americans with sincerely held religious beliefs.²¹ In addition, the SPLC routinely maligns several mainstream conservative and religious organizations as “hate” groups, simply because the SPLC disagrees with their views.²² The fact that the FBI would accept and circulate the SPLC’s partisan spin is highly concerning and undercuts the FBI’s assertion that it is unbiased and politically neutral.

On February 8, 2023, whistleblower Kyle Seraphin published a redacted version of the memorandum, condemning its partisan content.²³ The following day, news outlets immediately began reporting on the memorandum and its dangerous effect on protected First Amendment activity.²⁴ Virginia Attorney General Jason Miyares and 19 other state attorneys general even

¹⁵ Catholic Memorandum at FBI-HJC118-DP-000281. A Domain Perspective is “an operational or strategic level product that focuses on how a shift in, or new development related to, an environmental variable (EV) or EVs may affect threat(s) or the FBI’s effort to mitigate those threats” at FBI-HJC-000001 (on file with the Comm.).

¹⁶ *Id.*

¹⁷ *Id.* at FBI-HJC118-DP-000284.

¹⁸ *Id.* at FBI-HJC118-DP-000281 – FBI-HJC118-DP-000282.

¹⁹ *Id.* at FBI-HJC118-DP-000291.

²⁰ Southern Poverty Law Center, Radical Traditional Catholicism, <https://www.splcenter.org/fighting-hate/extremist-files/ideology/radical-traditional-catholicism> (last visited September 19, 2023).

²¹ *Id.*

²² See Susan Ferrechio, *SPLC finds fewer hate groups but still targets evangelicals, conservatives as haters*, WASH. TIMES (Mar. 10, 2022).

²³ Kyle Seraphin, *The FBI Doubles Down on Christians and White Supremacy in 2023*, UNCOVERDC (Feb. 8, 2023), <https://www.uncoverdc.com/2023/02/08/the-fbi-doubles-down-on-christians-and-white-supremacy-in-2023/>.

²⁴ See e.g. Tyler Arnold and Joe Bukuras, *FBI retracts leaked document orchestrating investigation of Catholics*, CATHOLIC NEWS AGENCY (Feb. 9, 2023); Evita Duffy, *FBI Retracts Memo Labeling Traditional Catholics ‘Violent White Supremacists,’ Pushing Infiltration Of Christian Communities*, THE FEDERALIST (Feb. 9, 2023); Michael Katz, *FBI Retracts Internal Memo Targeting Traditional Catholic Ideology*, NEWSMAX (Feb. 9, 2023); Kayla

wrote a letter to Attorney General Garland and FBI Director Wray calling the memorandum “un-American and unconstitutional.”²⁵ Another whistleblower further told the Committee that the memorandum was available to FBI employees in field offices across the country, and many of these employees were “uniformly disappointed” that the memorandum was published in the first place.²⁶ Not only did these FBI employees recognize the memorandum’s clear constitutional breach, but they also feared that the document could have potentially served as the basis for future intelligence products.²⁷



In the wake of widespread criticism about the memorandum, the FBI withdrew the memorandum and blamed the Richmond Field Office for its creation and dissemination. On February 9, 2023, the FBI released a public statement to supplement its retraction of the memorandum:

While our standard practice is to not comment on specific intelligence products, this particular field office product—disseminated only within the FBI—regarding racially or ethnically motivated violent extremism does not meet the exacting standards of the FBI. Upon learning of the document, FBI Headquarters quickly began taking action to remove the document from FBI systems and conduct a review of the basis for the document. The

Bailey, *FBI labeling Catholics as possible violent extremists is an excuse to oppress 'political enemies': Evita Duffy*, FOX NEWS (Feb. 12, 2023).

²⁵ Letter from Hon. Jason Miyares, Att’y Gen. of Va., et al., to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Justice and Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation (Feb. 10, 2023).

²⁶ Whistleblower disclosure to Committee.

²⁷ *Id.*

FBI is committed to sound analytic tradecraft and to investigating and preventing acts of violence and other crimes while upholding the constitutional rights of all Americans and will never conduct investigative activities or open an investigation based solely on First Amendment protected activity.²⁸

In response to these revelations, the Committee and Select Subcommittee began oversight into how the FBI could allow such a memorandum to be prepared, reviewed, approved, and disseminated. Although the FBI claims that it “will never conduct investigative activities or open an investigation based solely on First Amendment protected activity,” this memorandum itself is proof that the FBI has done just that, using taxpayer dollars. The FBI’s intrusion on Americans’ First Amendment rights demands that the Committee and Select Subcommittee conduct oversight into the circumstances of the memorandum’s creation and distribution, and to consider potential legislative reforms to ensure the FBI upholds the First Amendment.

Accordingly, on February 16, 2023, the Committee wrote to FBI Director Wray requesting documents and information regarding the FBI’s targeting of a set of Catholic Americans for their religious beliefs.²⁹ After receiving no response, the Committee sent a second letter on March 20, 2023.³⁰ On March 23, 2023, the Committee received a partial response consisting of only 18 pages—many with significant redactions—that prevented the Committee and Select Subcommittee from fully assessing the content and context of the documents.³¹

From this limited production, however, it was clear that the FBI, relying on information derived from at least one undercover employee, sought to use local religious organizations as “new avenues for tripwire and source development.”³² For example, in a section of the memorandum entitled “Opportunities,” the FBI wrote:

In addition to [redaction], engage in outreach to the leadership of other [Society of Saint Pius X (SSPX)] chapels in the FBI Richmond [area of responsibility] to sensitize these congregations to the warning signs of radicalization and **enlist their assistance to serve as suspicious activity tripwires.**³³

The FBI similarly noted two other opportunities to engage in outreach with “mainline Catholic parishes,” including St. Joseph Parish leadership and the local “diocesan leadership[.]”³⁴ The FBI also expressed an interest in “leverag[ing] existing sources and/or initiat[ing] Type 5 Assessments to develop new sources with the placement and access” to report on suspicious activity.³⁵

²⁸ Arnold and Bukuras, *supra* note 24.

²⁹ See February 16 Letter.

³⁰ See March 23 Letter.

³¹ *Id.*

³² Catholic Memorandum at FBI-HJC118-DP-000281.

³³ *Id.* at FBI-HJC118-DP-000285 (emphasis added).

³⁴ *Id.* at FBI-HJC118-DP-000286.

³⁵ *Id.*

Although the FBI claimed in its response to the Committee and Select Subcommittee to have “numerous” and “rigorous” policies to protect First Amendment rights,³⁶ the memorandum was reviewed and approved by two senior intelligence analysts and the Chief Division Counsel—the FBI’s top lawyer in the Richmond Field Office.³⁷ There are no indications that any FBI employees in Richmond had any concern with the content of the memorandum until after it was disclosed publicly.

This shocking, but limited, information reinforced the need for all material responsive to the Committee’s requests. To that end, on April 10, 2023, Chairman Jordan issued a subpoena to compel Director Wray to produce additional material regarding the memorandum.³⁸ On April 28, 2023—the day the FBI was due to comply in full with the subpoena—the Bureau produced an additional 248 pages of documents in response to the subpoena.³⁹

On July 25, 2023, the FBI produced a version of the memorandum with fewer redactions than the two previous versions it had produced for the Committee.⁴⁰ This new version showed that the FBI’s actions were not limited to “a single field office” as Director Wray testified to the Committee on July 12, 2023.⁴¹ Rather, the FBI relied on reporting from field offices around the country, including FBI Los Angeles and FBI Milwaukee, and in “[c]oordinat[ion] with” FBI Portland in making the assessment that led to the creation of the memorandum.⁴²

Since then, the Committee has received additional information about the genesis, review, and approval of the Richmond memorandum. On August 22, 2023, the Committee received a briefing from the FBI’s Inspection Division (INSD) about the FBI’s internal review of the memorandum. Following the briefing, the FBI produced another 31 pages of documents, including a redacted version of its report findings and another less-redacted version of the memorandum.⁴³ The Committee also conducted a transcribed interview with the Special Agent in Charge of the Richmond Field Office, Stanley Meador. Two months later, on October 27, the FBI produced an additional 261 pages of documents in response to the subpoena.⁴⁴

While this information sheds some light on how the FBI could abuse civil liberties so egregiously, the FBI’s responses remain deficient. The FBI has failed to produce the names of the FBI employees who were involved in drafting, reviewing, approving, or disseminating the

³⁶ March 23 Letter at 2.

³⁷ Catholic Memorandum at FBI-HJC118-DP-000286.

³⁸ See April 10 Subpoena.

³⁹ See Letter from Mr. Christopher Dunham, Acting Asst. Dir., Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Apr. 28, 2023) (on file with the Comm.).

⁴⁰ See Letter from Christopher Dunham Acting Asst. Dir., Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (July 25, 2023) (on file with the Comm.). This letter and production were in response to the Committee’s letter to Director Wray dated July 17, 2023, noting that the Committee may seek to enforce the subpoena through contempt proceedings.

⁴¹ *Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 118th Cong. at 68 (2023) (testimony of Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation) (on file with the Comm.).

⁴² Catholic Memorandum at FBI-HJC118-DP-000283 and FBI-HJC118-DP-000286.

⁴³ See Letter from Christopher Dunham, Acting Asst. Dir., Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 23, 2023) (on file with the Comm.).

⁴⁴ See Letter from Mr. Christopher Dunham, Acting Asst. Dir., Fed. Bureau of Investigation, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Oct. 27, 2023) (on file with the Comm.).

memorandum. Furthermore, the FBI's internal review is not a substitute for the Committee's independent and constitutional duty to oversee the FBI and to ensure the First Amendment's guarantee of the free exercise of religion is protected from government overreach.

NEW INFORMATION ABOUT THE FBI’S TARGETING OF CATHOLIC AMERICANS

The Committee and Select Subcommittee’s oversight reveals how the FBI abused its federal law-enforcement resources to single out a specific sect of Catholic Americans because of their religious beliefs. The documents and testimony recently obtained shed new light on the genesis, review, and approval of the Richmond memorandum that equated “racially or ethnically motivated violent extremists” (RMVEs) with persons holding a “radical-traditionalist Catholic” (RTC) ideology. It is evident that the FBI violated the First Amendment, and without widespread criticism, the memorandum may have remained in an FBI-wide system indefinitely.

I. The FBI’s own internal review identified errors at every step of the drafting, review, and approval of Richmond’s Catholic “intelligence product.”

Even after the Committee’s subpoena, the FBI neglected to fulfill the Committee’s requests, and instead delayed its compliance until the conclusion of an internal review spearheaded by the FBI’s Inspection Division (INSD). Several months later, the Committee finally received a briefing from the INSD, as well as the FBI’s Directorate of Intelligence (DI) and the Counterterrorism Division (CTD), regarding its internal review of the Richmond memorandum. As a part of this internal review, the FBI conducted 26 interviews with employees involved in drafting, reviewing, and approving the memorandum. Following the briefing, the FBI made two additional document productions, including a redacted version of its internal review report, which provides additional details about the creation of the memorandum, and email communications between the co-authors, peer reviewers, and supervisory analysts before the memorandum was published. In addition, on August 24, 2022, the Committee conducted an interview with Special Agent in Charge (SAC) Stanley Meador regarding the memorandum.

A. The two experienced Intelligence Analysts who authored the memorandum knew they were citing unreliable sources with a political bias.

The FBI’s internal review found that the idea of the memorandum was first conceived of in mid-September 2022 by two Richmond-based Intelligence Analysts (IA), whose names are redacted in the FBI’s internal report. At that time, the analysts started to discuss potential intelligence products to support Richmond’s outreach efforts in conjunction with the Richmond Field Office’s Strategic Plan for the fiscal year. The strategic plan for the year recognized “RMVE [racially or ethnically motivated violent extremists] as a DT [domestic terrorism] National Threat Priority” and included the objective of “strengthen[ing] [liaison] relationships through outreach.”⁴⁵

The analysts relied on a single investigation as an “opportunity” for FBI Richmond to conduct outreach with Catholic parishes in the Richmond area of responsibility.⁴⁶ The subject under investigation was “Richmond’s highest priority DT [domestic terrorism] subject” and was ranked likely to mobilize to violence.⁴⁷ The analysts examined the subject’s social media, where

⁴⁵ Strategic Review Report at FBI-HJC118-DP-000296.

⁴⁶ *Id.*

⁴⁷ *Id.*

he “self-identified” as a “radical traditionalist Catholic Clerical Fascist.”⁴⁸ According to the interviews conducted during the FBI’s internal review, this social media examination is how the analysts learned of the term “RTC”—the terminology they maintained in the subsequent memorandum without fully understanding its meaning.⁴⁹

A whistleblower also revealed that the FBI interviewed a priest and choir director of an SSPX-affiliated church in Richmond, Virginia.⁵⁰ The interviews appear to have occurred in November and December 2022—the same time the analysts started drafting the memorandum.⁵¹ This information, which the FBI has refused to disclose, confirms that the FBI directly communicated with Catholic clergy and staff about parishioners practicing their faith.

From November to December 2022, the analysts began researching and drafting the Richmond memorandum. On November 11, 2022, one analyst created a working document in an online collaborative platform for the Richmond Field Office.⁵² Meanwhile, the other analyst focused on finding “operational intelligence” reporting from other field offices, where he identified similar cases to the Richmond investigation in both the Milwaukee Field Office and the Portland Field Office—even though the Portland investigation was closed because the subject was recently deceased.⁵³ On December 30, 2022, the analyst contacted the case managers at FBI Milwaukee to confirm the details of its investigation.⁵⁴ Four days later, the analyst also reached out to the case managers at FBI Portland to coordinate an “evidence bullet point” that was eventually included in the final Richmond memorandum.⁵⁵ The FBI’s internal review maintained that “the agents and analysts in Milwaukee and Portland only reviewed the bullet points associated with their respective investigation and did not review or contribute to the broader [memorandum].”⁵⁶ To date, however, the FBI has been unable to confirm whether the investigations in Milwaukee and Portland also included self-described RTC subjects.⁵⁷ Instead, it appears that the Richmond analysts adopted the RTC term after use by a criminal in one case occurring in Richmond’s area of responsibility.

While one analyst led the effort to find operational intelligence from other field offices, the other analyst focused on gathering open-source information that would inform the memorandum’s narrative.⁵⁸ As previously known from public reporting on the memorandum, the analyst utilized sources such as the Southern Poverty Law Center (SPLC), *Salon*, and *The Atlantic*.⁵⁹ During an interview as part of the FBI’s internal review, one of the analysts even acknowledged that the “SPLC was known to have a political bias.”⁶⁰ Yet, the analysts did not

⁴⁸ *Id.* at FBI-HJC118-DP-000297.

⁴⁹ *Id.*

⁵⁰ Whistleblower disclosure to Committee.

⁵¹ *Id.*

⁵² Strategic Review Report at FBI-HJC118-DP-000302.

⁵³ *Id.* at FBI-HJC118-DP-000297.

⁵⁴ See *id.*; See also FBI-HJC118-DP-000303.

⁵⁵ *Id.* at FBI-HJC118-DP-000303.

⁵⁶ *Id.* at FBI-HJC118-DP-000297.

⁵⁷ Briefing with Fed. Bureau of Investigation before the H. Comm. on the Judiciary, 118th Cong. (Aug. 22, 2023) [hereinafter FBI Briefing].

⁵⁸ Strategic Review Report at FBI-HJC118-DP-000298.

⁵⁹ Catholic Memorandum at FBI-HJC118-DP-000291.

⁶⁰ Strategic Review Report at FBI-HJC118-DP-000298.

provide any caveats about the bias or credibility of the source in the memorandum. Instead, they wrote in the memorandum that “FBI Richmond makes this assessment *with high confidence*.”⁶¹ In other words, the analysts cited and relied on the SPLC, *Salon*, and *The Atlantic* knowing the sources were politically biased to support a false narrative.⁶²

During his transcribed interview with the Committee, SAC Meador testified about the experience levels of the analysts who co-authored the Richmond memorandum. Meador revealed that the primary author has been with the FBI for about 18 years, while the other analyst has been with the FBI for over 20 years. Meador testified:

Q: And how long had each of the intelligence analysts worked at Richmond at the time of the drafting of the—

A: I have general—I don’t know the specific in Richmond, but I know their – their approximate tenure in doing the job.

Q: Ten years in doing the—

A: Oh, no, no. The primary author is, I believe, 18 years, 18. The coauthor is—he may be upwards 20 plus years, maybe even as much as 25.

Q: And would they be considered senior intelligence analysts or just regular intelligence analysts?

A: . . . I don’t think we have a classification. We have supervisory intelligence analysts, but they’re—they’d be senior, the tenure they’d been doing it, yeah.⁶³

It is concerning that these “senior” analysts—having done the job for 18 and over 20 years, respectively—could produce a memorandum with such grave civil liberties concerns. Yet, Meador testified that the analysts are still responsible for drafting intelligence products.⁶⁴ If these seasoned analysts do not understand the parameters of the First Amendment, it raises concerns about the FBI’s training of its analysts and whether other such unconstitutional intelligence products exist on FBI systems—a question that the FBI could not answer to the Committee.⁶⁵

⁶¹ Catholic Memorandum at FBI-HJC118-DP-000281 (emphasis added).

⁶² Strategic Review Report at FBI-HJC118-DP-000298.

⁶³ Meador Interview at 64.

⁶⁴ *Id.* at 66.

⁶⁵ FBI Briefing.

B. The memorandum was peer-reviewed by other Richmond Field Office employees, who did not have any concerns about the substance of the memorandum.

During the FBI’s internal review, it found that FBI Richmond had no formal peer review process for intelligence products.⁶⁶ The general practice in the field office was to have other senior analysts review a draft of the document before the Supervisory Intelligence Analyst (SIA) reviewed it for final approval.⁶⁷ The FBI Richmond’s careless review process resulted in a prejudiced memorandum despite being reviewed by multiple employees in leadership positions. To date, these analysts who peer-reviewed the memorandum are still responsible for creating and peer-reviewing intelligence products.⁶⁸

When the draft of the memorandum was complete, the analysts requested that two other analysts—one familiar with the issue and one senior analyst—peer review the memorandum. This peer-review process occurred on January 12, 2023.⁶⁹ In particular, the primary authoring analyst specifically asked another analyst, “who had completed two years of Catholic seminary,” to review the memorandum for proper usage of “unique Catholic terms.”⁷⁰ In his email response to the co-authoring analysts, the peer reviewer wrote, “[g]reat product, I really enjoyed the read!”⁷¹ The peer-reviewing analyst did not comment on the substance of the memorandum and only suggested “some items” for clarification.⁷² Meador testified to the Committee that this analyst had worked at FBI Richmond for less than two years.⁷³

In addition, the co-authors also requested that a senior intelligence analyst peer review the memorandum. Although the senior analyst was trained as an “Analytical Tradecraft Reviewer,” bound by the Office of the Directorate of Intelligence’s (ODNI) Analytic Tradecraft Standards (ATS), she only edited the memorandum for “mechanical” and “structural” edits.⁷⁴ According to the FBI’s report, the senior reviewer “did not conduct a tradecraft review or edit for substance because the [memorandum] was not an external product,” which purportedly requires intelligence products to undergo more scrutiny.⁷⁵ Therefore, the memorandum contained issues regarding the “readability, main assessment, sourcing, assumptions, perspective, analysis, and outlook,” which the FBI asserted would have all been avoided by conducting a “tradecraft review.”⁷⁶ Meador testified to the Committee that this senior analyst who reviewed the memorandum had worked at FBI Richmond for approximately 18 years.⁷⁷ Perhaps most

⁶⁶ Strategic Review Report at FBI-HJC118-DP-000298.

⁶⁷ *Id.*

⁶⁸ Meador Interview at 70.

⁶⁹ Strategic Review Report at FBI-HJC118-DP-000298 and FBI-HJC118-DP-000303.

⁷⁰ *Id.* at FBI-HJC118-DP-000298.

⁷¹ FBI-HJC118-DP-000330.

⁷² *Id.*

⁷³ Meador Interview at 69.

⁷⁴ Strategic Review Report at FBI-HJC118-DP-000298. Analytic Tradecraft Standards “govern the production and evaluation of analytic products” and “articulates the responsibility of intelligence analysts to strive for excellence, integrity, and rigor in their thinking and work practices....” Office of the Director of National Intelligence, Analytic Standards, Intelligence Community Directive 203 (Jan. 2, 2015).

⁷⁵ *Id.*

⁷⁶ *Id.* at FBI-HJC118-DP-000309.

⁷⁷ Meador Interview at 64.

concerning, the FBI found that no Richmond employee reviewed the memorandum for substance or tradecraft standards, especially Meador.⁷⁸ In fact, Meador testified to the Committee that he does “not recall in [his] career . . . ever having seen . . . analytic tradecraft standards.”⁷⁹

The rubber-stamp peer review process does not appear to be limited to the Richmond Field Office. In fact, the FBI has no “delineated” roles and responsibilities in its policy that require intelligence products to undergo a more scrutinizing peer review process.⁸⁰ According to Meador, “some offices have [review processes] and “some don’t.”⁸¹ So when FBI Headquarters identified issues with the memorandum, Meador requested that a supervisory analyst, who was ultimately responsible for approving the memorandum, to “start finding those peer-review processes throughout the Bureau so that [FBI Richmond] could formalize a peer review process.”⁸² The fact that there is no instituted peer-review process for intelligence products that drive federal law-enforcement investigations raises the question of how many other unconstitutional intelligence products the FBI has allowed to remain in its systems. Even the FBI briefers to the Committee could not answer this question as they admitted that the FBI has not conducted an internal review of any other existing intelligence products in FBI systems.⁸³

C. FBI Richmond’s top lawyer had no concerns with the memorandum and did not believe its content was unconstitutional.

On January 12, 2023, the authoring analysts requested legal review from Richmond’s Chief Division Counsel (CDC)—the field office’s top lawyer tasked with providing legal advice and services. Although the CDC had been with the Richmond Field Office for over 15 years, the FBI’s report found that he had never reviewed a domain perspective in his entire career.⁸⁴ This revelation is antithetical to internal FBI documents indicating that CDCs are the primary resource for reviewing intelligence products, especially if they contain “certain legally sensitive categories of information.”⁸⁵ Given that FBI Richmond’s top lawyer did not see the memorandum as a violation of religious freedom, there seem to be serious shortcomings with respect to how the FBI institutionally views constitutional rights.

A day after receiving the draft memorandum, the CDC concluded his analysis and indicated that the memorandum “look[ed] good” and that there were “no legal issues” with the content.⁸⁶ The CDC’s main suggestion was that the final product should explicitly include a “First Amendment legal caveat.”⁸⁷ Other than that, the CDC had no other concerns with the document so long as the memorandum “remained an internal product”—the same perception

⁷⁸ Strategic Review Report at FBI-HJC118-DP-000298.

⁷⁹ Meador Interview at 33.

⁸⁰ *Id.* at 32.

⁸¹ *Id.* at 66.

⁸² *Id.* at 33.

⁸³ FBI Briefing.

⁸⁴ Meador Interview at 73; *see also* Strategic Review Report at FBI-HJC118-DP-000298.

⁸⁵ Fed. Bureau of Investigation, U.S. Dep’t of Justice, Domain Perspective Guidance at FBI-HJC118-DP-000005 (Oct. 10, 2022) (on file with the Comm.).

⁸⁶ FBI-HJC118-DP-000326.

⁸⁷ Strategic Review Report at FBI-HJC118-DP-000298.

held by the peer-reviewing senior analyst.⁸⁸ In this same email thread, the author thanked the CDC for his suggestions and replied, “[t]his product is internal, however, we plan to write an external product and will follow your guidance.”⁸⁹ The CDC also “did not review the terminology and deferred to the SIAs [supervisory intelligence analysts] to use accurate terminology.”⁹⁰ Ultimately, the FBI report found that the CDC did not believe “the information in the [memorandum] violated the law” and “was not based solely on First Amendment protected information” even after hearing the plans to make the document into an external product.⁹¹

During his transcribed interview, SAC Meador testified that following public reporting of the memorandum, he had a conversation with the CDC about the CDC’s legal review of the document.⁹² Meador testified that he told the CDC to use “more care and caution” when it comes to reviewing intelligence products, especially when First Amendment rights are on the line.⁹³ Meador further testified that before the memorandum, he never had any previous concerns about the CDC’s performance.⁹⁴ To this date, the CDC still maintains responsibility for reviewing intelligence products originating from the Richmond Field Office.⁹⁵

D. Two supervisory analysts approved the memorandum without providing feedback or making any substantive edits.

Following the CDC’s review, the authoring analysts requested approval of the memorandum from two supervisory analysts. On January 17, 2023, the authoring analysts provided the final draft to the supervisory analyst who oversees all of FBI Richmond’s intelligence analysts.⁹⁶ Meador testified to the Committee that this supervisory analyst had worked at FBI Richmond for approximately three years and is still approving intelligence products.⁹⁷ This supervisory analyst made “[m]ostly minor word changes and suggestions” to the draft memorandum before forwarding it to another supervisory analyst, known as the Intelligence Program Coordinator, who oversees the Richmond Field Office’s intelligence program, for final approval on January 20, 2023.⁹⁸

On January 20, 2023, the final supervisory analyst reviewed and approved the memorandum and opined the memorandum was “[n]icely done.”⁹⁹ Although this supervisory analyst holds a “fairly senior”¹⁰⁰ position at FBI Richmond, “he did not know where the term ‘RTC’ originated,” but he still maintained the terminology.¹⁰¹ Although the CDC indicated that

⁸⁸ *Id.*

⁸⁹ FBI-HJC118-DP-000324.

⁹⁰ Strategic Review Report at FBI-HJC118-DP-000298.

⁹¹ *Id.*

⁹² Meador Interview at 76.

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.* at 73-74

⁹⁶ Strategic Review Report at FBI-HJC118-DP-000303.

⁹⁷ Meador Interview at 28.

⁹⁸ FBI-HJC118-DP-000357.

⁹⁹ FBI-HJC118-DP-000370.

¹⁰⁰ Meador Interview at 26.

¹⁰¹ Strategic Review Report at FBI-HJC118-DP-000299.

he deferred the accuracy of the memorandum's terminology to the final approvers, the supervisory intelligence analysts also apparently did not try to correct the biased terminology.¹⁰²

FBI Richmond published the memorandum on Sentinel—the FBI's official record keeping system—on January 24, 2023, and then added the memorandum to its online collaborative platform on January 26, 2023.¹⁰³ That same day, a redacted employee informed SAC Meador and eleven other employees about the new product. The individual stated:

FYI A new [Richmond] Domain Perspective posted to the [online collaborative platform] . . . IAs [redacted] and [redacted] published the DP titled, “. . . Interest of Racially or Ethnically Motivated Violent Extremists in Radical-Traditionalist Catholic Ideology Almost Certainly Presents New Mitigation Opportunities.” Your feedback is appreciated.¹⁰⁴

While the FBI claims that all pre-existing information concerning the Richmond memorandum has been permanently deleted, the FBI was able to retrieve a comment from SAC Meador in response to this notification. In addition, despite its affirmation that documents referring to the memorandum had been deleted, the FBI produced more relevant documents in its most recent production.

E. SAC Meador viewed the memorandum as an opportunity to conduct outreach with the Diocese of Richmond and Catholic parishes.

A week after receiving an email notification about the memorandum, SAC Meador provided feedback about the document through FBI Richmond's internal collaborative site. On February 3, 2023, Meador made the following comment:

Appreciate the perspective, especially after what was gleaned from the [redacted] investigation. I plan to engage in additional conversation regarding engagement at the Dioceses of Richmond. I think there is an opportunity here to consider putting several folks in a room (from different locations) to have this conversation.¹⁰⁵

During his transcribed interview with the Committee, Meador testified that the investigation he referred to in his comment was the same Richmond case referenced in the memorandum.¹⁰⁶ He testified that he was familiar with that specific Richmond investigation because it was an “extremely” high-profile case.¹⁰⁷ According to the FBI, Meador's comment is the only one that exists in response to the Richmond memorandum because all references to the document were

¹⁰² *Id.* at FBI-HJC118-DP-000298.

¹⁰³ *Id.* at FBI-HJC118-DP-000299.

¹⁰⁴ FBI-HJC118-DP-000280 (on file with the Comm.).

¹⁰⁵ FBI-HJC118-DP-000279 (on file with the Comm.).

¹⁰⁶ Meador Interview at 80.

¹⁰⁷ *Id.* at 13.

removed from FBI systems.¹⁰⁸ The FBI explicitly maintained “it is unknown if any other feedback was provided on the [memorandum].”¹⁰⁹

During his transcribed interview, Meador testified that he did not read the memorandum in its entirety but wanted to show appreciation for his employees’ work.¹¹⁰ Meador testified that when he saw the memorandum for the first time, he “remember[ed] pulling it up and skimming some” of the document.¹¹¹ In addition, Meador testified that he made the comment because “one of the important things in the FBI is to have executive management engagement with the intelligence program.”¹¹² He explained further:

[O]nce a document has been approved and published, the supervisors will send . . . an email to supervisors and command staff letting us know a new product has been posted in the [online collaborative platform] For me, what’s important is that periodically I go in there so that my intelligence team knows that I pay attention and I care about their work, I appreciate their perspective.¹¹³

Thus, from his testimony, it appears that Meador did not perform any due diligence on the memorandum, but instead commented as a way of showing engagement with his team.

During his transcribed interview, Meador provided more detail about what he meant in his comment, making it clear that he wanted to conduct outreach with the Diocese of Richmond and local Catholic parishes. Meador testified that the memorandum was specifically “an outreach document.”¹¹⁴ He further testified that his goal with the memorandum would have been to “put [FBI] folks around the table and talk about this and what that outreach would look like.”¹¹⁵ However, he testified that “we didn’t even get to that point” before the memorandum was released publicly.¹¹⁶

Meador’s attempt to rationalize the purpose of the memorandum as simply a mechanism for community “outreach” is a weak effort to gloss over the concerning rhetoric directed towards Catholic sects and conservative viewpoints. During his transcribed interview, Meador repeatedly testified to the Committee that he was unable to conduct outreach with Catholic parishes because the memorandum was revealed to the public by a whistleblower.¹¹⁷ However, he later conceded that the existence of the memorandum was not a necessary condition for conducting outreach in the community.¹¹⁸ When asked if he needed a formal intelligence document to conduct outreach

¹⁰⁸ Strategic Review Report at FBI-HJC118-DP-000299.

¹⁰⁹ *Id.*

¹¹⁰ Meador Interview at 78.

¹¹¹ *Id.* at 77.

¹¹² *Id.* at 78.

¹¹³ *Id.*

¹¹⁴ *Id.* at 108.

¹¹⁵ *Id.* at 80.

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 51, 80, and 121.

¹¹⁸ *Id.* at 121-122.

in the community, he admitted “No, I can just do it.”¹¹⁹ Meador’s rationalization of the memorandum as a community engagement exercise defies belief.

F. The FBI acknowledged that the memorandum lacked “sufficient evidence” and any “articulable support.”

The FBI found that the authors of the memorandum first conceived of the idea for the intelligence product from a single investigation in the Richmond area. Because the subject under investigation identified as a “self-described” “radical-traditionalist Catholic” the memorandum’s authors kept the terminology and associated it with “racially or ethnically motivated violent extremists (RMVE).”¹²⁰ The FBI further concluded that this association between “radical-traditionalist Catholics” and RMVEs lacked “sufficient evidence or articulable support” to justify the FBI’s attempt to conduct investigative activity on Catholic parishes.¹²¹ The FBI also found that the memorandum “failed to consider the potential bias and credibility of open-source information cited in support of the [document’s] assessment” such as the Southern Poverty Law Center (SPLC), *Salon*, and *The Atlantic*.¹²²

The FBI also found that the employees involved in drafting, reviewing, and approving the memorandum failed to adhere to FBI standards. The employees “lacked professional judgement” and “lack[ed] . . . training and awareness” of Domestic Terrorism (DT) terminology, causing them to utilize amorphous and ill-defined terms such as “RTC” and “far-right.”¹²³ Furthermore, the FBI’s internal review found that the Richmond Field Office lacked a formal review process.¹²⁴ As a result, the reviewers used “less scrutiny because it was an internal intelligence product.”¹²⁵ Ultimately, according to the FBI, this “lack of adherence” to FBI standards “led to the creation of the final version” of the Richmond memorandum.¹²⁶

In response to the problems with the Richmond memorandum, the FBI proposed a few corrective actions to address the deficiencies identified in the document. The FBI’s internal review concluded that all employees involved in drafting, reviewing, and approving the memorandum “shall be admonished” and “their respective supervisors will engage with [the] Human Resources Division to ensure deficiencies are addressed.”¹²⁷ The review also required additional training on “analytical tradecraft standards” and “DT [Domestic Terrorism] terminology.”¹²⁸ Furthermore, the FBI indicated that it will now require “heightened approval,” which now requires the SAC and FBI Headquarters to review and approve intelligence products involving “sensitive investigative matter[s]” such as protected First Amendment activity.¹²⁹ Lastly, the FBI promised to update its policy regarding the use of third-party sources, which will

¹¹⁹ *Id.* at 122.

¹²⁰ Strategic Review Report at FBI-HJC118-DP-000294.

¹²¹ *Id.*

¹²² *Id.*

¹²³ *Id.* at FBI-HJC118-DP-000295.

¹²⁴ *Id.* at FBI-HJC118-DP-000298.

¹²⁵ *Id.* at FBI-HJC118-DP-000295.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.*

include “consideration and documentation of the access, reliability, bias, and other factors affecting the credibility of all sources cited” in future intelligence documents.¹³⁰

Although these corrective measures are warranted, they alone are not sufficient. The FBI must be held accountable for its actions. It is not enough for the FBI to investigate itself and remedy its own wrongdoings, especially when it involves law-enforcement overreach involving fundamental religious freedoms. While the FBI’s internal report affirmed the Committee’s and Select Subcommittee’s suspicions of the Richmond memorandum, the report does not encompass the complete picture of the memorandum’s inception and fallout. For example, following news reporting, FBI Deputy Director Paul Abbate ordered a permanent removal of the memorandum, as well as any edits or references, from all FBI systems.¹³¹ The FBI asserts that due to this order, there is no other communication or documentation about the memorandum, other than what has been already given to the Committee. The redactions in the FBI report also leave gaps in the information provided, such as the names of the employees responsible for drafting, reviewing, and approving the memorandum. It seems clear, then, that the FBI’s internal report, in addition to its latest document production, does not encompass the entire picture.

II. Without widespread criticism from other agents and public reporting about the Richmond memorandum, the document would have remained in FBI systems.

Shortly after the memorandum was published on an FBI-wide system, an intelligence analyst with the FBI’s Milwaukee Field Office sent an email announcement to agents across the other field offices about recently published intelligence products, including the Richmond memorandum.¹³² One agent, whose name was redacted by the FBI, responded to the email thread: “Is anyone really asking for a product like this? Apparently we are at the behest of the SPLC [Southern Poverty Law Center]”¹³³ Another agent who appears to be from the Milwaukee Field Office replied, “yeah, our overreliance on the SPLC for hate designations is . . . problematic.”¹³⁴ From these comments, it is apparent that some line agents disagreed with the content of the memorandum, especially for its reliance on biased information. These documents also directly show that the memorandum was spread throughout the FBI, which is contrary to previous assertions that the memorandum was limited to the Richmond Field Office.

On February 8, 2023, news organizations started to report on a redacted version of the Richmond memorandum.¹³⁵ In the wake of backlash against the content of the memorandum, the FBI ordered the Richmond Field Office to withdraw it.¹³⁶ While the FBI’s internal review sheds some light on how the memorandum was removed, it does not show the complete picture, especially as the FBI alleges it permanently deleted the memorandum. The transcribed interview with SAC Meador, however, highlighted some details that were omitted or neglected in the FBI internal report provided to the Committee.

¹³⁰ *Id.* at FBI-HJC118-DP-000296.

¹³¹ *Id.* at FBI-HJC118-DP-000299 and FBI-HJC118-DP-000304.

¹³² FBI-HJC118-DP-000536.

¹³³ FBI-HJC118-DP-000558.

¹³⁴ FBI-HJC118-DP-000561.

¹³⁵ Arnold and Bukuras, *supra* note 24.

¹³⁶ *Id.*

A. Meador coordinated with FBI Headquarters leadership to immediately and permanently delete the memorandum.

On the same day that the memorandum became publicly available, Deputy Director Abbate ordered Meador to “pull it down.”¹³⁷ Meador interpreted Abbate’s instruction as an order to expunge the memorandum from all FBI Richmond systems.¹³⁸ Soon after, Meador notified two Assistant Special Agents in Charge (ASAC) of the news reporting on the memorandum and how to facilitate its removal.¹³⁹ On February 9, 2023, Meador conducted a morning meeting with his Executive Management, Supervisory Intelligence Analysts (SIAs), and CDC to discuss the news reporting on the memorandum and how to remove the document, and any references made to the document, from FBI Richmond’s online collaborative platform.¹⁴⁰ Following the meeting, Meador ordered another intelligence analyst, who had no earlier involvement with the memorandum, to remove the document from FBI Richmond’s online collaborative platform, including any edits and references made to it.¹⁴¹ The analyst deleted everything associated with the memorandum that same day, and “ensured the deleted [memorandum] was removed from the site’s recycle bin.”¹⁴²

Meanwhile, Meador tasked the CDC to work with the FBI’s Office of General Counsel (OGC) to facilitate the memorandum’s removal from the FBI-wide Sentinel program.¹⁴³ To do so, the Richmond Field Office had to perform a process called a “Permanent Charge-Out” (PCO), which “refers to a deletion of a record from all [FBI] electronic recordkeeping systems.”¹⁴⁴ An ASAC was assigned to oversee the removal of the memorandum from FBI systems.¹⁴⁵ To justify the removal, the ASAC noted in a “lead” that the memorandum contained information that “should have been restricted or prohibited” and indicated that OGC “concurred” with the need for removal.¹⁴⁶ On February 10, 2023, the removal process was officially completed.¹⁴⁷

Meador’s testimony provides more information about how FBI Executive Management directed and monitored the removal process. Meador testified that the decision to pull the memorandum off FBI systems “was made after” public reporting and after he received direction from Deputy Director Abbate to “pull it down” he also received a “follow-up call” from Tonya Ugoretz, the FBI’s Assistant Director of the Directorate of Intelligence.¹⁴⁸ According to Meador, Ugoretz told Meador that he needed to notify both the Deputy Director and herself “when [he] had taken the necessary steps” to remove the memorandum, and anything referring to the document, from FBI systems.¹⁴⁹

¹³⁷ Strategic Review Report at FBI-HJC118-DP-000299 and FBI-HJC118-DP-000304.

¹³⁸ *Id.*

¹³⁹ *Id.* at FBI-HJC118-DP-000304.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.* at FBI-HJC118-DP-000300.

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ *Id.* at FBI-HJC118-DP-000304.

¹⁴⁷ *Id.*

¹⁴⁸ Meador Interview at 97.

¹⁴⁹ *Id.*

B. There were no prior concerns about the memorandum before news reporting. In fact, Meador was interested in quickly effectuating the memorandum.

If the memorandum had not become public knowledge, the document would have remained in an FBI-wide system. During his transcribed interview, Meador testified that the Richmond Field Office had received no concerns about the contents of the memorandum until it became public. Meador testified:

Q: And prior to February 8th, when the existence of the domain perspective hit the news, had anyone raised concerns to you about the propriety of the domain perspective?

A: “Propriety” meaning what?

Q: Whether or not it held up to the exacting standards of the FBI?

A: No.

Q: Had you had any discussions with anyone at headquarters prior to February 8th about the domain perspective?

A: No.¹⁵⁰

Meador also testified that if the memorandum did not become public, it would still be in FBI systems.¹⁵¹ In fact, Meador testified that he would have prioritized outreach to the Diocese of Richmond as a result of the memorandum.¹⁵² He stated:

Q: Do you know, if the domain perspective had not been . . . made public, would it still be in FBI systems?

A: Yes.

Q: Would outreach have been conducted based upon the domain perspective?

A: . . . I would’ve prioritized and had the discussion. Quite likely, I would’ve reached out to the Diocese.¹⁵³

It is concerning that if a whistleblower had not disclosed the existence of the memorandum, then an official FBI document of its nature—one that infringes on religious

¹⁵⁰ *Id.* at 97-98.

¹⁵¹ *Id.* at 98.

¹⁵² *Id.*

¹⁵³ *Id.*

liberties—would still be in effect. During the briefing, the Committee asked the FBI whether it conducts periodic reviews of other intelligence products to see if other concerning memorandums may be in existence.¹⁵⁴ The FBI’s briefers responded that the FBI does not conduct periodic reviews, and if it were to do reviews, they were doubtful they would have caught the memorandum.¹⁵⁵ This information, coupled with Meador’s testimony, is alarming, especially as Meador maintained that “the purpose of [the memorandum] was to engage in outreach to [the Diocese of Richmond].”¹⁵⁶

C. The memorandum originated as an internal product but was proposed to leadership to become an external, FBI-wide product, and discussions toward that goal are ongoing.

The FBI’s report revealed that the FBI had plans for an external, FBI-wide product based on the Richmond memorandum.¹⁵⁷ Not only is this concerning because other field offices around the country would effectuate the memorandum by using federal law enforcement resources to surveil Catholic parishes, but it would also allow other intelligence products to build upon the unconstitutional foundation of the Richmond memorandum. The Committee and Select Subcommittee have also learned that the FBI may still be attempting to fashion information from the Richmond memorandum into an external-facing document.

During his transcribed interview, Meador provided information about the differences between an internal and external intelligence product. Meador testified that an external product is “Bureau-wide” and “all external products go through headquarters” for review.¹⁵⁸ On the other hand, internal products do not go to headquarters for review.¹⁵⁹ However, an internal product does not mean that it stays solely within the Richmond Field Office. Meador testified that although the memorandum was an internal product, “it could be [used] to inform . . . management in the Richmond Field Office, but it also could be [used] to inform . . . other intelligence analysts across the country.”¹⁶⁰

As the first draft of the memorandum was nearly completed, the co-authors began informing leadership of its contents.¹⁶¹ On January 5, 2023, one of the authoring analysts emailed the Richmond’s domestic terrorism supervisory agent that an “internal intelligence product” was being written.¹⁶² In the same email, the analyst also informed the supervisory agent that the other co-authoring analyst was coordinating with the Counterterrorism Division on an “external product” known as a Strategic Perspective Executive Analytic Report (SPEAR).¹⁶³ On January 12, the supervisory analyst received a draft of the memorandum for his awareness.¹⁶⁴

¹⁵⁴ FBI Briefing.

¹⁵⁵ *Id.*

¹⁵⁶ Meador Interview at 121.

¹⁵⁷ Strategic Review Report at FBI-HJC118-DP-000303.

¹⁵⁸ Meador Interview at 74.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.* at 74-75.

¹⁶¹ Strategic Review Report at FBI-HJC118-DP-000303.

¹⁶² *Id.*

¹⁶³ *Id.* at FBI-HJC118-DP-000304.

¹⁶⁴ *Id.* at FBI-HJC118-DP-000303.

After FBI Richmond published the memorandum internally, a subsequent draft of the memorandum was proposed to leadership to become an external product.¹⁶⁵ By February 2, 2023, an FBI employee sent a draft of the external-facing SPEAR report to the Counterterrorism Division.¹⁶⁶ In the FBI's latest production, the draft of the external SPEAR report had a pending release for February 2023, suggesting an interest for a prompt release.¹⁶⁷ On February 6, 2023, the Counterterrorism Division viewed the draft of the report and suggested making the document into an Emerging Intelligence Report (EIR).¹⁶⁸ During his transcribed interview, Meador described his awareness of the interest in making the memorandum into an external product. He testified:

A: Post the leak and the discussions I did learn . . . as I was having conversations, asking questions, that there . . . had been communication with [the Counterterrorism Division] on the release of this information in an external product, in a SPEAR, and that the response from them based on the [memorandum] was that the information should go into a different type of product, which is called an EI—for an external release, an EIR, emerging intelligence report, . . . versus a SPEAR.

Q: And was the topic of the external product, whatever the form, the SPEAR or the EIR, what was the topic going to be for that external product?

A: I don't know. I know—I think I would have to defer back to the inspection, because I think there's an indication that it was based on the [memorandum].¹⁶⁹

SAC Meador gleaned that the proposed external product was going to be based on the memorandum.¹⁷⁰ While this is concerning, knowing that the FBI wanted to further infringe on religious liberties Bureau-wide, equally concerning is that there are discussions still taking place with FBI Richmond on how to effectuate this external memorandum. Meador further testified:

Q: Do you know if the FBI is still pursuing an external product based upon the [memorandum]?

A: There—I know internally there have been some discussions . . . throughout the months of a desire to still try and get this information out somehow, but . . . I've not seen anything as

¹⁶⁵ *Id.* at FBI-HJC118-DP-000304.

¹⁶⁶ *Id.*

¹⁶⁷ FBI-HJC118-DP-000474.

¹⁶⁸ Strategic Review Report at FBI-HJC118-DP-000304.

¹⁶⁹ Meador Interview at 115.

¹⁷⁰ *Id.*

a result of that.

Q: What information [about]?

A: The subject—I think just a general subject, RMVE connection—

Q: An RTC?

A: Yeah.¹⁷¹

Despite all the problems that the FBI found with the memorandum, FBI Richmond still “desires” to get this information out about “radical-traditionalist Catholics.” This revelation is disturbing because the memorandum relied on biased sources and a single investigation, suggesting that the memorandum and its contents are not fully supported. Yet, despite the shortcomings of the Richmond memorandum and the widespread criticism for its creation, the FBI still apparently desires to convey the outrageous message that some Catholic Americans with traditional beliefs pose a domestic terror threat to our country.

III. SAC Meador met with several members of the clergy to mend the FBI’s relationship with the Catholic community.

After the leak of the Richmond memorandum and the ensuing backlash from the religious community, leaders of the Catholic faith, and news outlets, SAC Meador sought to repair the FBI’s relationship with leaders of the Diocese of Richmond. In particular, SAC Meador requested a meeting with the Bishop of the Diocese of Richmond and attended a meeting with a Cardinal of the Catholic Church to discuss issues with the Richmond memorandum.¹⁷² During these meetings, SAC Meador claimed that the purpose of the memorandum was to promote outreach by the FBI and offered private apologies for the “negative light that it had placed the organization in,” but not for the memorandum’s content.¹⁷³ Despite SAC Meador’s efforts, many in the religious and Catholic community continue to have concerns that the FBI is targeting them because of their sincerely held beliefs and that the FBI has shown an alarming disregard for religious liberty rights as protected by the First Amendment of the Constitution.¹⁷⁴

A. SAC Meador reached out to the Catholic Diocese of Richmond to meet with the Bishop and apologize for the memorandum.

After the disclosure of the memorandum began receiving coverage in news media outlets, the Catholic Diocese of Richmond issued a public statement about it on February 13, 2023.¹⁷⁵ In his statement, Bishop Knestout wrote that he was “alarmed” to read the memorandum and that it

¹⁷¹ *Id.* at 115-116.

¹⁷² *Id.* at 119-124.

¹⁷³ *Id.* at 120-121.

¹⁷⁴ U.S. Const. amend. I.

¹⁷⁵ Press Release, Catholic Diocese of Richmond, Bishop Knestout’s Statement Following Leaked Internal Memo from the FBI Richmond Field Office about Traditional Catholics and the Virginia Attorney General’s Response (Feb. 13, 2023).

“should be troubling and offensive to all communities of faith, as well as Americans.”¹⁷⁶ Bishop Knestout further wrote: “A preference for traditional forms of worship and holding closely to the Church’s teachings on marriage, family, human sexuality, and the dignity of the human person does not equate with extremism.”¹⁷⁷ Bishop Knestout also specifically recognized the duty of the Commonwealth of Virginia and Congress “to exercise their role of oversight, to publicly condemn this threat to religious liberty, and to ensure that such offenses against the constitutionally protected free exercise of religion do not occur again.”¹⁷⁸ The Committee and Select Subcommittee have done just that.

Bishop Knestout's Statement Following Leaked Internal Memo from the FBI Richmond Field Office about Traditional Catholics and the Virginia Attorney General's Response

For Immediate Release: February 13, 2023

Bishop Knestout's Statement Following Leaked Internal Memo from the FBI Richmond Field Office about Traditional Catholics and the Virginia Attorney General's Response

On Monday, Feb. 13, 2023, Bishop Knestout issued a statement following a January 10, 2023 memorandum generated by the Richmond Field Office made public last week. The memorandum targeted Virginia Catholics, specifically traditional Catholics, some of whom are not in full communion with the Roman Catholic Church. On Feb. 10, 2023, Virginia's Attorney General announced that he had received a leaked internal memo from the FBI Richmond Field Office that included multiple attorneys general from other states.

"People of all faith groups have long found refuge in the constitutional protections of our great nation. We all seek to share in God's gift of life, enjoy the fruits of liberty that our nation offers and assist one another in ensuring the common good.

"I was alarmed to read the reports written late last week about the contents of the internal memo created by the Richmond Field Office of the Federal Bureau of Investigation. I was also surprised to learn that the memo mentioned the Priestly Fraternity of Saint Peter (FSSP), a religious order, which celebrates the Mass. FSSP has served with devotion for many years the parishes within our diocese. FSSP members are faithful of our diocese who appreciate this form of the Catholic Mass in our diocese.

"The leaked document should be troubling and offensive to all communities of faith, as well as all Americans. I am grateful for the Virginia Attorney General and 19 attorneys general who have called upon the government to publicly release all materials related to the production of this memo. If evidence of such targeting is rooted out, but not at the expense of religious freedom. A preference for traditional forms of worship and holding closely to the Church's teachings on marriage, family, human sexuality, and the dignity of the human person does not equate with extremism.

"Religious freedom is an important matter acknowledged every June by the U.S. President. The U.S. Catholic Bishops (USCCB) in which my brother bishops and I value and celebrate religious freedom. Most recently, on Jan. 16, 2023, the U.S. celebrated Religious Freedom Day with USCCB Chair for Religious Liberty, Cardinal Timothy M. Dolan, noting "there is no freedom without the truth." It is my hope we get to the truth of the memo published last week.

"Our faith and our Church instruct us to be a people of peace and to uphold human dignity. We must reject violence. As Pope Francis wrote in his 2017 letter for the celebration of World Day of Prayer for the Unity of Religions, "the name of God cannot be used to justify violence. Peace is the fruit of justice."

"I call on all national representatives from the Commonwealth of Virginia in the House and Senate to exercise their role of oversight, to publicly condemn this threat to religious liberty, and to ensure that such offenses against the constitutionally protected free exercise of religion do not occur again. We must ensure that violence, and discrimination have no place in our Church or teachings."

###

Within the memo, it mentioned the targeting of Virginia Catholics, specifically traditional Catholics, some of whom are not in full communion with the Roman Catholic Church.

"I was alarmed to read the reports written late last week about the contents of the internal memo created by the Richmond Field Office of the Federal Bureau of Investigation.

"The leaked document should be troubling and offensive to all communities of faith, as well as all Americans. I am grateful for the Virginia Attorney General and 19 attorneys general who have called upon the government to publicly release all materials related to the production of this memo.

"I call on all national representatives from the Commonwealth of Virginia in the House and Senate to exercise their role of oversight, to publicly condemn this threat to religious liberty, and to ensure that such offenses against the constitutionally protected free exercise of religion do not occur again.

On March 9, 2023, after receiving permission from the Deputy Director of the FBI, SAC Meador went to the Diocese of Richmond to meet with clergy officials to apologize for the memorandum, including the Vicar General, the general counsel, and the Bishop of the Diocese of Richmond.¹⁷⁹ During his transcribed interview, SAC Meador testified that although he had never met with anyone from the Diocese of Richmond prior to the disclosure of the memorandum, he wanted to offer “an apology on behalf of the field office for the negative attention . . . and inform them as to why—and give them what information I could as to why this—what it was and what it wasn’t and help inform them.”¹⁸⁰ However, it does not appear that SAC Meador offered an apology for the content of the memorandum or for his role in approving it, despite the memorandum failing to meet the “exacting standards” of the FBI.¹⁸¹ SAC Meador did

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.*

¹⁷⁹ Meador Interview at 120.

¹⁸⁰ *Id.*

¹⁸¹ Joe Bukuras, *U.S. bishops: FBI document targeting Catholics is religious profiling*, CATHOLIC NEWS AGENCY (Feb. 17, 2023).

acknowledge that the Diocese of Richmond took issue with the memorandum, testifying that “common sense, to me, is that they would’ve been concerned.”¹⁸² SAC Meador went on to say that he wanted to explain through his conversation with the Bishop that “the purpose of [the memorandum] was to engage in outreach to them.”¹⁸³

After their meeting, on March 13, 2023, SAC Meador reached out to the Diocese of Richmond again, thanking it for the opportunity to meet.¹⁸⁴ He wrote the following email:

Father [redacted],

Thank you for allowing me the opportunity to meet with you and Bishop Knestout. I sincerely appreciate you taking the time to meet and do hope the discussion was helpful. I wanted to follow up and extend an open invitation to you and Bishop Knestout to visit our Richmond FBI Field Office. In addition to showing you around, I think it would be a great opportunity to have you both meet some of our team members, who could also, if you like, provide a short briefing on some of our priority threats. My team and I would be happy to host so please feel free to reach out to me directly if you feel this would be of interest.... Look forward to hearing from you. In the interim, if you need anything from my direction, please do not hesitate to reach out anytime.¹⁸⁵

SAC Meador later extended an invitation for a second meeting with the Diocese at the FBI Richmond Field Office.¹⁸⁶ In response, a diocesan attorney accepted the invitation, but advised SAC Meador that:

Bishop Knestout recognizes that a cooperative relationship with law enforcement could prove useful to protect the diocese and its parishioners from current threats and any identified in the future. However, he would prefer that any such cooperation occur through his legal team, to that end, the diocesan attorney, including myself and [redacted], would make ourselves available to come to your office.¹⁸⁷

Routing all communications through his legal team may be evidence of the Bishop’s reluctance to engage with the FBI directly and further evidence of the FBI’s strained relationship with religious leaders in the community as a result of the memorandum. However, Diocesan attorneys still coordinated a visit to the field office on March 24, 2023, during which FBI Richmond briefed officials from the Diocese on domestic terrorism, international terrorism, and

¹⁸² Meador Interview at 120.

¹⁸³ *Id.* at 121.

¹⁸⁴ FBI-HJC118-DP-000217 (on file with the Comm.).

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ FBI-HJC118-DP-000218 (on file with the Comm.).

hate crimes.¹⁸⁸ The Bishop did not attend the briefing.¹⁸⁹ Since that meeting, SAC Meador has not had any contact with the Diocese of Richmond.¹⁹⁰

B. SAC Meador also met with a Cardinal of the Catholic Church to discuss the memorandum.

As part of more outreach to the Catholic community, SAC Meador informed the Committee during his transcribed interview that he also met with a Cardinal of the Catholic Church, along with the Assistant Director in Charge (ADIC) of the Washington Field Office (WFO).¹⁹¹ Meador testified:

A: I learned of the meeting from one of the special agents in charge of the Washington Field Office. He had told me that he was coordinating that meeting and wanted me to know. And I asked if I could attend to help with that meeting, and they said, of course. . . .

Q: Did the cardinal request that meeting, or did WFO reach out to the cardinal?

A: That's in WFO's territory.

Q: What was discussed at the meeting?

A: . . . I presented similar information that I did with the Bishop.

Q: Did you get the sense that the cardinal was concerned about the domain perspective?

A: Well, I think they were just concerned at large. I don't have any information expressed to me from the cardinal on his thoughts, on his stance related to it. I was there in a proactive sense and to help the ADIC because I had more of the firsthand information on the product.¹⁹²

Despite the apparent efforts at mending the FBI's relationship with the Catholic community, the memorandum has clearly created a lasting cause for concern. An FBI visit alone falls far short of the action necessary to repair the damage that is caused by a federal law enforcement intelligence product, such as the Richmond memorandum, that demonstrates an animus towards a particular faith group. FBI Richmond's failure to issue a public apology for the

¹⁸⁸ Meador Interview at 123.

¹⁸⁹ *Id.*

¹⁹⁰ *Id.* at 124-25.

¹⁹¹ *Id.* at 125-26.

¹⁹² *Id.* at 126-27.

content of the memorandum will only delay the process of rebuilding trust in communities of faith.

CONCLUSION

“Religious Liberty is under attack in many places because it is dangerous to those who want to hold complete power.”
– Justice Samuel Alito, July 28, 2022

Religious liberty is enshrined in the First Amendment to the Constitution.¹⁹³ Accordingly, the FBI’s own policy claims it “never conduct[s] investigative activities or open[s] an investigation based solely on First Amendment protected activity.”¹⁹⁴ The Richmond memorandum, however, paints a different picture. It is a stark reminder that sincerely held religious beliefs must be vigorously protected or be subjugated to an overzealous federal law enforcement focused on the ends, with little regard for the means. In the words of Stanley Meador, the Special Agent in Charge in Richmond, when he first “saw the document, I did not give it the review that it’s being given today.”¹⁹⁵ This ill-conceived and ill-administered memorandum is a stark warning of the need for scrupulous review of FBI documents with the potential to circumvent Americans’ civil liberties and the right to free exercise of religion.

Under the guise of domestic terrorism, the Richmond memorandum cast swaths of Catholic Americans as “radical-traditionalist Catholics” and those practicing it as ripe opportunities for FBI “threat mitigation.”¹⁹⁶ Due to the actions of a brave whistleblower, this document was introduced into the public eye largely before it could be acted on. Perhaps most concerning is that without the whistleblower, this document would still be actionable in FBI systems, potentially endangering the religious liberties of countless Americans who might be investigated simply for espousing certain sincerely held views.¹⁹⁷ That is unacceptable and antithetical to the protections of the First Amendment.

In the interim, the FBI must take decisive action to rebuild public trust. FBI Richmond has not issued a public apology or removed any of the employees involved in creating the document.¹⁹⁸ Moreover, the FBI continues to resist several of the Committee’s requests for transparency and answers.¹⁹⁹ While the Committee’s and Select Subcommittee’s oversight continues, this work will continue to inform potential legislative reforms that are necessary to protect the right to religious liberty from government overreach.

¹⁹³ U.S. Const. amend. I.

¹⁹⁴ Bukuras, *supra* note 181.

¹⁹⁵ Meador Interview at 21.

¹⁹⁶ Catholic Memorandum at FBI-HJC118-DP-000281.

¹⁹⁷ *See id.*; *See also* Meador Interview at 98.

¹⁹⁸ Meador Interview at 67-68.

¹⁹⁹ *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Christopher A. Wray, Dir., Fed. Bureau of Investigation (Aug. 9, 2023).



**FIGHTING THE WEAPONIZATION OF THE INTERNAL REVENUE SERVICE:
THE END OF ABUSIVE UNANNOUNCED FIELD VISITS**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



October 27, 2023

EXECUTIVE SUMMARY

The Committee on the Judiciary and its Select Subcommittee on the Weaponization of the Federal Government are empowered by the House of Representatives to examine how the Executive Branch interacts with American citizens and to investigate civil liberties abuses. History has shown how the Internal Revenue Service (IRS), with its vast power to reach into the lives of Americans, has the tremendous potential to violate the civil liberties of American citizens.¹ As Justice John Marshall noted over two-hundred years ago, the “power to tax involves the power to destroy.”² The Committee’s and Select Subcommittee’s oversight demonstrates that Justice Marshall’s warning is as potent now as it was then.

In 2022, Democrats in Congress flooded the IRS with \$78.9 billion in new funding, \$45 billion of which was earmarked solely for tax enforcement purposes.³ Democrats chose to enable the IRS to hire as many as 87,000 agents to aggressively pursue American taxpayers.⁴ One of the first priorities for the new Republican majority in the 118th Congress was to severely curtail this new funding.⁵ The Committee’s and Select Subcommittee’s oversight shows the wisdom of this action.

In just the first nine months of this Congress, the Committee and Select Subcommittee have shed light on several civil liberties abuses at the IRS. For example:

- **The IRS conducted an unannounced field visit to the home of journalist Matt Taibbi the same day he testified before Congress about government abuse.** The IRS opened a case against Mr. Taibbi on Christmas Eve—a Saturday—just three weeks after Mr. Taibbi began reporting on the Twitter Files. In the four-and-one-half years between when the IRS alleges it last tried to contact Mr. Taibbi and the day it conducted an unannounced field visit, neither he nor his accountant ever received notice from the IRS about an issue with his tax return. The IRS conducted its field visit even though Mr. Taibbi did not owe the IRS anything, rather, the IRS owed Mr. Taibbi a substantial refund. The unannounced field visit alarmed Mr. Taibbi, who viewed it as an attempt to chill his reporting about government abuses.
- **An IRS agent gave a fake name and used deception to gain entry into the house of an Ohio taxpayer and then threatened her when asked to leave.** Without any notice, an IRS revenue officer conducted an unannounced field visit to the home of a taxpayer in Ohio. The revenue officer used an alias and was deceptive about his purposes for appearing at the taxpayer’s home. After the taxpayer’s attorney told the revenue officer to leave, the revenue officer defiantly stated, “I can be at and go into anyone’s house at any time I want to be.” The revenue officer threatened to put a lien on the taxpayer’s home

¹ See discussion *infra* Section I.A.

² *M’Culloch v. Maryland*, 17 U.S. 316, 431 (1819).

³ Inflation Reduction Act, P.L. 117-169, 117th Cong. (2022); Alex Muresianu, *IRS Strategic Operating Plan Shows Promise, but Concerns Remain*, TAX FOUNDATION (Apr. 13, 2023).

⁴ Sen. J.D. Vance, *Meet the New IRS, Same as the Old IRS*, WALL ST. J. (Aug. 17, 2023).

⁵ Family and Small Business Taxpayer Protection Act, 118th Cong. (2023); Brooke Singman, *House votes to rescind billions in funding to the IRS in first major majority action with McCarthy as speaker*, FOX NEWS (Jan 9, 2023).

and freeze her assets if she did not immediately give the IRS a substantial amount of money. After the taxpayer called the police, the revenue officer even filed a complaint against the police department. The IRS later confirmed that the taxpayer owed nothing and acknowledged the situation “never should have gotten this far.” This shocking abuse of power is a startling indication that the IRS believes it may do what it wants, when it wants.

- **The IRS has repealed its policy of unannounced field visits after the Committee’s and Select Subcommittee’s oversight uncovered IRS abuses.** Pressure and oversight about these abusive field visits led the IRS to repeal its policy of allowing its agents to conduct unannounced field visits to taxpayers’ homes. The IRS is no longer able to weaponize its field visits to target, harass, and intimidate taxpayers.

It has been over ten years since the IRS disclosed its targeting of conservative groups seeking tax-exempt status.⁶ The man who President Obama chose to clean up the IRS’s mess in 2013, Danny Werfel, is the same man who President Biden chose to lead the agency today. The agency that felt emboldened ten years ago to intentionally and unfairly scrutinize conservative nonprofit organizations is the same agency that feels emboldened now to force its way into a taxpayer’s home. As the *National Review* observed:

It is a tax code so perverse, ambiguous, and complex that it cedes to those IRS agents unwarranted power to interpret the law and, along with that, power to neglect, pester, or tyrannize citizens.⁷

Consistent with the Committee’s and Select Subcommittee’s obligations to keep the House of Representatives informed of its oversight, this interim report documents the weaponization of the IRS against Americans. Although more information continues to surface concerning the IRS’s weaponization, this report presents the findings to date. The Committee and Select Subcommittee will continue to pursue additional information about the actions and events described in this report.

⁶ See, e.g., H. COMM. ON OVERSIGHT & GOV’T REFORM, THE INTERNAL REVENUE SERVICE’S TARGETING OF CONSERVATIVE TAX-EXEMPT APPLICANTS: REPORT OF FINDINGS FOR THE 113TH CONGRESS (Dec. 23, 2014).

⁷ Amity Shlaes, *Wrong Target: Republicans and the IRS*, NAT’L REV. (Aug. 23, 2023).

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
TABLE OF CONTENTS.....	3
I. BACKGROUND ON THE IRS’S ABUSES.....	4
A. The IRS’s history of abusing its power.....	4
B. The potential for abuse in the IRS’s unannounced field visits	5
II. THE IRS VISITS THE HOME OF JOURNALIST MATT TAIBBI WHILE HE TESTIFIED BEFORE CONGRESS	7
A. Twitter Files journalist Matt Taibbi testified before the Select Subcommittee about how the Biden Administration worked with Big Tech to censor Americans	7
B. The IRS conducted an unannounced field visit to Mr. Taibbi’s home on the same day he testified before the Select Subcommittee.....	10
C. Internal IRS documents revealed how the IRS used a field visit to intimidate Mr. Taibbi	11
III. THE IRS LIED TO AN OHIO TAXPAYER TO GAIN ACCESS TO HER HOUSE DURING AN UNANNOUNCED FIELD VISIT	14
A. An IRS agent, using a false name, harassed and intimidated an Ohio taxpayer.....	14
B. The IRS Agent filed a complaint against the local police department for investigating his unusual conduct	15
C. The IRS admitted its agent’s actions were improper	18
IV. AS A RESULT OF THE COMMITTEE’S AND SELECT SUBCOMMITTEE’S OVERSIGHT, THE IRS TERMINATED ITS POLICY OF CONDUCTING UNANNOUNCED FIELD VISITS	19
CONCLUSION.....	21

I. Background on the IRS's Abuses

As President Ronald Reagan famously said, “the nine most terrifying words in the English language are: I’m from the government, and I’m here to help.”⁸ The IRS, with its tax collection authority, represents this threat unlike any other agency in government.

A. The IRS's abusive history

The IRS has a long history of weaponizing its power. In the 1930s, President Franklin Roosevelt weaponized the IRS against his political enemies, including newspaper publishers who opposed the New Deal.⁹ In the 1940s and 1950s, corruption and bribery became so widespread at the IRS that the Truman Administration dismissed and indicted hundreds of staffers as the agency was reorganized to prevent political influence.¹⁰ In the late 1990s, the Senate Finance Committee held several oversight hearings to investigate the IRS's “Gestapo-like” conduct against taxpayers.¹¹ In response to these hearings, Congress passed the IRS Restructuring and Reform Act of 1998 to put limits on the IRS's enforcement powers and to make right a “tax agency out of control.”¹² In 2013, during the Obama Administration, the IRS targeted dozens of conservative nonprofits seeking tax-exempt status by subjecting the nonprofits to “heightened scrutiny and inordinate delays.”¹³ Congress investigated this scandal at length,¹⁴ and several top IRS officials resigned in shame.¹⁵

With the extensiveness of the IRS's past abuses, it is no surprise that the IRS is the least trusted federal agency in government.¹⁶ Americans ranked the IRS the lowest among 16 agencies in terms of favorability, with 51 percent expressing an unfavorable view of the agency and only 42 percent expressing a favorable view.¹⁷ Seventy-three percent of Americans do not believe the government is spending their tax dollars wisely, and 72 percent of Americans believe their tax rate is already far too high.¹⁸ But mismanagement and over-taxation is only half of the issue.

The IRS's greatest challenge is a trust deficit. In 2021, only 66 percent of Americans reported that they trusted the IRS to fairly enforce the tax laws—the lowest percentage since

⁸ U.C. Santa Barbara, The American Presidency Project, The President's Press Conference (Aug. 12, 1986), <https://www.presidency.ucsb.edu/documents/the-presidents-news-conference-957>.

⁹ James Bovard, *A Brief History of IRS Political Targeting*, WALL ST. J. (May 14, 2013).

¹⁰ Dena Aubin, *Factbox: IRS's rich history of scandals, political abuse*, REUTERS (May 16, 2023).

¹¹ Thomas H. Moore, *IRS Nightmares Get Senate Hearing*, CNN (Sept. 24, 1997); David Cay Johnston, *Senate Committee Is Told of a Vast Range of Abuses by I.R.S.*, N.Y. TIMES (Apr. 29, 1998).

¹² R. Morris Barrett, *IRS Commissioner Will Order Management Review*, CNN (Sept. 25, 1997); Internal Revenue Service Restructuring and Reform Act, P.L. 105-206, 105th Cong. (1998).

¹³ Peter Overby, *IRS Apologizes For Aggressive Scrutiny Of Conservative Groups*, NPR (Oct. 27, 2017).

¹⁴ H. COMM. ON OVERSIGHT & GOV'T REFORM, THE INTERNAL REVENUE SERVICE'S TARGETING OF CONSERVATIVE TAX-EXEMPT APPLICANTS: REPORT OF FINDINGS FOR THE 113TH CONGRESS (Dec. 23, 2014).

¹⁵ Josh Hicks, *Central figure in IRS tea party controversy resigns*, N.Y. TIMES (Sept. 23, 2013).

¹⁶ J. Baxter Oliphant and Andy Cerda, *Americans feel favorably about many federal agencies, especially the Park Service, Postal Service and NASA*, PEW RESEARCH CENTER (Mar. 30, 2023).

¹⁷ *See id.* (“Democrats view the IRS least favorably of the 16 federal agencies: They are only 13 percentage points more likely to view it favorably than unfavorably (53% vs. 40%).”).

¹⁸ John S. Kiernan, *2023 WalletHub Tax Survey*, WALLETHUB (Mar. 6, 2023).

2014.¹⁹ A more recent Gallup Poll from October 2022 found Americans’ disapproval of the IRS is as consistent as the agency’s history of abuse—just 35 percent of Americans have a fair view of the IRS, with another 31 percent having a poor view of the agency.²⁰ The IRS would like Americans to believe that its problems are budget related and that more money will resolve its issues. But the more money Congress gives the IRS, the more problems that seem to result.

B. The potential for abuse in the IRS’s unannounced field visits

For decades, the IRS has authorized its officers to appear at taxpayers’ homes or businesses without prior notice to collect delinquent taxes. These unannounced field visits have traditionally been reserved for rare cases in which a taxpayer or business is unresponsive to prior IRS communications and the agency’s requests for information. Surprisingly, these supposedly rare instances add up. Each year, the IRS makes tens of thousands of unannounced visits to homes and businesses.²¹

In most cases involving delinquent tax accounts, the IRS’s Automated Collection System (ACS) is the main avenue for taxpayers to resolve their tax issues.²² This system is managed by the Taxpayer Advocate System, which is an “independent organization within the IRS” that “helps taxpayers resolve problems and recommends changes that will prevent problems.”²³ Every year, ACS mails millions of tax delinquency notices, levy notices, and federal tax lien notices to taxpayers and businesses.²⁴

For other accounts, generally those with a tax debt that exceeds \$100,000, the IRS assigns a revenue officer to the case to resolve the outstanding balance.²⁵ These officers, of which the IRS currently employs roughly 2,300 nationwide, “are unarmed civil agency employees whose duties include visiting households and businesses to . . . collect taxes that are delinquent and have not been paid to the IRS and to secure tax returns that are overdue from taxpayers.”²⁶ The power revenue officers wield is not insignificant; they can “[g]arnish bank accounts and wages as well as seize real and personal property to satisfy delinquent taxes.”²⁷

Once assigned to a case, the revenue officer makes initial contact with the taxpayer to resolve his or her accounts. Normally, a revenue officer’s first effort to contact a taxpayer is in writing to notify and/or remind the taxpayer of his or her delinquency and the date the

¹⁹ Comprehensive Taxpayer Attitude Survey (CTAS), Internal Revenue Serv. (2021), <https://www.irs.gov/pub/irs-pdf/p5296.pdf>.

²⁰ Jeffrey M. Jones, *Government Agency Ratings: CIA, FBI Up; Federal Reserve Down*, GALLUP NEWS (Oct. 5, 2022).

²¹ Alan Rappeport, *I.R.S. Halts Surprise Visits to Homes and Businesses*, N.Y. TIMES (July 24, 2023).

²² *Automated Collection System (ACS)*, Taxpayer Advocate Service, <https://www.taxpayeradvocate.irs.gov/tax-terms/automated-collection-system-acs> (last visited Oct. 23, 2023).

²³ *About Us*, Taxpayer Advocate Service, <https://www.taxpayeradvocate.irs.gov/about-us> (last visited Oct. 23, 2023).

²⁴ Daniel J. Pilla, *IRS to Stop Unannounced Visits to Taxpayers*, NAT’L REV. (Aug. 16, 2023).

²⁵ Rappeport, *supra* note 21.

²⁶ *How to know it is an IRS revenue officer*, Internal Revenue Serv. (July 2023), <https://www.irs.gov/newsroom/how-to-know-it-is-an-irs-revenue-officer>.

²⁷ *Internal Revenue Officer*, Business and Tax Enforcement, IRS Careers, <https://www.jobs.irs.gov/resources/job-descriptions/business-tax-enforcement> (last visited Oct. 23, 2023).

outstanding balances and forms are due.²⁸ Only in rare instances with “unique, specific circumstances” may these officers initiate contact with taxpayers in person as opposed to a phone call or by mail.²⁹ However, with tens of thousands of unannounced field visits occurring each year as revenue officers carry out investigative actions, it is apparent that unannounced field visits are not just reserved for exceptional cases.

Prior to the IRS’s recent change in policy due to the Committee’s and Select Subcommittee’s oversight, these officers frequently conducted unannounced, unprompted field visits at taxpayers’ homes and businesses without attempting to first contact the taxpayer by other less intrusive means. The IRS has now discontinued this decades-long practice of revenue officers conducting unannounced field visits on unsuspecting taxpayers.³⁰ While the IRS promises that “taxpayers should know they have a tax issue before these visits occur since multiple mailings occur,”³¹ the abusive field visits the Committee and Select Subcommittee exposed included no prior notice whatsoever. Worse yet, neither instance involved the taxpayer owing the IRS any balance on their accounts.

²⁸ *How to know it is an IRS revenue officer, supra* note 26.

²⁹ *Id.*

³⁰ See Rappeport, *supra* note 21; Kanishka Singh, *US IRS ends policy of unannounced revenue officer visits to taxpayers*, REUTERS (July 24, 2023).

³¹ *How to know it is an IRS revenue officer, supra* note 26.

II. The IRS Visits the Home of Journalist Matt Taibbi While He Testified Before Congress

After Elon Musk purchased Twitter in October 2022,³² Twitter granted access to a handful of journalists to review its internal communications to examine the degree to which Twitter colluded with the federal government to censor lawful speech online.³³ The resulting “Twitter Files,” a series of 20 threads published by these journalists, confirmed the existence of the “censorship industrial complex” and its prevalence in stifling free speech.³⁴ The Twitter Files detailed extensively how various federal agencies colluded with Twitter and other Big Tech companies to censor lawful speech and silence dissent online.³⁵ Matt Taibbi, an award-winning reporter,³⁶ was one journalist who contributed to the Twitter Files.

A. Twitter Files journalist Matt Taibbi testified before the Select Subcommittee about how the Biden Administration worked with Big Tech to censor Americans

The Committee and Select Subcommittee have conducted aggressive oversight in the 118th Congress to investigate the degree to which the Executive Branch censored Americans. As a necessary part of this oversight, the Select Subcommittee has convened hearings on the weaponization of the federal government to obtain public testimony about the Executive Branch’s censorship regime.

On March 9, 2023, Mr. Taibbi, along with fellow journalist Michael Shellenberger, testified before the Select Subcommittee about his reporting on the Twitter Files.³⁷ Mr. Taibbi authored 12 of the 20 threads that make up the Twitter Files, including the very first segment.³⁸ During the hearing, Mr. Taibbi described the serious government abuse. He testified:

The original promise of the internet was that it might democratize the exchange of information globally. . . . What we found is in the [Twitter] files was a sweeping effort to reverse that promise and use

³² Kate Conger and Lauren Hirsch, *Elon Musk Completes \$44 Billion Deal to Own Twitter*, N.Y. TIMES (Oct. 27, 2022).

³³ The Editorial Board, *The Twitter Censorship Files*, WALL ST. J. (Dec. 4, 2022); Joseph A. Wulfsohn, *Federal Trade Commission demands Elon Musk ‘identify all journalists’ who had access to Twitter Files*, FOX NEWS (March 7, 2023).

³⁴ Jonathan Turley, *Why efforts to dismiss Musk’s ‘Twitter Files’ by liberal media won’t work this time*, FOX NEWS (Dec. 6, 2022); HEARING ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY (March 9, 2023) [hereinafter: “WEAPONIZATION HEARING”] (testimony of Michael Shellenberger) (“The censorship industrial complex is a network of ideologically-aligned governmental, NGO, and academic institutions that discovered over the last few years the power of censorship to protect their own interests against the volatility and risks of the democratic process.”).

³⁵ See Matt Taibbi, *Capsule Summaries of all Twitter Files Threads to Date, With Links and a Glossary*, RACKET NEWS (Jan 4, 2023).

³⁶ See Dave Maley, *Independent Media Award Winners Announced*, IC NEWS (Mar. 10, 2020) (announcing Mr. Taibbi winning the Park Center for Independent Media at Ithaca College’s 2020 Izzy Award for outstanding achievement in independent media); Press Release, 43rd Annual National Magazine Awards Winners Announced, American Society of Magazine Editors (May 1, 2008) (announcing Mr. Taibbi winning the 2008 Magazine Award for columns and commentary).

³⁷ WEAPONIZATION HEARING (testimony of Matt Taibbi); see *id.* (testimony of Michael Shellenberger).

³⁸ See Taibbi, *supra* note 35.

machine learning and other tools to turn the internet into an instrument of censorship and social control. Unfortunately, our own government appears to be playing a lead role.³⁹

Mr. Taibbi later elaborated on the magnitude of the scandal. He said:

[T]his Twitter Files story and what we’re looking at now and what we’re investigating now . . . is by far the most serious thing that I’ve ever looked at, and it’s certainly the most grave story that I’ve ever worked on, personally.⁴⁰

Mr. Taibbi’s and Mr. Shellenberger’s testimony came on the heels of the Committee’s and Select Subcommittee’s discovery that an arm of the Executive Branch—the Federal Trade Commission—demanded from Twitter the identities of all journalists given access to Twitter’s internal communications.⁴¹ The FTC also demanded Twitter to describe the “nature of access granted [to] each person” and how allowing such access was consistent with Twitter’s privacy and information security obligations under an existing consent order.⁴² Elon Musk responded to the FTC’s demands for information about journalists and said it was “a serious attack on the Constitution by a federal agency” and “a shameful case of weaponization of a government agency for political purposes and suppression of the truth!”⁴³ In his testimony, Mr. Taibbi said in response to the FTC’s weaponization,

I was upset, obviously. . . . This kind of thing—when the government is looking for information about reporters—is usually a canary in the coal mine that something worse is coming in terms of an effort to exercise control over the press. So, on that level, it’s absolutely disturbing.⁴⁴

As an additional layer of attack, during the hearing itself, Democrats on the Select Subcommittee, including Ranking Member Stacey Plaskett and Representative Sylvia Garcia, attempted to slander Mr. Taibbi and Mr. Shellenberger as “so-called journalists” and pressured

³⁹ WEAPONIZATION HEARING (testimony of Matt Taibbi).

⁴⁰ Rep. Mike Johnson (@RepMikeJohnson), TWITTER (Mar. 9, 2023, 11:11 AM), <https://twitter.com/RepMikeJohnson/status/1633862981401321473>.

⁴¹ Ryan Tracy, *FTC Twitter Investigation Sought Elon Musk’s Internal Communications, Journalist Names*, WALL ST. J. (Mar. 8, 2023); see also H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF FED. GOV., *THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION: AN AGENCY’S OVERREACH TO HARASS ELON MUSK’S TWITTER: REPORT OF FINDINGS FOR THE 118TH CONGRESS* (Mar. 7, 2023).

⁴² H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF FED. GOV., *THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION: AN AGENCY’S OVERREACH TO HARASS ELON MUSK’S TWITTER: REPORT OF FINDINGS FOR THE 118TH CONGRESS* (Mar. 7, 2023).

⁴³ Elon Musk (@elonmusk), TWITTER (Mar. 7, 2023, 5:59 PM), <https://twitter.com/elonmusk/status/1633240925429288960>; Elon Musk (@elonmusk), TWITTER (Mar. 7, 2023, 5:22 PM), <https://twitter.com/elonmusk/status/1633231562962780160>.

⁴⁴ WEAPONIZATION HEARING (statement of Matt Taibbi).

them to reveal their sources.⁴⁵ The following exchange between Select Subcommittee Democrats and Mr. Taibbi exemplifies this pressure:

Rep. Plaskett: Who is the individual that gave you permission to access the emails?

Mr. Taibbi: Well, the attribution from my story is sources at Twitter, and that's what I am going to refer to.

Rep. Plaskett: Okay. Did Mr. Musk contact you, Mr. Taibbi?

Mr. Taibbi: Again, the attribution for my story is sources at Twitter.

Rep. Garcia: Mr. Taibbi, I want to follow up a little bit on the Ranking Member's questions. When was the first time that Mr. Musk approached you about writing the Twitter Files?

Mr. Taibbi: Again, Congresswoman . . . I can't give it to you unfortunately because this a question of sourcing and I don't give them. I'm a journalist. I don't give up my sources.

Rep. Garcia: So, you're not going to tell us when Musk first approached you?

Mr. Taibbi: Again, Congresswoman, you're asking a journalist to reveal his sources.

Rep. Garcia: So, then you consider Mr. Musk to be the direct source of all of this?

Mr. Taibbi: No, now you're trying to get me to say that he is the source. I just can't answer your question.

Rep. Garcia: Well, he either is or he isn't. If you're telling me [that] you can't answer because it's your source, well then the only logical conclusion is that he is, in fact, your source. . . . You can't have it both ways.

⁴⁵ *Id.* (statement of Rep. Stacey Plaskett, Delegate, United States Virgin Islands); Brian Flood and Nikolas Lanum, 'Twitter Files' hearing erupts as Matt Taibbi refuses to reveal sources in heated exchange with Democrat, FOX NEWS (Mar. 9, 2023).

Rep. Plaskett: Either Musk is the source and he can't talk about it, or Musk is not the source and if Musk is not the source, then he can discuss his conversations with the source.⁴⁶

B. The IRS conducted an unannounced field visit to Mr. Taibbi's home on the same day he testified before the Select Subcommittee

As Mr. Taibbi testified before the Select Subcommittee, an IRS agent visited, unannounced and unprompted, Mr. Taibbi's home. The agent, after receiving no response from Mr. Taibbi because he was in Washington for his testimony, left a note for Mr. Taibbi to call the IRS four days later.⁴⁷

When Mr. Taibbi called the IRS, the IRS informed him that the agency had rejected his electronic 2018 and 2021 tax return filings due to concerns of identity theft.⁴⁸ However, in 2019, the IRS notified his accountant that it had accepted his 2018 filing, and in the four-and-a-half years since then, the IRS never notified Mr. Taibbi or his accountant of any issue with this return.⁴⁹ With respect to his 2021 return, Mr. Taibbi was aware the IRS rejected his electronic filing twice, even after his accountant filed with an IRS-provided pin number.⁵⁰ However, in both cases, the IRS did not attempt to make contact with Mr. Taibbi by other means before its unannounced field visit. The IRS further informed Mr. Taibbi during the call that the problems were not “monetary” or due to a delinquent amount owed; in fact, the IRS owed Mr. Taibbi a substantial tax return for both years.⁵¹

Due to the circumstances surrounding the IRS's unannounced and unprompted visit to Mr. Taibbi's home—at the exact time that he was testifying to Congress about “the most serious” government abuse he witnessed in his career as a journalist—the Committee and Select Subcommittee set out to determine whether the field visit was a thinly-veiled attempt by the IRS to influence or intimidate a witness before Congress. On March 27, 2023, the Committee and Select Subcommittee sent a letter to the IRS asking about the unannounced field visit to Mr. Taibbi's home.⁵² The Committee and Select Subcommittee provided the IRS with express permission from Mr. Taibbi to receive and review these documents.⁵³

⁴⁶ *Id.*

⁴⁷ E-mail from Matt Taibbi to H. Comm. on the Judiciary (March 21, 2023) (on file with Committee); *see also* Gabe Kaminsky, *'Twitter Files' journalist received IRS agent visit at home the same day he testified in Congress*, WASH. EXAM. (Mar. 28, 2023).

⁴⁸ Letter from Matt Taibbi to H. Comm. on the Judiciary (March 21, 2023) (on file with Committee).

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *See id.* (“[T]he IRS according to its own records owes me a considerable return [for 2018]...again, I had already paid what was owed and more by estimated tax [for 2021].”); Charles Creitz, *Twitter Files journalist rips IRS over home visit after agency finds it owes him money*, FOX NEWS (May 24, 2023).

⁵² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Janet Yellen and Mr. Daniel Werfel, c/o U.S. Dep't of the Treasury and Internal Revenue Serv. (Mar. 27, 2023).

⁵³ Mr. Taibbi signed a waiver to give the Committee and Select Subcommittee access to his tax return information pursuant to 26 U.S.C. § 6103(c).

The curious timing of the IRS’s visit, on the heels of the FTC demand that Twitter turn over names of journalists, raised serious “questions about potential intimidation.”⁵⁴ In Mr. Taibbi’s own words, “[I]t’s hard not to see [my case] as some kind of retaliation or an attempt to intimidate. Maybe not me, but future reporters who would look at this kind of material.”⁵⁵

C. Internal IRS documents revealed how the IRS used a field visit to intimidate Mr. Taibbi

On May 6, 2023, the IRS produced 267 pages of documents, some of which were responsive to the Committee’s and Select Subcommittee’s request.⁵⁶ The IRS asserted that it sent a letter to Mr. Taibbi on October 24, 2019—nine days after Mr. Taibbi filed his 2018 tax return—asking Mr. Taibbi to verify his return because it met identity theft criteria.⁵⁷ The IRS also alleged that it sent a second letter to Mr. Taibbi on March 23, 2020.⁵⁸ However, according to Mr. Taibbi, neither he nor his accountant received either of these letters or any other notification from the IRS that there was an issue with his 2018 tax return before the IRS conducted a field visit at Mr. Taibbi’s home several years later. Furthermore, the IRS failed to include proof of these letters in its production to the Committee and Select Subcommittee.

The IRS’s production revealed that the IRS opened its examination of Mr. Taibbi’s 2018 tax return on December 24, 2022, over three years after the IRS alleged it tried to contact Mr. Taibbi the first time.⁵⁹ Not only was December 24, 2022, a Saturday and Christmas Eve, but it also happened to be just three weeks after Mr. Taibbi published the first Twitter Files thread, detailing government abuses, and the same day that Mr. Taibbi published the ninth segment of the Twitter Files, detailing how federal government agencies “from the State Department to the Pentagon to the CIA” coordinated to censor and coerce speech on various social media platforms.⁶⁰ The IRS’s production failed to explain why the IRS opened its examination of Mr. Taibbi’s tax return on such an unusual date.

The production revealed that one month later, on January 27, 2023, the IRS assigned a revenue officer to Mr. Taibbi’s case to initiate face-to-face contact, rather than attempt to contact Mr. Taibbi through less intrusive means. It was at this point, the IRS alleged, that the officer discovered the IRS had not processed Mr. Taibbi’s 2021 tax return either.⁶¹ The IRS documents revealed that the revenue officer performed an extensive investigation into Mr. Taibbi, using both publicly available search engines and commercial investigative software to compile a

⁵⁴ The Editorial Board, *The IRS Makes a Strange House Call on Matt Taibbi*, WALL ST. J. (Mar. 27, 2023).

⁵⁵ Creitz, *supra* note 51.

⁵⁶ See Letter from Daniel Werfel, Comm’r, Internal Revenue Serv., to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (May 5, 2023).

⁵⁷ *Id.* Mr. Taibbi has consented to the Committee’s and Select Subcommittee’s use of personal information in this report.

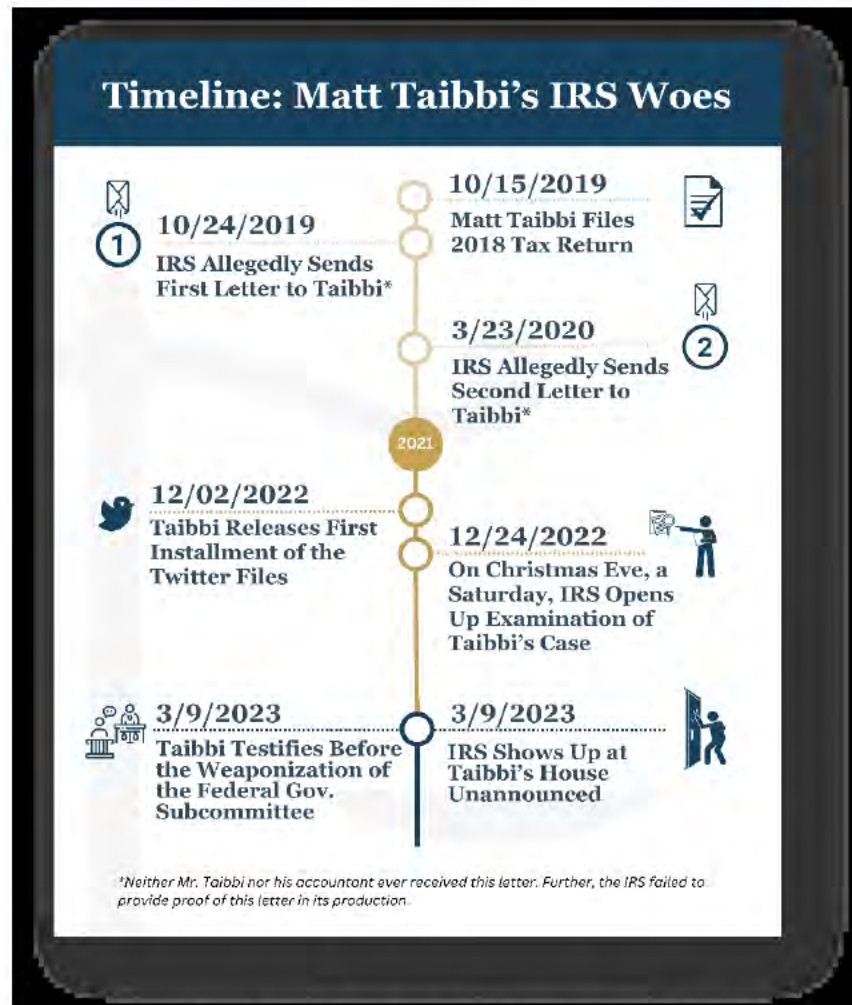
⁵⁸ *Id.*

⁵⁹ Steven Nelson, *IRS opened Matt Taibbi tax probe on Christmas Eve following ‘Twitter Files’ document dump*, N.Y. POST (May 24, 2023); Stephen Dinan, *IRS worked overtime to probe Twitter Files journalist Matt Taibbi*, WASH. TIMES (May 24, 2023).

⁶⁰ See Matt Taibbi (@mtaibbi), TWITTER (Dec. 26, 2022, 12:20 PM), <https://twitter.com/mtaibbi/status/1606701405443874816>.

⁶¹ Letter from Daniel Werfel, Comm’r, Internal Revenue Serv., to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (May 5, 2023).

dossier about Mr. Taibbi. The IRS's dossier on Mr. Taibbi included information such as Mr. Taibbi's voter registration records, whether he possessed a hunting or fishing license, and whether he had a concealed weapons permit. The revenue officer also examined and saved Mr. Taibbi's Wikipedia page, which contained extensive details about Mr. Taibbi's work on the Twitter Files.⁶² Instead of reinitiating contact with Mr. Taibbi by less intrusive means after several years had passed since he filed his 2018 return,⁶³ the revenue officer scheduled its field visit for March 9, 2023—the day Mr. Taibbi was to testify before Congress.



The IRS's production confirmed one crucial fact—Mr. Taibbi did not owe the IRS anything. Rather, the IRS owed Mr. Taibbi a substantial refund. After the IRS's field visit, Mr. Taibbi promptly resolved his tax filing on March 21, 2023. The IRS closed Mr. Taibbi's case the next day, and on March 23, 2023, the IRS sent Mr. Taibbi a Notice of Case Resolution to inform Mr. Taibbi that his case had been closed and that no taxes or tax returns were due.

⁶² See *Matt Taibbi*, WIKIPEDIA, https://en.wikipedia.org/wiki/Matt_Taibbi (last visited Oct. 23, 2023).

⁶³ The IRS claims that the delay in following up with Mr. Taibbi was the result the COVID-19 pandemic restricting field visits. Letter from Daniel Werfel, Comm'r, Internal Revenue Serv., to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (May 5, 2023).

After the Committee and Select Subcommittee sent a follow-up letter to IRS Commissioner Daniel Werfel on May 24, 2023,⁶⁴ the IRS repealed the practice of unannounced field visits altogether. Nevertheless, the IRS’s unannounced visit to Mr. Taibbi’s home only stokes the fear of many Americans that the IRS, flush with its new \$80 billion in funding from Congress, will “unleash its fearsome power against political opponents.”⁶⁵

⁶⁴ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Daniel Werfel, Comm’r, Internal Revenue Serv. (May 24, 2023).

⁶⁵ The Editorial Board, *supra* note 54.

III. The IRS Lied to an Ohio Taxpayer to Gain Access to Her House During an Unannounced Field Visit

In addition to the IRS's harassment of Mr. Taibbi, the Committee and Select Subcommittee learned that the IRS has used similarly abusive tactics against other American taxpayers, including one egregious example from Marion County, Ohio.⁶⁶

A. An IRS agent, using a false name, harassed and intimidated an Ohio taxpayer

On April 25, 2023, an IRS revenue officer conducted an unannounced field visit to the home of a Marion County, Ohio taxpayer. This agent, who introduced himself to the taxpayer as "Bill Haus" with the IRS's Criminal Division, informed the taxpayer he was at her home to discuss issues concerning an estate for which the taxpayer was the fiduciary. After Agent "Haus" shared details about the estate that only the IRS would know, the taxpayer let him into her home. Agent "Haus" told the taxpayer that she did not properly complete the filings for the estate and that she owed the IRS "a substantial amount." Prior to the visit, however, the taxpayer had not received any notice from the IRS of an outstanding balance on the estate.

During the visit, the taxpayer told Agent "Haus" that the estate was resolved in January 2023 and provided him with documentary proof that she had paid all taxes for the decedent's estate. At this point, Agent "Haus" conceded that the true purpose of his visit was not due to any issue with the decedent's estate, rather Agent "Haus" was at the taxpayer's home because the decedent allegedly had several delinquent tax return filings.⁶⁷

Agent "Haus" then furnished several documents to the taxpayer for her to complete. Because these documents included sensitive information about the decedent, the taxpayer offered Agent "Haus" the opportunity to speak with her accountant, which he accepted. However, when her accountant did not answer, the taxpayer called her attorney who immediately and repeatedly told Agent "Haus" to leave the taxpayer's home since the taxpayer had not received any prior notice from the IRS of any issue with the decedent's estate or delinquent tax returns. Agent "Haus" responded aggressively, insisting, "I am an IRS agent, I can be at and go into anyone's house at any time I want to be." At the end of his unannounced visit, Agent "Haus" told the taxpayer he would mail her paperwork for her to execute and threatened that she would have exactly one week to satisfy the remaining balance or he would freeze all her assets and put a lien on her house.

⁶⁶ See The Editorial Board, *The IRS Makes Another House Call*, WALL ST. J. (June 16, 2023). The taxpayer consented to the Committee's and the Select Subcommittee's use of this information.

⁶⁷ On May 4, 2023, Agent Haus's supervisor confirmed with the taxpayer that the decedent only had one delinquent filing from 2016. The supervisor also confirmed the decedent's 1041 final return was completed and that nothing was due.

B. The IRS Agent filed a complaint against the local police department for investigating his unusual conduct

Following the visit, the taxpayer immediately contacted the Marion, Ohio Police Department (MPD) to determine if Agent “Haus” was attempting to scam her.⁶⁸ The officer ran Agent “Haus’s” license plate and discovered the vehicle belonged to an individual whom the taxpayer confirmed was the agent, only Bill Haus was not the name on the registration.⁶⁹ The officer then called Agent “Haus” to verify his identity.⁷⁰ Agent “Haus” attested that he was an IRS agent but admitted Bill Haus was not his real name; he was using an alias.⁷¹ In response to the officer revealing his true identity, Agent “Haus” immediately filed a complaint against the officer with the Treasury Inspector General for Tax Administration (TIGTA).⁷² It was not until a major from the MPD called TIGTA in response to the complaint that the MPD learned Agent “Haus” was a legitimate IRS agent.⁷³

A police report filed by the responding officer detailed how the officer believed Agent “Haus” was truly trying to scam the taxpayer: “[Agent ‘Haus’] advised me that he was an IRS agent and I did not believe him . . . I then called the Summit County Sheriffs Office and explained to them the call that I handled and that it appears that [Agent ‘Haus’] is going around pretending to be an IRS agent[.]”⁷⁴

As detailed by a major at the MPD in correspondence with the Committee and Select Subcommittee, the circumstances surrounding this instance “certainly go[] against the grain of what we believe to be historical practice on the part of the IRS.”⁷⁵ The major indicated that he was surprised to learn that IRS agents are allowed to go by aliases to hide their true names: “I was informed by [the] Agent [at TIGTA] that IRS field agents are given alias names to perform their tasks and to avoid people knowing their true identity. I found this entire situation odd but [the] Agent [from TIGTA] sounded like a legitimate agent in our conversation.”⁷⁶

⁶⁸ Police Report, Marion Cnty. Police Dep’t (Apr. 25, 2023, 2:29 PM) (on file with the Committee).

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *Id.*; *see also* E-mail from Major, Marion Cnty. Police Dep’t, to H. Comm. on the Judiciary (May 1, 2023, 4:01 PM) (on file with the Committee). Prompted by a call from the TIGTA, the taxpayer filed a complaint against the agent on May 9, 2023.

⁷³ E-mail from Major, Marion Cnty. Police Dep’t, to H. Comm. on the Judiciary (May 1, 2023, 4:01 PM) (on file with the Committee).

⁷⁴ Police Report, *supra* note 68.

⁷⁵ E-mail from Major, Marion Cnty. Police Dep’t, to H. Comm. on the Judiciary (May 1, 2023, 4:01 PM) (on file with the Committee).

⁷⁶ *Id.*

To House Committee on the Judiciary

From Major [REDACTED], Marion County Police Department

Mrs. [REDACTED] proceeded to call MPD believing that Haus was likely an imposter and we responded. The agent had already left and it was the belief of our responding officer that this individual was an imposter. The phone interaction that ensued between our officer and the agent was indicative of that belief. Agent Haus then proceeded to tell our officer that he filed a complaint against MPD with the Inspector General and provided us with the following information, demanding that we call the Inspector General's Office to participate in the complaint that he filed against our officers.

Agent Bill Haus
 Identification Number [REDACTED]
 IRS field employee identification center phone number [REDACTED]
 Office of Inspector General [REDACTED]

Haus' business card indicates that he is an "independent". Mrs. [REDACTED] told her that I did not know as I am unfamiliar with their processes.

Treasury Agent [REDACTED] (with office of Inspector General) phone number [REDACTED]

I called the Inspector General's number and spoke with an Agent [REDACTED] who works for Treasury and apparently assists in Inspector General Complaints. He indicated that this matter truly involved a legitimate (non LE) agent of the IRS. The IRS agent took issue with our officers running his license plate that apparently was connected to his personal vehicle and revealed his true name. I was informed by Agent [REDACTED] that IRS field agents are given alias names to perform their tasks and to avoid people knowing their true identity. I found this entire situation odd but Agent [REDACTED] sounded like a legitimate agent in our conversation.

However, even the agent at TIGTA recognized the degree to which Agent "Haus" weaponized his field visit against the Ohio taxpayer. As the major reported, "[The Agent from TIGTA] agreed with me that the agent should have notified MPD that he was in the area working so that we could know that he was legitimate (if he is legitimate)."⁷⁷

He agreed with me that the agent should have notified MPD that he was in the area working so that we could know that he was legitimate (if he is legitimate). When Haus spoke with Ofc. [REDACTED] he told him that they do not have to provide information to local agencies. While this is acknowledged as true, doing so allows us to legitimize his presence to people when they call and try to report an agent as an imposter, as was the case here.

The TIGTA agent assured the major that "the IRS only makes personal visits after receiving no response from the taxpayer."⁷⁸ However, like Mr. Taibbi, the Ohio taxpayer had not received any notice from the IRS about an issue prior to the unannounced field visit.

I again spoke with Agent [REDACTED] this past Friday when Mrs. [REDACTED] came to MPD to collect a copy of the police report. Agent [REDACTED] could only tell me that the version of events I was hearing from Mrs. [REDACTED] were largely the same reported to him by Agent Haus (or whatever his real name is) but he assured me that the IRS only makes personal visits after receiving no response from the taxpayer. He also told me that he has been with the Inspector General for 3 years and he gave me a sense that the IRS approach is changing to an extent that maybe he doesn't fully understand himself.

⁷⁷ *Id.*

⁷⁸ *Id.*

The events left quite the mark on the taxpayer who remained incredibly fearful that Agent “Haus” would return to her house and that the IRS would target her again. As the major reported, “She is truly in fear of this man. What is more concerning, she contacted the IRS, verified she has a zero balance and she indicates that the person she spoke with on the phone had no idea why an agent would be coming to her home.”⁷⁹

When Mrs. ██████ stopped in, she was so concerned with this agent that she was asking our records clerk questions about how to secure her home, fearful that the agent would return and perhaps break into her house. She is truly in fear of this man. What is more concerning, she has contacted the IRS, verified she has a zero balance and she indicates that the person she spoke with on the phone has no idea why an agent would be coming to her home. Could this be a miscommunication between the IRS and their criminal division?

The IRS did nothing to ease the taxpayer’s fears. As the major explained to the Committee and Select Subcommittee, “When [the taxpayer] called the IRS to ask questions about this, she mentioned that the message on the IRS system warns callers to beware of imposters posing as IRS agents.”⁸⁰ Furthermore, the major attested that “MPD has indeed regularly shared information on [its] social media platforms warning of scams and telling our residents that the IRS WILL NOT do many of the things that this woman claims to have experienced.”⁸¹ Searching for clarity, the major stated, “Either [Agent ‘Haus’] is not who he says he is, he does things differently than the IRS has done before, or the IRS has aggressively changed their approach.”⁸²

Agent ██████ (phone number ██████) made clear to me that he could not provide specific details on this matter due to taxpayer privacy laws. While I was not trying to obtain any privileged details, I am certain that Mrs. ██████ is more fearful of this agent than she is of having info shared with her local police department. When she called the IRS to ask questions about this, she mentioned that the message on the IRS system warns callers to beware of imposters posing as IRS agents. MPD has indeed regularly shared information on our social media platforms warning of scams and telling our residents that the IRS WILL NOT do many of the things that this woman claims to have experienced. Either this person is not who he says he is, he does things differently than the IRS has before, or the IRS has aggressively changed their approach.

When the major inquired about how the taxpayer could file a complaint against Agent “Haus” to ensure something like this does not happen to her again in the future, the TIGTA agent told him that “it would be a waste of her time.”⁸³ The major aired his frustrations with how the IRS has either been weaponized or is entirely incompetent:

It is very concerning that the IRS does not know that the IRS is sending agents to the home of a taxpayer. It is concerning to me that they do not have to use their real names and can apparently make threats and so forth, against the narrative that the IRS publicly

⁷⁹ *Id.*

⁸⁰ E-mail from Major, Marion Cnty. Police Dep’t, to H. Comm. on the Judiciary (May 1, 2023, 4:01 PM) (on file with the Committee).

⁸¹ *Id.*

⁸² *Id.*

⁸³ *Id.*

reports. It is concerning for me that it is so difficult for even a police agency to verify the credentials of a federal agent, who took such offense to his identity being challenged that he chose to file a complaint against the MPD officers with the Office of the Inspector General.⁸⁴

Lastly, the major spoke to the quality of the taxpayer and her husband as people, “The[y] . . . seem to be good, well-intentioned people that are easy to identify with. I truly feel bad for their situation (knowing only what they have told me).”⁸⁵

C. The IRS admitted its agent’s actions were improper

On May 4, 2023, the taxpayer spoke with Agent “Haus’s” direct supervisor who confirmed nothing was owed on the estate.⁸⁶ The supervisor apologized to the taxpayer for Agent “Haus’s” conduct and went so far as to admit that “some things that were said were wrong . . . things never should have gotten this far.”⁸⁷ On May 30, 2023, the taxpayer received a letter from the IRS that the case had been closed.⁸⁸ The next day, on May 31, 2023, an IRS liaison told the Committee and Select Subcommittee, “The IRS has long provided training and procedures to promote the proper customer experience, and also for confirming our identity for taxpayers and local law enforcement upon request. The interactions described to us suggest those procedures were not followed.”⁸⁹ Again, the IRS disregarded its own protocol by failing to contact the taxpayer through less intrusive means before conducting an unannounced field visit.

This weaponized behavior from an IRS agent to an American taxpayer—conducting an unannounced field visit, providing an alias, using deception to secure entry into the taxpayer’s home, abusing his authority, and then filing an Inspector General complaint against a police officer examining that matter—is highly concerning and reveals the degree to which the IRS is broken.

⁸⁴ *Id.*

⁸⁵ E-mail from Major, Marion Cnty. Police Dep’t, to H. Comm. on the Judiciary (May 1, 2023, 4:01 PM) (on file with the Committee).

⁸⁶ E-mail from taxpayer to H. Comm. on the Judiciary (May 17, 2023, 4:07 PM) (on file with the Committee).

⁸⁷ *Id.*

⁸⁸ Letter from Internal Revenue Serv. to taxpayer (May 30, 2023).

⁸⁹ E-mail from Internal Revenue Serv. to H. Comm. on the Judiciary (May 31, 2023, 3:57 PM) (on file with the Committee).

IV. As a Result of the Committee’s and Select Subcommittee’s Oversight, the IRS Terminated Its Policy of Conducting Unannounced Field Visits

As a result of the Committee’s and Select Subcommittee’s oversight, the IRS terminated its unannounced field visit policy altogether, ending a decades-long practice that had been weaponized by the IRS and undermined American trust in the agency.⁹⁰

On July 24, 2023, the IRS publicly announced that it would no longer conduct most unannounced field visits to taxpayers’ homes, including those like what occurred with Mr. Taibbi and the Ohio taxpayer.⁹¹ As the IRS confirmed in its announcement: “Effective immediately, unannounced visits will end except in a few unique circumstances and will be replaced with mailed letters to schedule meetings.”⁹² Commissioner Werfel said the policy change was a “common-sense step” to better serve the taxpayers and increase public confidence in the IRS’s work.⁹³ Confidence in the IRS is, and has been, irreparably low in large part due to policies like unannounced field visits that undermine Americans’ trust in an impartial and apolitical IRS.⁹⁴

Commissioner Werfel stated in the IRS press release that unannounced field were a safety risk and that repealing the policy would “improve overall safety for taxpayers and IRS employees.”⁹⁵ The IRS’s attempt to justify its decision as being in the best interest of the safety of its revenue officers lacks concrete evidence. To the extent this data does exist, the IRS has not made it publicly available or supplied it to the Committee or Select Subcommittee.

Commissioner Werfel further used the excuse of scam artists “bombarding taxpayers has increased confusion about home visits” as justification for repealing the IRS’s policy of unannounced field visits.⁹⁶ The Commissioner argued these visits “created extra anxiety for taxpayers already wary of potential scam artists” and promised that the “only losers with this change in policy are scammers posing as the IRS”⁹⁷ However, it was not just scam artists “bombarding” taxpayers and creating confusion about unannounced home visits—it was the IRS itself. The testimony of the Ohio taxpayer and the MPD make clear that the IRS’s own actions

⁹⁰ Press Release, IRS ends unannounced revenue officer visits to taxpayers; major change to end confusion, enhance safety as part of larger agency transformation efforts, Internal Revenue Serv. (July 24, 2023) [hereinafter: “IRS Press Release”].

⁹¹ *Id.*

⁹² *Id.*

⁹³ *Id.*

⁹⁴ Bruce Drake, *On Tax Day, Americans’ views of taxes and the IRS*, PEW RESEARCH CENTER (Apr. 15, 2014) (“We tested 13 government agencies in a survey last fall, and the IRS ranked at the bottom of the list with 51% expressing an unfavorable view of it while 44% regarded it positively. It was the only one of the agencies where a majority did not have a favorable view.”); Oliphant and Cerda, *supra* note 16 (“The least popular federal agency of the 16 asked about is the IRS. About half of Americans (51%) have an unfavorable opinion of this agency, while 42% have a favorable view.”).

⁹⁵ IRS Press Release.

⁹⁶ *Id.*

⁹⁷ *Id.*

generated genuine fear, so much so that the Ohio taxpayer sought advice on how to secure her home in case Agent “Haus” returned.⁹⁸

The Committee’s and Select Subcommittee’s oversight and investigation of the IRS’s abusive actions yielded real results for the American people. The Committee and Select Subcommittee identified how IRS employees abused an IRS policy, and it forced the IRS to reevaluate its policy. Commissioner Werfel stated that ending the policy after decades was “the right thing to do and the right time to end it.”⁹⁹ While the policy should have been ended decades ago, taxpayers no longer have to worry the IRS will come knocking on their door without prior notice.

⁹⁸ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Daniel Werfel, Comm’r, Internal Revenue Serv. (June 29, 2023).

⁹⁹ IRS Press Release.

CONCLUSION

The Committee's and Select Subcommittee's oversight revealed, and led to the swift end of, the IRS's weaponization of unannounced field visits to harass, intimidate, and target taxpayers. Taxpayers can now rest assured the IRS will not come knocking without providing prior notice—something that should have been the IRS's practice all along. No American should fear again an unannounced visit from the powerful tax collector. No American should fall victim to deception from their own government to threaten and pressure them into submission. The details that the Committee and Select Subcommittee gathered about IRS abuses are shocking examples of the federal government's weaponization.

The IRS's swath of new funding and intentions to expand its enforcement activities compel the Committee and Select Subcommittee to stay vigilant for new ways the IRS will inevitably try to abuse its power. This means the Committee's and the Select Subcommittee's oversight of the IRS is only beginning. The Committee and Select Subcommittee are already aware that the IRS is intentionally, and repeatedly, backdating tax documents to levy insurmountable penalties against taxpayers and businesses seeking to lawfully capitalize on available avenues for tax relief.¹⁰⁰ The Committee and Select Subcommittee are also looking into the IRS's continued efforts to chill the political speech of nonprofit organizations.¹⁰¹ Taxpayers deserve better from the IRS; therefore, the Committee's and Select Subcommittee's oversight into the weaponization of the IRS will continue until the agency charts a new course and proves it is no longer a threat to Americans' civil liberties.

¹⁰⁰ Aysha Bagchi, *IRS Sanctioned by Court for 'Bad Faith' on Backdated Document*, BLOOMBERG TAX (Aug. 29, 2023); see also Steve Hayes, *IRS Agents Backdate Documents Filed with the Court—a Felony*, FAIRTAX (June 23, 2023); Miranda Nazzaro, *IRS accused of backdating penalties*, THE HILL (Aug. 21, 2023); Aysha Bagchi, *IRS Asked to Admit to More Easement Penalty Approval Backdating*, BLOOMBERG TAX (Aug. 21, 2023); Caleb Harshberger, *IRS Backdating Court Order Spotlights Culture, Attorneys Say*, BLOOMBERG LAW (Aug. 24, 2023).

¹⁰¹ Bradley A. Smith, *The IRS still plays political speech police*, WASH. EXAM. (May 29, 2023).

II. The Biden-Harris Administration’s coordination with financial institutions to surveil Americans

The Select Subcommittee began an investigation into government-led financial surveillance after a whistleblower disclosed that following the events of January 6, 2021, Bank of America (BoA), voluntarily and without legal process, provided the FBI with a list of names of all individuals who used a BoA credit or debit card in the Washington, D.C. region around that time.¹²⁸ In response to these allegations and corroborating testimony from FBI officials, the Select Subcommittee requested documents from BoA and six other national financial institutions about the provision of Americans’ private financial information to federal law enforcement without legal process.¹²⁹ On March 6, 2024, the Select Subcommittee released an interim report revealing that federal law enforcement had used sweeping search terms like “MAGA” and “TRUMP” to target Americans and even treated purchases of religious texts or firearms as indicators of “extremism.”¹³⁰ That report, “[Financial Surveillance in the United States: How Federal Law Enforcement Commandeered Financial Institutions to Spy on Americans](#),” detailed how federal law enforcement derisively viewed American citizens—treating Americans who expressed opposition to firearm regulations, open borders, COVID-19 lockdowns, vaccine mandates, and the “deep state” as potential domestic terrorists.¹³¹ On March 7, 2024, the Select Subcommittee held a hearing examining how Big Government and Big Banks colluded to surveil Americans’ private financial data.¹³²

After it released the first interim report, the Select Subcommittee requested additional documents and communications from seventeen different entities—including national banks, crowdfunding sites, money service businesses, and the U.S. Treasury Department—to further examine whether the federal government was abusing its access to Americans’ sensitive financial information.¹³³ Upon reviewing these documents, the Select Subcommittee released a second interim report, “[Financial Surveillance in the United States: How the Federal Government Weaponized the Bank Secrecy Act to Spy on Americans](#).” Those documents revealed that federal law enforcement has virtually unchecked access to private financial data, is testing out new methods and technology to embed financial surveillance into the American financial framework, and has deputized the financial sector as an investigative arm.¹³⁴ In particular, the Select Subcommittee received documents indicating that the FBI has manipulated the Suspicious Activity Report (SAR) filing process by encouraging banks to file SARs based on names and

¹²⁸ See Transcribed Interview of Mr. George Hill at 74-76 (Feb. 7, 2023).

¹²⁹ See, e.g., Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer, Bank of Am. Corp. (May 25, 2023).

¹³⁰ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print Mar. 6, 2024).

¹³¹ *Id.*

¹³² *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Government of the H. Comm. on the Judiciary* (Mar. 7, 2024).

¹³³ See, e.g., Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer, Bank of Am. Corp. (Apr. 24, 2024).

¹³⁴ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW THE FEDERAL GOVERNMENT WEAPONIZED THE BANK SECRECY ACT TO SPY ON AMERICANS (Comm. Print Dec. 6, 2024).

selectors the FBI sends to the financial institution.¹³⁵ The FBI uses this practice to obtain warrantless access to Americans' sensitive data.¹³⁶ In addition, the Select Subcommittee discovered that financial institutions confidentially report millions of Americans' transactions to the federal government and that tens of thousands of government officials have access to search and download Americans' financial information from government repositories without ever having to get a warrant.¹³⁷

Although the Select Subcommittee's oversight initially focused on the early days of 2021, further investigation revealed that financial surveillance goes far beyond the targeting of one political ideology. Indeed, Big Government and Big Banks have warped information-sharing into a tool designed to constantly surveil Americans' daily activities.

¹³⁵ *See, e.g., id.* at 28.

¹³⁶ *Id.* at 7, 16, 45.

¹³⁷ *Id.* at 16.



**FINANCIAL SURVEILLANCE IN THE UNITED STATES:
HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL
INSTITUTIONS TO SPY ON AMERICANS**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



March 6, 2024

EXECUTIVE SUMMARY

The Committee on the Judiciary and its Select Subcommittee on the Weaponization of the Federal Government are charged by the House of Representatives with upholding fundamental American civil liberties.¹ As a part of this mission, the Committee and Select Subcommittee have uncovered startling evidence that the federal government was engaged in broad financial surveillance, prying into the private transactions of American consumers. This financial surveillance was not predicated on any specific evidence of particularized criminal conduct and, even worse, it keyed on terms and specific transactions that concerned core political and religious expression protected by the Constitution.

On February 7, 2023, the Committee and Select Subcommittee received testimony from retired Federal Bureau of Investigation (FBI) Supervisory Intelligence Analyst George Hill.² During his transcribed interview, Mr. Hill testified that, following the events at the U.S. Capitol on January 6, 2021, Bank of America (BoA), voluntarily and without legal process, provided the FBI with a list of names of all individuals who used a BoA credit or debit card in the Washington, D.C. region between the dates of January 5 and January 7, 2021.³ Mr. Hill also testified that this BoA “data dump” of customer information also included a list of individuals who had *ever* used a BoA credit or debit card to purchase a firearm, regardless of when or where it was purchased.⁴ This testimony was later confirmed by another former senior FBI official, Joseph Bonavolonta.⁵ In fact, when the BoA information was brought to the attention of Steven Jensen, the then-Section Chief of the FBI’s Domestic Terrorism Operations Section, he acted to “pull” the BoA information from FBI systems because the “leads lacked allegations of federal criminal conduct,” and out of “concern[.]” from where it “originated.”⁶

In response to this testimony, the Committee and Select Subcommittee requested documents from BoA and six other national financial institutions about the provision of Americans’ private financial information to federal law enforcement without legal process.⁷ In the months that followed this initial request, the Committee and Select Subcommittee’s oversight has uncovered the magnitude of law enforcement’s access to private financial records of American citizens.

These documents show that following the events of January 6, 2021, federal law enforcement officials from the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) and the FBI initiated multiple discussions with financial institutions.⁸ These meetings included some of the largest financial institutions in the United States, including Barclays, U.S. Bank, Charles Schwab, HSBC, BoA, Paypal, KeyBank, Standard Chartered, Western Union,

¹ Rules of the U.S. House of Representatives, R. X (2023); H. Res. 12, 118th Cong. (2023).

² Transcribed Interview of Mr. George Hill (Feb. 7, 2023).

³ *Id.* at 74-76.

⁴ *Id.*

⁵ Transcribed Interview of Mr. Joseph Bonavolonta at 13 (May 4, 2023).

⁶ Transcribed Interview of Mr. Steven Jensen at 149, 150, 152 (May 19, 2023).

⁷ *See, e.g.*, Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer of Bank of Am. Corp. (May 25, 2023).

⁸ *See, e.g.*, BofA-HJUD-00000008, 11, 14, 15, 16, 22, 29, 33.

Wells Fargo, Citibank, Santander, JPMorgan Chase, and MUFG.⁹ These meetings were geared toward discussing options for financial institutions to share customer information voluntarily with federal law enforcement outside of normal legal processes.¹⁰

The information obtained by the Committee and Select Subcommittee also shows that law enforcement and private institutions shared intelligence products in the aftermath of January 6 through a web portal run by the Domestic Security Alliance Council (DSAC).¹¹ The DSAC is a public-private partnership led by the FBI's Office of Private Sector and the Department of Homeland Security's (DHS) Office of Intelligence and Analysis.¹² The DSAC promotes the "exchange of security and intelligence information" between the federal government and its 650 "member" companies, collectively comprising "two-thirds of the U.S. Gross Domestic Product" and "35 million employees."¹³ Following January 6, the FBI shared an intelligence product titled "Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach," prepared by the FBI, DHS, and the National Counterterrorism Center (NCTC), with financial institutions to alert them to individuals that may fit the profile of criminal and domestic violent extremists (DVEs).¹⁴

This FBI intelligence product, along with other materials shared by federal law enforcement, detail the extent to which federal law enforcement derisively viewed American citizens. For example, one report shared with financial institutions noted that those Americans who expressed opposition to firearm regulations, open borders, COVID-19 lockdowns, vaccine mandates, and the "deep state" may be potential domestic terrorists.¹⁵ Federal law enforcement used this report and materials like it to commandeer financial institutions' databases and ask the financial institutions to conduct sweeping searches of individuals not suspected of committing any crimes. For example, federal law enforcement suggested that banks filter Zelle payments using keywords like "MAGA" and "TRUMP" as part of an ostensible investigation into the events on January 6, 2021, and also warned that "the purchase of books (including religious texts) and subscriptions to other media containing extremist views," could be evidence of "Homegrown Violent Extremism."¹⁶

FinCEN also distributed materials to financial institutions instructing them on how to use Merchant Category Codes (MCCs) to search through transactions to detect potential criminals or "extremists."¹⁷ These MCCs use keywords to comb through transactions, such as "small arms" purchases or recreational stores such as "Cabela's," "Bass Pro Shop," and "Dick's Sporting Goods."¹⁸ Americans doing nothing other than shopping or exercising their Second Amendment rights were being tracked by financial institutions and federal law enforcement. Despite these

⁹ *Id.*; See also USBANK_HJC_000032.

¹⁰ See, e.g., USBANK_HJC_000032.

¹¹ See, e.g., BofA-HJUD-00000051.

¹² See *About DSAC*, DOMESTIC SECURITY ALLIANCE COUNCIL, <https://www.dsac.gov/about> (last visited Jan. 17, 2024).

¹³ *Id.*

¹⁴ See, e.g., BofA-HJUD-00000040.

¹⁵ BofA-HJUD-00000041, 42.

¹⁶ HJC118_00000006, 7.

¹⁷ See, e.g., HJCSWFG_0000454.PPTX.

¹⁸ *Id.* at 4.

transactions having no criminal nexus, FinCEN seems to have adopted a characterization of these Americans as potential threat actors and subject to surveillance.

Without the FBI whistleblowers' disclosures to the Committee and Select Subcommittee, these documents would not have come to light. While it is alarming enough that federal law enforcement and Bank of America used January 6, 2021, as a pretext for surveilling potentially thousands of Americans without a warrant, the documents received by the Committee and Select Subcommittee show a pattern of financial surveillance aimed at millions of Americans who hold conservative viewpoints or simply exercise their Second Amendment rights. This raises serious concerns and doubts about federal law enforcement's and financial institutions' commitment to respecting Americans' privacy rights and fundamental civil liberties.

As the investigation continues, the Committee and Select Subcommittee will continue to work to understand the extent and status of this widespread financial surveillance while also exploring how Congress could enact legislation to further protect Americans' civil liberties.

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS.....	4
BACKGROUND.....	5
THE STATUTORY FRAMEWORK FOR ACCESS TO AMERICANS’ PRIVATE FINANCIAL DATA.....	8
A. The Right to Financial Privacy Act.....	8
B. Section 314(a) of the USA Patriot Act.....	9
C. The Bank Secrecy Act.....	10
FINANCIAL SURVEILLANCE OF AMERICAN CONSUMERS.....	13
A. Federal law enforcement used informal meetings and backchannel discussions with financial institutions to devise the best methods for gathering Americans’ private financial information.....	13
B. Federal law enforcement circulated politicized materials that evidenced hostility towards conservative viewpoints and weaponized financial institutions’ databases by treating lawful transactions as suspicious.....	14
i. Federal law enforcement shared information equating conservative beliefs with domestic terrorism through a controlled-access portal managed by the “Domestic Security Alliance Council.”.....	14
ii. The FBI commandeered financial institutions’ databases to conduct sweeping searches without an individualized nexus to particularized criminal conduct.....	18
CONCLUSION.....	35

BACKGROUND

As part of the oversight conducted by the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government, the Committee and Select Subcommittee received testimony from retired FBI Supervisory Intelligence Analyst George Hill on February 7, 2023.¹⁹ Mr. Hill testified that Bank of America (BoA) provided the FBI—voluntarily and without any legal process—with a list of individuals who had made transactions in the Washington, D.C., metropolitan area with a BoA credit or debit card between January 5 and January 7, 2021, and that individuals who had previously purchased a firearm with a BoA debit card or credit card were elevated to the top of the list regardless of when or where the purchase was made.²⁰

In his transcribed interview, Mr. Hill stated:

The Bank of America, with no directive from the FBI, data-mined its customer base. And they data-mined a date range of 5 to 7 January [of 2021] any BOA customer who used a BOA product. And by ‘BOA product,’ I mean a debit card or a credit card. They compiled that list. And then, on top of that list, they put anyone who had purchased a firearm during any date. So it was a huge list²¹

Mr. Hill’s testimony was corroborated by the testimony of his former supervisor and former Special Agent-in-Charge of the Boston Field Office, Joseph Bonavolonta.²² Mr. Bonavolonta testified that Boston’s Joint Terrorism Task Force Squad Supervisor, Chief Division Counsel, and Assistant Special Agent-in Charge of Counterterrorism also brought the BoA data to his attention.²³ Mr. Bonavolonta testified:

[A] lead had been sent to our office from a unit within FBI Headquarters that fell under the Office of Private Sector . . . in the body of the lead, there was . . . information that was provided by Bank of America following a certain number of criteria that in essence aggregated a list of individuals that were supposedly living up in the New England area who . . . either had potentially made . . . certain credit card purchases . . . for hotel reservations or plane tickets, or potential purchases at certain gun stores in and around . . . January 6th or planned for the inauguration date.²⁴

Mr. Bonavolonta also testified that, “one of the [list’s] criteria . . . in terms of Bank of America’s data . . . was related to purchases that had been made at either gun shops or, you

¹⁹ See Transcribed Interview of Mr. George Hill (Feb. 7, 2023).

²⁰ *Id.* at 74-76.

²¹ *Id.* at 74.

²² See Transcribed Interview of Mr. Joseph Bonavolonta at 12 (May 4, 2023).

²³ *Id.* at 11.

²⁴ *Id.* at 12.

know, stores that would sell firearms.”²⁵ Mr. Bonavolonta also stated that the BoA customer data was sent to other FBI field offices across the country, including the Springfield, Illinois field office.²⁶

Mr. Bonavolonta’s testimony was further supported by Steven Jensen, the then-Section Chief of the FBI’s Domestic Terrorism Operations Section. In his transcribed interview, Mr. Jensen testified that the FBI “maintain[s] partnerships with the private sector, to include Bank of America” and that he was “aware that they provided information to the FBI,” but that, to his knowledge, the FBI did not ask for this information from BoA.²⁷ Instead, he testified that the information “was certain purchaser transaction records of individuals that Bank of America provided over to the FBI that wasn’t requested by the FBI. It was of their own volition . . . without any process being issued.”²⁸ When that information was brought to his attention, Mr. Jensen acted to “pull” the BoA information from FBI systems because “the leads lacked allegations of federal criminal conduct,” and out of “concern[]” from where “it originated.”²⁹ At a hearing before the Committee on July 12, 2023, FBI Director Chris Wray responded to a question about the BoA information and stated that “a number of business community partners all the time, including financial institutions, share information with us about possible criminal activity In the specific instance that you’re asking about, my understanding is that that information was shared with field offices for information only, but, then, recalled to avoid even the appearance of any kind of overreach.”³⁰

Mr. Hill, Mr. Bonavolonta, and Mr. Jensen’s testimony raise serious concerns about federal law enforcement’s compliance with existing legal processes designed to protect Americans’ financial privacy. In light of these revelations, the Committee and the Select Subcommittee requested information from BoA and six other financial institutions to understand how and to what extent financial institutions worked with federal law enforcement to collect, share, and monitor Americans’ data.³¹ In response to these requests, the Committee and Select Subcommittee have received, to date, over a thousand pages of documents from six of the largest financial institutions in the United States, that, together, are responsible for managing trillions of dollars in assets and millions of Americans’ bank accounts.³² Although the former FBI officials

²⁵ *Id.* at 17.

²⁶ *Id.* at 13.

²⁷ Transcribed Interview of Mr. Steven Jensen at 146-47 (May 19, 2023).

²⁸ *Id.* at 147, 150.

²⁹ *Id.* at 149-50, 152.

³⁰ See *Oversight of the Federal Bureau of Investigation Before the H. Comm. on the Judiciary*, 118th Cong. (2023).

³¹ See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer of Bank of Am. Corp (May 25, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. William S. Demchak, Chief Exec. Officer of PNC Fin. Serv. (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Andrew Cecere, Chief Exec. Officer of U.S. Bancorp (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Charles W. Scharf, Chief Exec. Officer of Wells Fargo (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. William H. Rogers, Chief Exec. Officer of Truist Fin. Corp. (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Ms. Jane Fraser, Chief Exec. Officer of Citigroup (June 12, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. James Dimon, Chief Exec. Officer of JPMorgan Chase & Co. (June 12, 2023).

³² See FEDERAL RESERVE STATISTICAL RELEASE: LARGE COMMERCIAL BANKS (2023); see also Steve Cocheo, *JPMorgan Chase Defends Contrarian Branch Strategy as Deposit-Gathering Machine*, THE FIN. BRAND (May 24, 2023).

who testified before the Committee and Select Subcommittee believed that BoA acted alone in sending customer data to federal law enforcement, the documents indicate that federal law enforcement encouraged financial institutions to engage in financial surveillance of American citizens. These documents shed light on back-channel networks that facilitate discussions between financial institutions and federal law enforcement, as well as the information-sharing methods that federal law enforcement used as part of an ostensible investigation into the events of January 6.

THE STATUTORY FRAMEWORK FOR ACCESS TO AMERICANS' PRIVATE FINANCIAL DATA

The emergence of credit cards, mobile banking, and other digital marketplaces have resulted in an unprecedented amount of private data entrusted to financial institutions, potentially revealing all sorts of sensitive information about a customer.³³ For that reason, financial records have become an important investigative tool for federal law enforcement.³⁴ Still, federal law enforcement's interest in financial records must be weighed against the privacy interests of Americans. Without greater oversight and the necessary legislative reforms reflecting the advances in modern-day banking practices, Americans' private financial data is still vulnerable to the shortcomings of an outdated legal framework and pervasive government surveillance.

In 1976, the Supreme Court of the United States held in *United States v. Miller* that customers of financial institutions have no reasonable expectation of privacy in documents voluntarily conveyed to a third party.³⁵ In effect, that decision meant that law enforcement did not have to obtain a warrant in order to retrieve bank records held by a financial institution.³⁶ The *Miller* decision triggered Congress to enact the Right to Financial Privacy Act of 1978 (RFPA), which afforded some privacy protections to financial records held by a third party.³⁷ Most notably, the RFPA requires law enforcement to utilize certain legal processes as a condition of receiving financial records, subject to a number of exceptions.³⁸ In addition, the Bank Secrecy Act (BSA) imposes additional reporting obligations on financial institutions and Section 314(a) of the USA Patriot Act of 2001 gave federal law enforcement greater access to account information entrusted to financial institutions.³⁹ From the information obtained by the Committee and Select Subcommittee, these pieces of legislation have failed to adequately protect Americans' financial information. What it has left is an expansive, backdoor information-sharing regime led by the nation's most powerful law enforcement agencies and their partners in the financial sector.

A. The Right to Financial Privacy Act

In general, the RFPA protects customer information by limiting access to the "financial records of any customer from a financial institution unless the financial records are reasonably described" and the "government authority" receives customer consent, or the records are disclosed in accordance with certain notice requirements pursuant to an administrative subpoena, search warrant, judicial subpoena, or formal written request.⁴⁰ However, if one of the eighteen exceptions under the RFPA apply, legal process and notice may not be required.⁴¹ In some circumstances, these exceptions allow the FBI and the Financial Crimes Enforcement Network

³³ See Nicholas Anthony, *The Right to Financial Privacy*, CATO (May 2, 2023), <https://www.cato.org/policy-analysis/right-financial-privacy>.

³⁴ See, e.g., FINANCIAL CRIMES ENFORCEMENT NETWORK, LAW ENFORCEMENT OVERVIEW.

³⁵ 425 U.S. 435, 442-46 (1976).

³⁶ See *id.* at 446.

³⁷ See Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423; see also Nicholas Anthony, *supra* note 33.

³⁸ See, e.g., 12 U.S.C. § 3413.

³⁹ See FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN'S 314(A) FACT SHEET; see also FINANCIAL CRIMES ENFORCEMENT NETWORK, THE BANK SECRECY ACT.

⁴⁰ See 12 U.S.C. § 3402; see also 12 U.S.C. §§ 3404-3408.

⁴¹ See, e.g., 12 U.S.C. § 3413(g) (relating to disclosure pursuant to legitimate law enforcement inquiry).

(FinCEN), along with other government authorities, to pursue certain customer bank records without utilizing any legal process.⁴² Doing so, however, may limit the kinds of records the requester may receive.⁴³

Under many circumstances, the exceptions to the RFPA function as the rule. For example, the RFPA does not permit the “withholding of financial records or information required to be reported in accordance” with any other statute or rule⁴⁴ and allows financial institutions to voluntarily notify any “[g]overnment authority that such institution, or officer, employee, or agent has information which *may be relevant to a possible violation of any statute or regulation*.”⁴⁵ The customer has no redress available against the institution for such a disclosure or for its failure to provide the customer with notice.⁴⁶ Another exception to the RFPA allows for “disclosure pursuant to legitimate law enforcement inquiry.”⁴⁷ That exception permits law enforcement to seek the “name, address, account number, and type of account of any customer or ascertainable group of customers associated with a financial transaction or class of financial transactions”⁴⁸ Similarly, the RFPA does not protect . . . against actions initiated by the U.S. Secret Service or other “government authorit[ies] authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities . . . or a government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.”⁴⁹ The FBI is also excepted from the RFPA’s general protections and legal process requirements if the FBI certifies to a financial institution that the records are “sought for foreign intelligence purposes to protect against international terrorism or clandestine intelligence activities.”⁵⁰ The financial institution is generally prohibited from disclosing to any person, including its impacted customers, that any such intelligence-related request has been made.⁵¹

B. Section 314(a) of the USA Patriot Act

Section 314(a) of the USA PATRIOT Act of 2001 required the Secretary of the Treasury to “adopt regulations to encourage regulatory and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities.”⁵² The law authorized “federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 37,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be

⁴² *Id.*

⁴³ *Id.*

⁴⁴ 12 U.S.C. § 3413(d).

⁴⁵ 12 U.S.C. § 3403(c) (emphasis added).

⁴⁶ *Id.*

⁴⁷ 12 U.S.C. § 3413(g).

⁴⁸ *Id.*

⁴⁹ 12 U.S.C. § 3414(a)(1).

⁵⁰ 12 U.S.C. § 3414(a)(5).

⁵¹ 12 U.S.C. § 3414(c).

⁵² FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN’S 314(A) FACT SHEET (Feb. 26, 2019), [https://www.fincen.gov/sites/default/files/shared/314\(a\)%20FACTS%20AND%20FIGURES.pdf](https://www.fincen.gov/sites/default/files/shared/314(a)%20FACTS%20AND%20FIGURES.pdf).

involved in terrorism or money laundering.”⁵³ When a request is received, “financial institutions must query their records for data matches,” and then report whether there is a positive match to FinCEN within two weeks of receiving the request.⁵⁴ These requests are subject to strict confidentiality requirements prohibiting their disclosure.⁵⁵

Put differently, federal law enforcement is able to direct more than 16,000 financial institutions to conduct a search of their financial records if law enforcement “reasonably suspect[s], based on credible evidence,” that the suspected individual or entity is engaging in terrorist activity or money laundering.⁵⁶ If the financial institution identifies a positive match, it reports to FinCEN the name, account and transaction, as well as the social security number, taxpayer identification, passport number or any other identifying information related to the individual.⁵⁷ This is done without any judicial involvement.⁵⁸ The Committee and Select Subcommittee have obtained documents indicating that federal law enforcement invoked its “terrorist activity” authority under Section 314(a) as a part of its investigation into the events at the U.S. Capitol on January 6, 2021.⁵⁹

C. The Bank Secrecy Act

Finally, the Bank Secrecy Act (BSA) authorizes the Department of the Treasury to impose certain far-reaching reporting obligations on businesses and financial institutions.⁶⁰ As part of these requirements, financial institutions must file a Currency Transaction Report (CTR) with FinCEN reflecting the information of any individual involved in any transaction of over \$10,000, including the individual’s government-issued identification and Social Security Number.⁶¹ The BSA also “requires that a bank or other financial institution file a SAR [suspicious activity report] whenever it identifies a ‘suspicious transaction *relevant to a possible violation of law or regulation*,’”⁶² while placing a *de facto* gag order on financial institutions prohibiting the revelation of “any information that would reveal the transaction has been reported” to any third party.⁶³ Indeed, “SARs contain personally identifiable information about

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ 31 C.F.R. § 1010.520(b)(3)(iv)(B).

⁵⁶ 31 C.F.R. § 1010.520(b)(3).

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ TFC000007-8; *see also* Letter from John Adams, Legal Counsel for Truist. Fin. Corp., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary (July 18, 2023) (discussing “several channels through which banks routinely communicate with law enforcement,” that include “responding to requests for account information governed by Section 314(a) of the Patriot Act.”).

⁶⁰ *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, THE BANK SECRECY ACT.

⁶¹ *See, e.g.*, FINANCIAL CRIMES ENFORCEMENT NETWORK, NOTICE TO CUSTOMERS: A CTR REFERENCE GUIDE; *see also Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI) Before the H. Comm. on Financial Services*, 118th Cong. 2 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.) (observing that the value of \$10,000 in 1974 at the time of the BSA’s enactment is roughly worth \$63,900 today).

⁶² Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (emphasis added).

⁶³ *See* 31 U.S.C. 5318(g)(1); *see also* 31 C.F.R. § 1020.320; Letter from Ms. Karen Christian and Mr. Raphael Prober, Legal Counsel for Bank of Am., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary (June 22, 2023) (discussing the Bank Secrecy Act and obligations to “confidentially report potentially suspicious activity”).

individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation . . . subject to strong confidentiality protections”⁶⁴ The BSA also grants broad immunity to “[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency.”⁶⁵ By contrast, failure to file a SAR can result in large monetary penalties.⁶⁶ This creates a strong incentive for financial institutions to file defensively, even when there is little reason to do so.⁶⁷

In other words, the BSA shields financial institutions from ever facing liability for any disclosure made to law enforcement regarding its customers’ transactions—regardless of the financial institutions’ reasonableness or motivations—and the institution never has to disclose to the customer that the transaction was reported to law enforcement, leaving meaningful judicial review lacking. The BSA also cloaks the reporting of a “suspicious transaction” activity report in a nearly impenetrable veil, which some banks have used in an attempt to shield these reports from congressional oversight.⁶⁸ Combined, this framework treats banks as agents of the government and obstructs congressional oversight of federal law enforcement and its relationship with the financial sector, leaving the American financial system ripe for pervasive surveillance. Indeed, the Supreme Court of the United States has expressed skepticism about the BSA’s reporting requirements in considering its constitutionality, noting in a 1974 opinion that the “reporting requirements . . . would pose substantial and difficult constitutional questions” and warning that “the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process.”⁶⁹

To illustrate the breadth of the BSA’s reporting requirements, FinCEN announced that in 2019 it received over 20 million filings from more than 97,000 financial institutions as required by the BSA.⁷⁰ According to FinCEN, those filings “provid[ed] a *wealth of potentially useful* information to [government] agencies”⁷¹ Among those BSA-required filings, FinCEN reported that it received over 4.3 million SARs in 2022, nearly doubling from the number it received in 2019. FinCEN also reported that “Other Suspicious Activities” was the most reported reason for filing a SAR, with “terrorist financing” as one of the least reported SAR activity

⁶⁴ Letter from Corey Tellez, *supra* note 62 at 2.

⁶⁵ 31 U.S.C. 5318(g)(3).

⁶⁶ FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN PENALIZES U.S. BANK OFFICIAL FOR CORPORATE ANTI-MONEY LAUNDERING FAILURES (Mar. 4, 2020) (noting that FinCEN assessed \$450,000 civil penalty against U.S. Bank Official for “failure to prevent violations of the Bank Secrecy Act” and \$185 million civil penalty against U.S. Bank for “willfully violating the BSA’s requirements”).

⁶⁷ *Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI) Before the H. Comm. on Financial Services*, 118th Cong. 4 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.).

⁶⁸ *See, e.g.*, Letter from Ms. Karen Christian and Mr. Raphael Prober, Legal Counsel for Bank of Am., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2-3 (June 22, 2023) (discussing confidentiality under the Anti-Money Laundering Act and Bank Secrecy Act.).

⁶⁹ 416 U.S. 21, 79-80 (1974).

⁷⁰ Nicholas Anthony, *Reporting FinCEN’s Suspicious Activity*, CATO (Apr. 13, 2022), <https://www.cato.org/blog/reporting-fincens-suspicious-activity>.

⁷¹ *Id.* (emphasis added).

types.⁷² This means that FinCEN is using the BSA and its SAR reporting requirements to track far more transactions than just those limited to money laundering and terrorist financing. Similarly, FinCEN reported that it received over 20.6 million CTRs in 2022, averaging to nearly 56,500 per day.⁷³ A CTR contains sensitive financial data and is required to be filed for any transaction over \$10,000, regardless of whether anything about that transaction is “suspicious” or otherwise related to criminal activity.⁷⁴

As a result, a vast amount of personal financial information is regularly shared with FinCEN and, in turn, to other law enforcement agencies via a searchable BSA database.⁷⁵ For example, in 2020, “FinCEN reported that DOJ agencies conducted more than 500,000 searches of SARs through its database.”⁷⁶ However, neither Congress nor American consumers have any real access to examine the propriety of the SARs or law enforcement’s use of them.⁷⁷ The Committee and Select Subcommittee’s investigation has obtained documents revealing that SARs were likely filed on sprawling classes of transactions and individuals despite the lack of any link to criminal—or even “suspicious”—activity.

⁷² FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) YEAR IN REVIEW FOR FY 2022 (2023); *see also Special Report: suspicious activity reports surge; 2023 filings on pace for another record*, THOMSON REUTERS (June 9, 2023).

⁷³ FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) YEAR IN REVIEW FOR FY 2022 (2023).

⁷⁴ *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, NOTICE TO CUSTOMERS: A CTR REFERENCE GUIDE.

⁷⁵ U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-22-105-242, BANK SECRECY ACT: ACTION NEEDED TO IMPROVE DOJ STATISTICS ON USE OF REPORTS ON SUSPICIOUS FINANCIAL TRANSACTIONS at 12 (2022).

⁷⁶ *Id.*

⁷⁷ *See, e.g.*, 31 U.S.C. 5318(g)(2)(A); 31 C.F.R. § 1020.320(e)(1).

FINANCIAL SURVEILLANCE OF AMERICAN CONSUMERS

The Committee and Select Subcommittee have obtained documents showing that federal law enforcement’s investigation, predicated on the events that transpired at the U.S. Capitol on January 6, 2021, devolved into a fishing expedition for Americans’ financial data. Federal law enforcement agencies, including FinCEN and the FBI, treated lawful transactions as suspicious and shared information with financial institutions through backdoor channels, often circulating materials exhibiting a clear animus towards conservative viewpoints. In addition, FinCEN and the FBI relied on Zoom discussions, private and online government-run portals, as well as sweeping searches of financial institutions’ records to conduct its investigation. Given the important civil liberties at stake, federal law enforcement’s overreach and political bias is alarming.

A. Federal law enforcement used informal meetings and backchannel discussions with financial institutions to devise the best methods for gathering Americans’ private financial information.

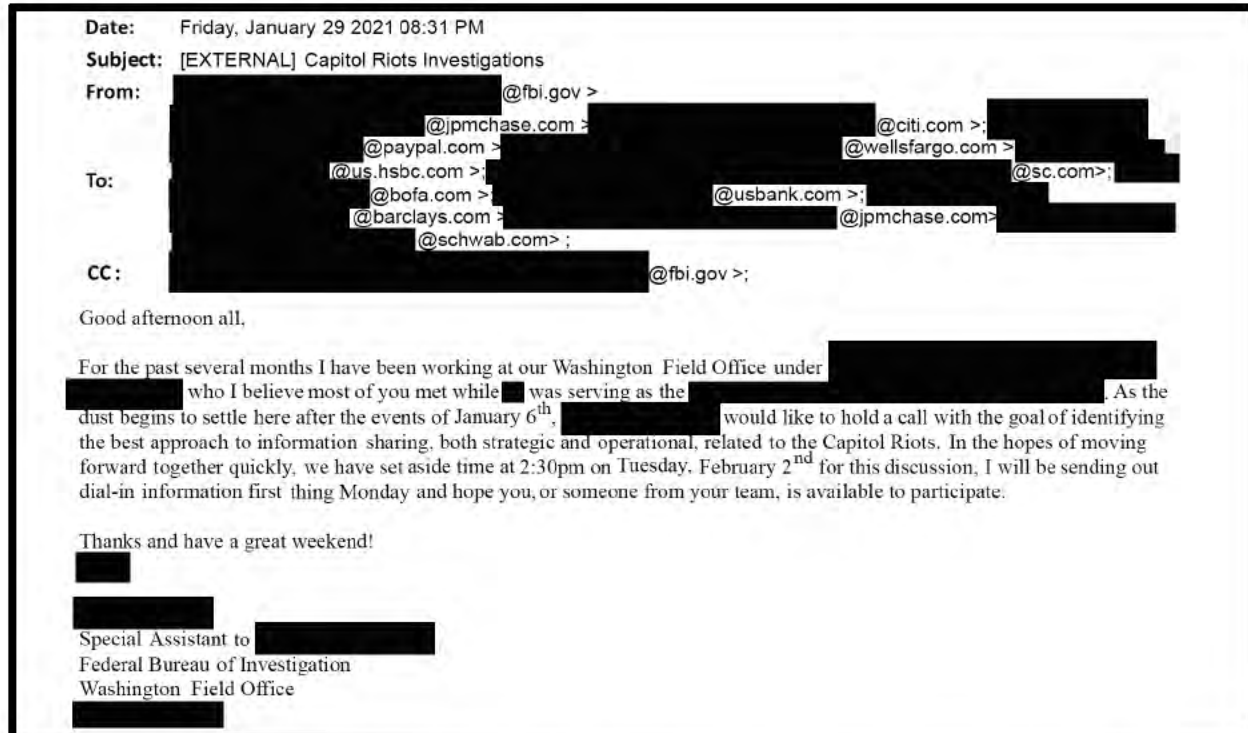
Federal law enforcement officials organized Zoom discussions with financial institutions as part of their investigation into the events of January 6, 2021.⁷⁸ Participants in these meetings included Barclays, U.S. Bank, Charles Schwab, HSBC, BoA, Paypal, KeyBank, Standard Chartered, Western Union, Wells Fargo, Citibank, Santander, JPMorgan Chase, Union Bank, and MUFG.⁷⁹ In one meeting, an FBI official from the Washington Field Office reached out to a number of financial institutions to arrange a meeting with the goal of “identifying the best approach to information sharing, both strategic and operational,” in the wake of the events of January 6.⁸⁰ At least five other Zoom meetings were scheduled by FinCEN officials and financial institutions and included the subject “Capitol Riots.”⁸¹ Viewed together, these meetings suggest that federal law enforcement officials were brainstorming informal methods—outside of normal legal processes—for obtaining private customer information from financial institutions.

⁷⁸ See, e.g., BofA-HJUD-00000008, 11, 14, 15, 16, 22, 29, 33; USBANK_HJC_000032 [hereinafter “Zoom Meetings”].

⁷⁹ *Id.*

⁸⁰ USBANK_HJC_000032.

⁸¹ Zoom Meetings, *supra* note 78.



B. Federal law enforcement circulated politicized materials that evidenced hostility towards conservative viewpoints and weaponized financial institutions’ databases by treating lawful transactions as suspicious.

Federal law enforcement circulated materials to financial institutions as part of an information-sharing operation that alerted financial institutions to the risk of customers and accounts that may be associated with conservative views.⁸² In particular, federal law enforcement attempted to cast swaths of lawful and otherwise harmless transactions as potentially suspicious.⁸³ Given that these materials were distributed to some of the largest financial institutions and companies in the world, their reach could potentially impact the transactions and accounts of hundreds of millions of customers without the customers ever knowing it.

i. Federal law enforcement shared information equating conservative beliefs with domestic terrorism through a controlled-access portal managed by the “Domestic Security Alliance Council.”

One way that information is shared from federal law enforcement to certain corporations and financial institutions is through an obscure government-run portal led by the Domestic Security Alliance Council (DSAC) that is only accessible to its “members.”⁸⁴

⁸² See, e.g., HJCSWFG_0000454.PPTX.

⁸³ See, e.g., BofA-HJUD-00000225.

⁸⁴ About DSAC, DOMESTIC SECURITY ALLIANCE COUNCIL, <https://www.dsac.gov/about> (last visited Jan. 17, 2024); see also BofA-HJUD-00000051.

The DSAC is a program spearheaded by the FBI’s Office of Private Sector Engagement Programs and Initiatives (OPS) and the Department of Homeland Security’s Office of Intelligence and Analysis that promotes “timely and effective exchange of security and intelligence information between the federal government and the private sector.”⁸⁵ According to the official website, the DSAC is a “corporate membership program,” that requires all of its members to be “for-profit” and “generate a minimum of \$1 billion in annual revenue”⁸⁶ Its mission includes facilitating “enduring relationships among its private sector member companies, across the FBI enterprise, and with the Department of Homeland Security (DHS) Headquarters . . . to detect, prevent, and deter criminal acts.”⁸⁷ Since its creation in 2005, “[t]he DSAC program has grown to include more than 650 member companies . . . collectively account[ing] for nearly two-thirds of the U.S. Gross Domestic Product and employ[ing] more than 35 million people.”⁸⁸ Through the DSAC portal, among other avenues, the FBI, DHS, and other government agencies are able to share non-public intelligence products, including Liaison Information Reports, with members of the private sector.⁸⁹

One such intelligence product, titled “Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach,” was shared as a Liaison Information Report and prepared by the FBI, DHS, and the National Counterterrorism Center (NCTC).⁹⁰ The FBI’s Office of Private Sector shared the report with financial institutions and other DSAC members on January 18,

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ FEDERAL BUREAU OF INVESTIGATION, OFFICE OF PRIVATE SECTOR, PRIVATE SECTOR ENGAGEMENT PROGRAMS AND INITIATIVES.

⁹⁰ BofA-HJUD-00000040.

2021 to “alert private sector partners that the 6 January 2021 violent breach by suspected domestic violent extremists (DVEs) into the U.S. Capitol Building may serve as a driver for a diverse set of DVEs.”⁹¹ In the report, the FBI described reasons that “may play in mobilizing criminal actors and DVEs to violence.”⁹² Among the reasons that may mobilize DVEs to violence is “the belief in the existence of global or ‘deep state’ actors who work to manipulate various social, political and/or economic conditions”⁹³ It also assesses that “DVEs’ efforts to engage in violence at lawful gatherings will probably increase throughout 2021, as some DVEs perceive increased socio-political pressures.”⁹⁴ Those “pressures” mobilizing DVEs to violence, in the eyes of the FBI, included opposition to “firearm legislation, the easing of immigration restrictions, and new limits on the use of public land,” as well as “narratives by DVEs that the 2020 General Election was illegitimate,” or “discontent with renewed measures to mitigate the spread of COVID-19, the ordered dissemination of COVID-19 vaccinations, and the efficacy and/or safety of COVID-19 vaccinations.”⁹⁵

⁹¹ BofA-HJUD-00000040 (email from FBI to BoA “attach[ing] LIR titled ‘Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach’” and referencing the report as an “addition to” the “daily *Overnight News*” intelligence shared via the DSAC portal) (emphasis added); *see also* BofA-HJUD-00000041, 42, 43 (including LIR report); USBANK_HJC_000037.

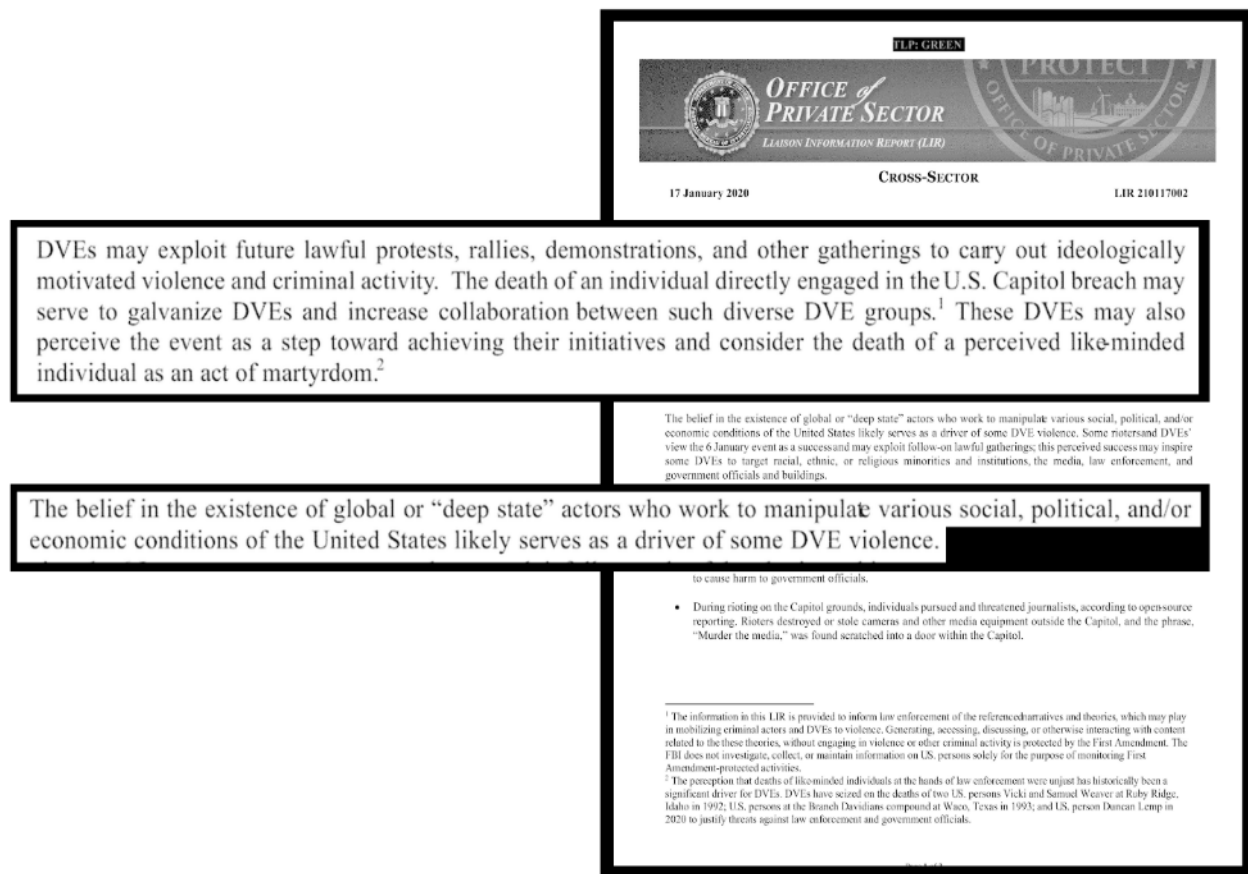
⁹² *Id.* at 41.

⁹³ *Id.*

⁹⁴ *Id.* at 42.

⁹⁵ *Id.*

In other words, according to the FBI, an American citizen’s opposition to firearm regulations, open borders, or COVID-19 lockdowns and vaccine mandates—all of which are viewpoints protected by the First Amendment to the Constitution—“feed into” an “existing narrative many DVEs subscribe to regarding the U.S. government’s exercise of power.”⁹⁶ Put another way, expressing a belief in the existence of the “deep state,” support for typical conservative policies with respect to firearms or immigration, or doubt about the conventional narrative, may result in an individual being labeled by the FBI as a “DVE Actor” and “Likely to Pose [an] Increasing Threat at Lawful Protests, Rallies, [and] Demonstrations. . .”⁹⁷ It is disturbing that the most powerful law enforcement agency in the country would consider views widely held by millions of Americans as the signs of domestic violent extremism. Worse yet, the federal government endorsed this determination with its partners by sharing the report with the largest and most powerful for-profit corporations in the world to alert them about potential “threat[s]” from the people it describes.⁹⁸



Astoundingly, the FBI’s report was an incredibly tone-deaf exercise of government gaslighting. In a clear example, the report deplored the belief in the existence of a “deep state” as

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Id.* at 40; see also FEDERAL BUREAU OF INVESTIGATION, OFFICE OF PRIVATE SECTOR, PRIVATE SECTOR ENGAGEMENT PROGRAMS AND INITIATIVES.

indicative of domestic violent extremism.⁹⁹ Ironically, the report itself was likely shared through a secret, government-run information-sharing portal that is only accessible to the government and some of the largest “for-profit companies” in the world.¹⁰⁰ To put a finer point on this hypocrisy, the report defines “deep state actors” as those who “work to manipulate various social [and] political” conditions.¹⁰¹ In the same breath, the report acknowledges the existence of “removal efforts” of social media platforms against potential domestic violent extremists.¹⁰² In effect, the report admits that social media companies are engaging in censorship—or the “manipulat[ion]” of speech—while labeling those who believe in the existence of such manipulation as potential domestic terrorists.¹⁰³

ii. The FBI commandeered financial institutions’ databases to conduct sweeping searches without an individualized nexus to particularized criminal conduct.

The Fourth Amendment to the Constitution protects against unreasonable searches and seizures by the federal government.¹⁰⁴ The founders likely would have never imagined a circumstance in which the federal government would conduct mass surveillance of Americans’ financial data. Yet, the information available to the Committee and Select Subcommittee shows how federal law enforcement sought sweeping searches of financial institutions’ customer databases without legal process, and even circulated materials instructing financial institutions on how to conduct those searches using Merchant Category Codes (MCCs) and other materials to alert them to customers likely to be associated with conservative political views.

1. The FBI contacted Bank of America directly and provided extremely broad search terms for querying its database and sharing any potential matches with federal law enforcement.

At 9:56 a.m. on January 15, 2021, an FBI official emailed BoA with the subject line “upcoming SAR product idea/brainstorming and check-in with you both.”¹⁰⁵ In the body of that email, the FBI official wrote that “[i]f either or both of you have time this morning to discuss SARs [Suspicious Activity Reports] and a couple ideas, that would be great.”¹⁰⁶

⁹⁹ *Id.* at 41.

¹⁰⁰ See BofA-HJUD-00000040, *supra* note 91; see also, e.g., BofA-HJUD-00000054 (Jan. 28, 2021, email from DSAC Portal to BoA (showing the DSAC portal distributing intelligence products titled “*Overnight News* – January 28, 2021” and suggesting distribution of the Liaison Information Report via the DSAC portal.) (emphasis added).

¹⁰¹ BofA-HJUD-00000041.

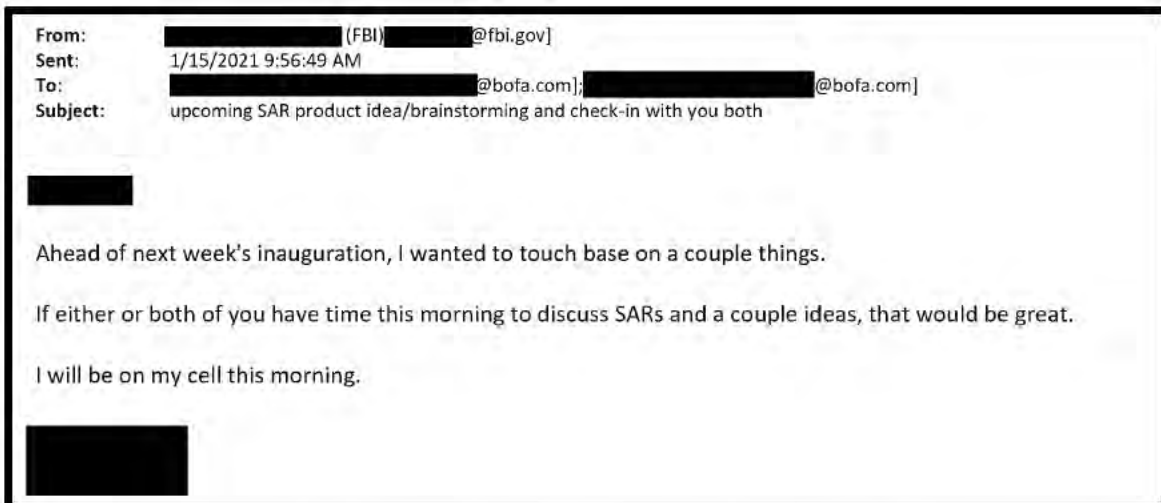
¹⁰² BofA-HJUD-00000041.

¹⁰³ Compare BofA-HJUD-00000041 with BofA-HJUD-00000042.

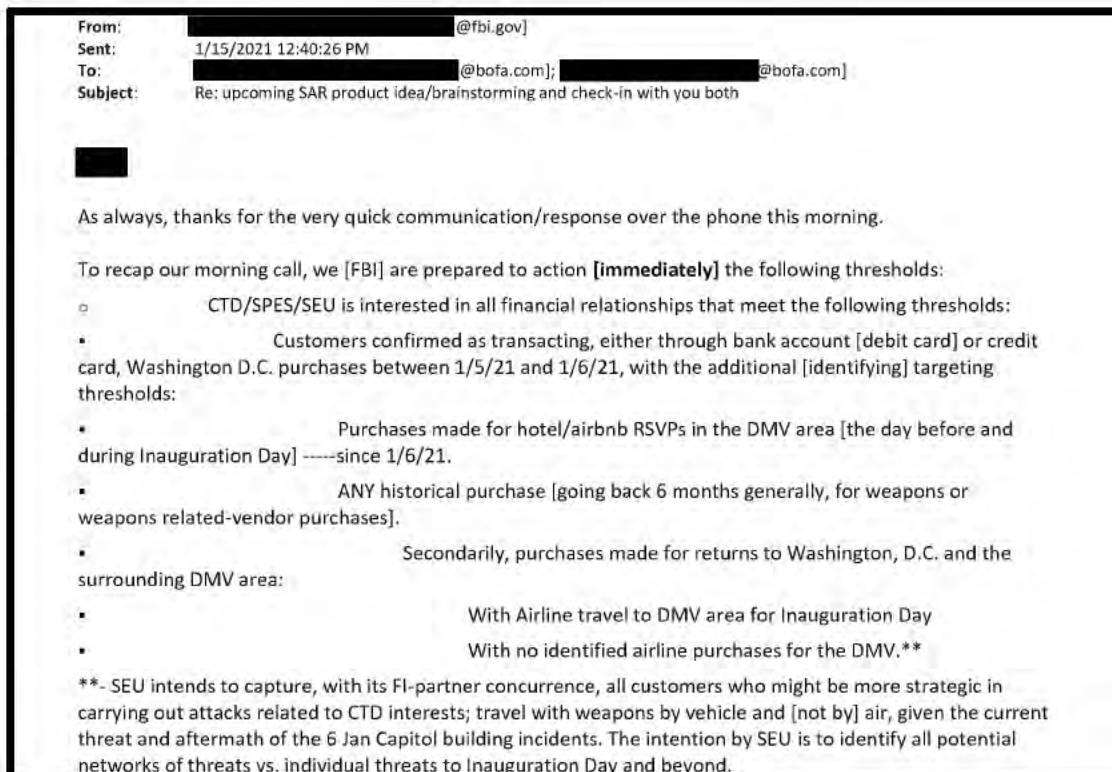
¹⁰⁴ U.S. Const. amend. IV.

¹⁰⁵ BofA-HJUD-00000001.

¹⁰⁶ *Id.*



In a subsequent email just a couple of hours later, the FBI told BoA “thanks for the very quick communication/response over the phone this morning . . . [t]o recap our morning call, we [FBI] are prepared to action **[immediately]** the following thresholds,” supplying BoA with broad search thresholds for querying the financial transactions of its customers for potential matches.¹⁰⁷ The FBI explained that it “is interested in all financial relationships” of any BoA customer transacting in Washington, D.C. and that made “ANY historical purchase” of a firearm, or that had purchased a hotel, Airbnb, or airline travel within a given date range.¹⁰⁸



¹⁰⁷ BofA-HJUD-00000002.

¹⁰⁸ *Id.*

Just one day later, BoA confirmed to the FBI that it was “doing some work around the parameters we discussed and should have something out before the end of the weekend.”¹⁰⁹ BoA delivered as promised. On the evening of Sunday, January 17, 2021, BoA replied to the FBI indicating that it had compiled a product that was responsive to the FBI’s parameters, explaining “you [FBI] should have an email from [redacted]@bofa.com with our filing on the parameters you discussed with [redacted] last week.”¹¹⁰

From: [redacted]@bofa.com]
Sent: 1/17/2021 7:54:23 PM
To: [redacted]@fbi.gov'; [redacted]@fbi.gov]
CC: [redacted]@bofa.com]; [redacted]@bofa.com]
Subject: RE: [SecMail:] secmail:RE: Follow-up

[redacted] -- you should have an email from [redacted]@bofa.com with our filing on the parameters you discussed with [redacted] last week.

Thanks,
[redacted]

From: [redacted]@fbi.gov [mailto:[redacted]@fbi.gov]
Sent: Saturday, January 16, 2021 11:26 AM
To: [redacted]@bofa.com>
Cc: [redacted]@bofa.com>; [redacted]@bofa.com>; [redacted]@fbi.gov
Subject: RE: secmail:RE: Follow-up

[redacted]

Great. Thanks. I will run with the info.

[redacted]

From: [redacted]
Sent: Sat, 16 Jan 2021 15:16:38 +0000
To: [redacted] (FBI)
Cc: [redacted]
Subject: Follow-up

Hi [redacted]

Following up from our conversation yesterday morning, we are doing some work around the parameters we discussed and should have something out before the end of the weekend.

¹⁰⁹ BofA-HJUD-00000197.

¹¹⁰ *Id.*

This massive search request, sent directly from the FBI to BoA, appears to have occurred via direct email, without any legal process or individualized criminal nexus.¹¹¹ As a result, a “filing” was created that was seemingly a “data dump” of BoA account information—reflecting potentially thousands of customers—that was turned over to the FBI.¹¹²

The Committee and Select Subcommittee requested, and subsequently subpoenaed, this “filing” from BoA.¹¹³ The Committee and Select Subcommittee also offered to accommodate BoA by allowing “redact[ions] to protect personal identifiable information.”¹¹⁴ Despite this, BoA declined to produce the requested documents, writing “[e]ven though a subpoena has now been issued, federal law, including the Anti-Money Laundering Act and the Bank Secrecy Act, together with their implementing regulations, still would prevent the Bank from disclosing certain documents.”¹¹⁵

While BoA has refused to provide the Committee and Select Subcommittee with its “filing on the parameters” it discussed and shared with the FBI, it is clear that the FBI was not interested in particularized criminal activity.¹¹⁶ Rather, the FBI cast a wide net with its search parameters and used BoA’s database to identify responsive accounts, creating a sprawling file of individuals whose financial accounts were flagged for federal law enforcement without any particularized allegation of engaging in federal criminal conduct. It is highly disturbing for any huge financial institution to comply with such a sweeping request from federal law enforcement and hand over its customers’ information without any legal process or regard for the privacy of its customers’ information.¹¹⁷

2. FinCEN, in coordination with a select group of financial institutions, shared Merchant Category Codes and politicized search terms and typologies for financial institutions to probe their databases for problematic accounts or transactions.

In addition to the sweeping requests from the FBI to financial institutions, FinCEN circulated materials to financial institutions containing instructions on how to search their databases and flag certain transactions using Merchant Category Codes (MCCs), typologies, and other key terms, phrases, or groups of concern. MCCs are used by “[p]ayment brands, issuers and acquirers . . . to categorize, track and restrict transactions” and can be used for “tax reporting, interchange promotion and gathering information about cardholder purchasing behavior.”¹¹⁸ MCCs, therefore, are a powerful tool for monitoring and restricting customer

¹¹¹ *See id.*

¹¹² *See id.*

¹¹³ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer of Bank of Am. Corp. (Nov. 16, 2023).

¹¹⁴ *Id.* at 4.

¹¹⁵ Letter from Ms. Karen Christian and Mr. Raphael Prober, Legal Counsel for Bank of Am., to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Dec. 15, 2023) (discussing the Anti-Money Laundering Act and the Bank Secrecy Act as “prevent[ing] the Bank from disclosing certain documents”).

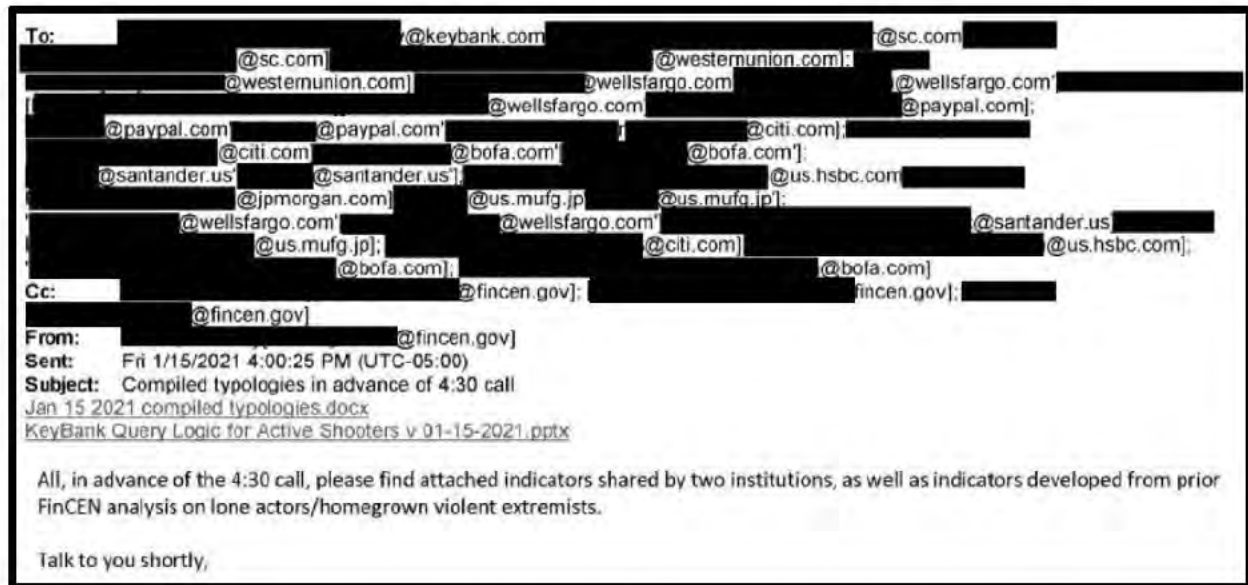
¹¹⁶ BofA-HJUD-00000002.

¹¹⁷ *See* BofA-HJUD-00000197; FEDERAL RESERVE STATISTICAL RELEASE, LARGE COMMERCIAL BANKS (2023).

¹¹⁸ *E.g.*, CITIBANK, MERCHANT CATEGORY CODES (2015), <https://www.citibank.com/tts/solutions/commercial-cards/assets/docs/govt/Merchant-Category-Codes.pdf>. For example, transactions related to “Motor Vehicle Supplies

purchases. The use of select MCCs and politicized search terms and phrases suggest a concerted effort to target a certain segment of the American population. Even worse, they show how federal law enforcement leveraged its relationship with financial institutions to search transactions and account records without legal process or the customers' knowledge or approval.

a. FinCEN provided financial institutions with politicized materials casting conservative points of view and lawful purchases as suspicious.



On January 15, 2021, at 4:00 P.M., FinCEN circulated two attachments to various financial institutions titled “Jan 15 2021 compiled typologies” and “KeyBank Query Logic for Active Shooters v. 01-15-2021.”¹¹⁹ These attachments provided financial institutions with suggested search terms—such as “AMERICA FIRST,” “TRUMP,” and “MAGA”—to use for identifying transactions that may be an indication “of involvement in riots or potential violence.”¹²⁰

and New Parts” may be identified with the MCC “5013” and transactions made at “Grocery Stores” may use the MCC “5411.”

¹¹⁹ HJC118_0000005 (showing email from FinCEN distributing “search terms” and “compiled typologies” of “extremism indicators” and “KeyBank Query Logic” PowerPoint slides as attachments to KeyBank, Standard Chartered, Western Union, Wells Fargo, Paypal, Citibank, Bank of America, Santander, HSBC, MUFG, and JPMorgan).

¹²⁰ HJC118_0000006.

1) Bank submission:

One of the things we've done is search Zelle payment messages for indications of involvement in the riots or potential violence. Here are the key words we used below to pull the data. [...] from our initial analysis "Storm the", "Capitol", "white power" and "Antifa" seem to be yielding the best results.

%PRESIDENT%
 %PREZ%
 %TRUMP%
 %KAMALA%
 %BIDEN%
 %DIE%
 %KILL%
 %SHOOT%
 %BLOW%
 %GUN%
 %DEATH%
 %MURDER%
 KRAKEN
 ANTIFA
 LAST SONS
 OATH KEEPER
 WHITE POWER
 CAPITOL
 STORM THE
 CIVIL WAR
 GROYPER ARMY
 CAMP AUSCHWITZ
 AMERICA FIRST
 THREEPERS
 MILITIA
 CAPITAL
 MAGA
 PATRIOT
 BOOGALOO
 PROUD B%
 CIVIL WAR
 PELOSI
 PENCE
 Schumer

2) Lone Actor/Homegrown Violent Extremism Indicators (developed from prior FinCEN analysis)

- ✓ Long periods of account inactivity, or show normal usage, but in the months or years preceding an attack, a sudden surge or change in activity type.
- ✓ Sudden purchase of firearms, firearm parts and accessories, ammunition, tactical gear at outdoor supply stores, and purchases at shooting ranges not commensurate with previously known customer behavior.

In addition, the documents include a "prior FinCEN analysis" suggesting indicators of potential "Lone Actor/Homegrown Violent Extremism."¹²¹ Those indicators included, among other items, "frequent ATM withdrawals and wire transfers with no apparent economic or business purpose"; "transportation charges, such as bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose"; "purchases that appear excessive or unusual for hobbyist or other legitimate use"; "the purchase of books (including religious texts) and

¹²¹ HJC118_000006.

subscriptions to other media containing extremist views”; and “donations to organizations known to promote radicalism.”¹²²

- ✓ Frequent cash deposits of unknown origin, followed by debit or credit card purchases at retailers not commensurate with previously known customer purchase activity.
- ✓ Frequent ATM withdrawals and wire transfers with no apparent economic or business purpose.
- ✓ Sudden account closings, asset liquidations, and disbursements in days or weeks leading up to attacks.
- ✓ Life insurance policy purchases not commensurate with typical behavior for the type of account holder.
- ✓ Transportation charges, such as bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose or not commensurate with the previous travel history of the customer, for example, travel to high-risk areas or indirect flightpaths for no apparent legitimate reason.
- ✓ Purchases that appear excessive or unusual for hobbyist or other legitimate use.
- ✓ The purchase of pre-cursor chemicals, fireworks, or potential bomb-making equipment, for example, ammonium nitrate, citric acid, aluminum powder, triacetone triperoxide [TATP], potassium nitrate, red iron oxide, tannerite, lengths of piping, BB pellets, cell phones, and others.
- ✓ Purchases of international calling cards not commensurate with previously known customer behavior.
- ✓ The purchase of books (including religious texts) and subscriptions to other media containing extremist views.
- ✓ Donations to organizations known to promote radicalism.

As shown, the list, prepared by FinCEN, demonstrates that federal law enforcement is interested in scrutinizing otherwise lawful transactions such as “ATM withdrawals,” transportation-related expenses for “no apparent legitimate reason,” “donations to organizations known to promote radicalism,” and “the purchase of books (including religious texts) and subscriptions to other media containing extremist views.”¹²³ In other words, the federal government broadly enlisted financial institutions to flag certain kinds of purchases made by Americans that the government deemed to be unnecessary—*e.g.*, taking trips for “no apparent legitimate reason”—or extreme—*e.g.*, purchasing certain books or “religious texts.”¹²⁴ There is no indication in the documents that FinCEN recognized the serious civil liberty concerns associated with its demands or took any steps to protect Americans’ financial privacy.

In the same email, FinCEN also circulated a PowerPoint slide deck as an attachment, authored by KeyBank, titled, “KeyBank’s Query Logic for Active Shooters,” that “intends to detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (‘Lone Wolves’).”¹²⁵ That slideshow showed in stark terms how federal authorities and financial institutions can weaponize MCCs to identify and target Americans using the financial system.

¹²² HJC118_0000007.

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ HJCSWFG_0000454.PPTX. at 2.

Active Shooter Detection – Intent of Query

- Intends to detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (“Lone Wolves”).
- Assumes individuals are creatures of habit and tend to frequent and/or shop at the same places when buying the same or similar items, rather than purchasing the same thing at multiple merchants or vendors.
 - Looks for purchases at multiple merchants or vendors who sell weapons and/or ammunition over a shorter period of time.
- Looks for “bursts” of potential suspicious purchase activity, especially when activity not seen previously.
 - Run query periodically, using a rolling lookback period of 60 days.
- Focuses on credit / debit card transaction activity with merchant / vendor counterparties.
 - Looks at specific counterparty Merchant Category Classification Codes (MCC Codes) and distinct merchant IDs.
 - MCC Codes are used by credit card companies to classify merchant businesses into market segments and industries, with each merchant / vendor location having a unique merchant ID.
 - No minimum dollar threshold for individual transactions.
 - Uses an iterative feedback loop process to build out and refine the exclusion and inclusion keyword lists (detailed in the next slides).
 - Limitations – Due to a lack of industry identifiers for counterparties for other transaction types, does not look at cash, check, ACH, or wire transactions at this time.
- SARs filed for public safety / law enforcement awareness purposes.
- **Alert Example** – John Doe makes 5 credit card purchases at 4 different gun shops, plus makes 4 charges at 3 gun ranges, spending \$3,000 on weapons-related transactions over a 5 week period. Doe does not appear to have any previous firearms purchases.

Classification: KeyCorp Confidential

1



The concern around the use of MCCs to sift through and flag certain purchases on behalf of federal law enforcement is well-documented. For example, in September of 2022, after being petitioned by Amalgamated Bank—an institution that leverages financial power to promote “sustainable organizations, progressive causes, and social justice”¹²⁶—the International Organization for Standardization (ISO) announced its intent to create a separate MCC for the sale of firearms in America with the unabashed support of gun control advocates.¹²⁷ That announcement sparked an outcry from many Americans who opposed ISO’s announcement out of fear that it would be used to track, harass, and limit firearm vendors’ and purchasers’ access to financial services.¹²⁸ As a result of the pressure, the program was reportedly put on pause.¹²⁹ However, the Committee and Select Subcommittee’s investigation has revealed that similar MCCs are already being weaponized against customers by financial institutions in collusion with federal law enforcement.¹³⁰

The KeyBank slide deck also included slides that provided financial institutions with search query logic terms and instructions on how to search through their transactions and accounts in order to “detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (‘Lone Wolves’).”¹³¹ These slides detail how financial institutions can wield MCCs, merchant IDs, and other keyword searches to monitor customer transactions for “suspicious” activity. As the previous slide

¹²⁶ AMALGAMATED BANK, <https://amalgamatedbank.com/who-we-are> (last visited Feb. 28, 2024).

¹²⁷ Andrew Sorkin, *Credit Card Issuers Join the Fight to Limit Mass Shootings*, N.Y. TIMES (Sept. 12, 2022).

¹²⁸ See, e.g., Letter from Rep. Elise Stefanik et. al, to Mr. Alfred F. Kelly, Chief Exec. Officer of Visa, Inc. (Sept. 14, 2022); see also J.D. Tuccille, *Credit Cards ‘Pause’ Efforts to Track Gun Purchases After Pushback*, REASON (Mar. 13, 2023).

¹²⁹ See J.D. Tuccille, *supra* note 128.

¹³⁰ See, e.g., HJCSWFG_0000454.PPTX.

¹³¹ HJCSWFG_0000454.PPTX. at 2.


explains, “MCC Codes are used by credit card companies to classify merchant businesses into market segments and industries, with each merchant / vendor location having a unique merchant ID” and should not use any “minimum dollar threshold for individual transactions.”¹³² In other words, every transaction is assigned an MCC and financial institutions use these codes to search through customers’ financial history for any activity it deems “suspicious.” If it finds a possibly suspicious transaction, it can report that information to federal law enforcement by filing a SAR or similar report without the customer ever knowing about it.¹³³

Active Shooter Detection – Methodology 1 – Keyword EXCLUSION (Broad Focus)

- Transaction Population:** Query for credit / debit card purchases involving any of the following MCC codes:
 - 3484:** Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - 3489:** Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - 5091:** Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales)*
 - 5099:** Durable Goods, Not Elsewhere Classified
 - 5933:** Pawn Shops
 - 5941:** Sporting Goods Stores (largest sellers of firearms and ammunition)
 - 5999:** Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - 7999:** Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)
- * Not universally recognized MCC code
- Keyword EXCLUSION (Above transactions must EXCLUDE these keywords / Not exhaustive list):**

• Amazon	• Bowling	• Fitness	• Laundry	• Roll	• Tobacco
• Angler	• Cance	• Food	• LifeVantage	• Scrubs	• Tonka
• Archery	• Card	• Football	• Linn	• Shoe	• Vape
• Bait	• Carquest	• Gift Shop	• Lodge	• Skate	• Vapor
• Baseball	• Cig	• Golf	• Lowe's	• Ski	• Victrolasacret
• Bath & Body	• Coffee	• Google	• Mercari (exact)	• Smoke	• Vitamin
• Beauty	• Comic	• Graze	• Mizalace	• Snorkel	• Volleyball
• Bicycle	• Communication	• Harris Teller	• Music	• Stove	• Water
• Bike	• Danbury Mint	• Hockey	• Party	• Spirit Manufacturing	• Wish.com (exact)
• Billy Beaz	• DirecTV	• Home Depot	• PayPal (unless it also includes "Gun")	• Square (exact)	• Yoga
• Binge	• Dive	• Hoops	• Pizza	• Storage	• Zuri
• Boat	• Ebay	• Hospital	• Pencil	• Swim	• Zully (exact)
• Body	• Engineering	• Indeed	• Print	• Tackle	
• BodySolid	• Estrow.com	• iTunes	• Printer	• Tan	
• Boutique	• Farm	• Jewel	• Culver	• Tee	
• Bow	• Fish	• Johnson Hill	• Resort	• Tennis	
- During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**
 - Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, **AND**
 - Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, **AND**
 - Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, **AND**
 - Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.

Classification: KeyCorp Confidential



As the KeyBank slide demonstrates, financial institutions often use MCCs to query and review transactions for potentially suspicious activity. This slideshow directs particular concern to firearm-related purchases, lawful or otherwise, under the guise of detecting DVEs.¹³⁴ It reveals that financial institutions can use special MCCs to identify certain purchases for review, including “3484: Small Arms,” “3489: Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30mm),” “5091: Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales),” “5099: Durable Goods, Not Elsewhere Classified,” “5933: Pawn Shops,” “5941: Sporting Goods Stores (largest sellers of firearms and ammunition),” “5999: Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers),” and “7999: Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges).”¹³⁵

¹³² *Id.*

¹³³ See 31 U.S.C. § 5318(g)(3)(A); see also 12 U.S.C. § 3403(c); 31 C.F.R. § 1020.320(a)(1), (e).

¹³⁴ HJCSWFG_0000454.PPTX, at 3.

¹³⁵ *Id.*; See also KEYBANK, KEY2 PURCHASE MCC,

https://www.key.com/content/dam/kco/documents/businesses_institutions/Key2Purchase_MCC.pdf (last visited Jan. 22, 2024). The Committee and Select Subcommittee note that KeyBank omits use of MCCs 3484, 3489, and 5091 in its publicly available MCC list.

Active Shooter Detection – Methodology 2 – Keyword INCLUSION (Narrow Focus)

- **Transaction Population:** Query for credit / debit card purchases involving any of the following MCC codes:
 - 3484: Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - 3489: Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - 5091: Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns safes)*
 - 5099: Durable Goods, Not Elsewhere Classified
 - 5933: Pawn Shops
 - 5941: Sporting Goods Stores (largest sellers of firearms and ammunition)
 - 5999: Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - 7999: Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)
- * Not universally recognized MCC code
- **Keyword INCLUSION (Above transactions must INCLUDE one of these keywords / Not exhaustive list):**

▪ Academy.com	▪ Cabela's	▪ Edge Works Manufacturing	▪ HarrisBipods.com	▪ NorthShoreFirearms.com	▪ SOG International
▪ Aere Precision	▪ CalLegalMags.com	▪ Ekknife Supply	▪ ImpactGuns.com	▪ Noveske.com	▪ SouthernOhioGun.com
▪ AimSurplus	▪ CarrierComp.com	▪ EkknifeWorks.com	▪ JP Enterprises	▪ NTCTrading.net	▪ SpikesTactical.com
▪ AnarchyOutdoors.com	▪ ChattanoogaShooting.com	▪ EkknifeWorks.com	▪ JPRifles.com	▪ Numrich Gun Parts	▪ SportsmanGuide.com
▪ Anderson Manufacturing	▪ ChesperThunDist.com	▪ EliteDefense.com	▪ JSESurplus.com	▪ OpticsPlanet.com	▪ STGuns.com
▪ AR-15.co	▪ ClassicCollectonFirearms.com	▪ Gander Mountain	▪ KAKIndustry.com	▪ OregonRifleworks.com	▪ STI International
▪ AR15.com	▪ ClassicCollectonFirearms.com	▪ Gander Mountain	▪ Karambit.com	▪ ParkerMountainMachine.com	▪ Taccom
▪ B & T Industries	▪ CopesDistributing.com	▪ GhostGuns.com	▪ KingFirearmsAndMore.com	▪ RobertsonTradingPost.com	▪ Taccom3G.com
▪ Backcountry World	▪ DawsonPrecision.com	▪ GhostGunnet.com	▪ KingFirearmsOnline.com	▪ Ruger	▪ TaccomCanada.com
▪ Bass Pro Shop	▪ DeltaDefense.com	▪ Glock	▪ MidwayUSA.com	▪ S&W	▪ TargetSportsUSA.com
▪ Blade HQ	▪ DeltaTeamTactical.com	▪ Gowa.com	▪ M&MTargets.com	▪ Sarcocinc.com	▪ WC Wolf Co.
▪ BladeOps.com	▪ Dick's Sporting Goods	▪ GRKnives.com	▪ Mike Gibson Manufacturing	▪ ShootingTargets7.com	▪ WideOpenSpaces.com
▪ Bladefire	▪ DillonPrecision.com	▪ GrindGuns.com	▪ Mike's Gun Shop.net	▪ SIG Sauer	▪ WinthropHosters.com
▪ Bladefire.com	▪ DLTTrading.com	▪ GrindGuns.com	▪ Mike's Gun and Pawn	▪ SilencerShop.com	▪ WittMachinist.net
▪ BowysGunstocks.com	▪ DSG (Dick's Sporting Goods)	▪ GunBroker.com	▪ MileHighShooting.com	▪ Silent Precision	
▪ BravoCompanyUSA.com	▪ Dunskeibergers.com	▪ GunPartsCorp.com	▪ NewFrontierArmory.com	▪ SMKW.com	
▪ Brownells	▪ E-Sarcolinc.com	▪ GunSprings.com			
▪ Browning					
- **During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**
 - Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, **AND**
 - Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, **AND**
 - Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, **AND**
 - Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.

Classification: KeyCorp Confidential

These MCCs were also used to target transactions involving specific retailers and may have been flagged for federal law enforcement despite having no nexus to criminal activity.¹³⁶ As the KeyBank slide shows, transactions involving any of the previously named MCCs can be narrowed using additional keywords. Those keywords include transactions from retail stores like “Dick’s Sporting Goods,” “Gander Mountain,” “Bass Pro Shop,” “Cabela’s,” “Backcountry World,” “TargetSportsUSA.com,” “AR15.com,” “MidwayUSA,” among many others.¹³⁷

Another one of the KeyBank slides, circulated by FinCEN, directed financial institutions to other transactions of interest, listing such “red flags” that “[i]nvestigators may wish to consider” when “reviewing financial accounts” and included:

- “unexplained travel transactions, or unexplained transactions with a high-risk jurisdiction”;
- “any recent purchases of counter-surveillance equipment”;
- “any recent purchases of covert / secure communications equipment” such as “Virtual Private Networks (VPNs), online gaming, prepaid phones / calling cards”;
- “any recent rental of storage facilities”;
- “other excessive transactions” such as “hardware, beauty supply, auto parts, electronics, machinist / engineering, gym / martial arts, political donations / materials, religious donations / materials, work uniforms”;
- “excessive ATM, Prepaid Cards, Person-to-Person, or Virtual Currency transactions”;
- “recent life insurance purchases and/or bank account closures”;
- “any life stressor indicators” such as “no payroll deposits”;

¹³⁶ HJCSWFG_0000454.PPTX. at 4.

¹³⁷ *Id.*


- “recent excessive legal / medical expenses (legal / family status or health challenges)”;¹³⁸ and
- whether the individual is unemployed, was “recently fired or laid off,” has “delinquent / excessive debt,” or has “social media posts of concern.”¹³⁸

Of course, none of these transactions standing alone are unlawful—in fact, many are indicative of constitutionally protected political or religious activity.

Active Shooter Detection – Additional Red Flags to Consider

When Investigators are reviewing financial accounts, besides alerted transactions, other factors Investigators may wish to consider:

- Is the alerted transaction activity consistent with previous activity, or has it begun recently?
- Unexplained travel transactions, or unexplained transactions with a high-risk jurisdiction?
- Any recent purchases of counter-surveillance equipment?
- Any recent purchases of covert / secure communications equipment?
 - Virtual private networks (VPNs), online gaming, prepaid phones / calling cards, etc. transactions?
- Any recent rental of storage facilities?
- Other excessive transactions, especially if not consistent with previous activity?
 - Hardware, beauty supply, auto parts, electronics, machinist / engineering, gym / martial arts, political donations / materials, religious donations / materials, work uniforms, etc.
- Excessive ATM, Prepaid Cards, Person-to-Person (P2P), or Virtual Currency transactions?
- Any recent life insurance purchases and/or bank account closures?
- Any life stressor indicators?
 - Recent excessive legal / medical expenses (legal / family status or health challenges)?
 - No payroll deposits? Unemployed? Recently fired or laid off?
 - Delinquent / excessive debt?
- Any social media posts of concern?

Classification: KeyCorp Confidential 

Similarly, on January 16, 2021, FinCEN circulated additional slides prepared by the Global Financial Crimes Division (GFCD) at MUFG Bank, the largest bank of Japan, to other financial institutions and that included a “list of subjects of interest and high-level typologies.”¹³⁹ That slide revealed typologies for review as they relate to the events of “1/6” and included a broad scope of credit, debit, and ATM transactions, suggesting a look-back period ranging from November 3, 2020, to January 12, 2021.¹⁴⁰ These typologies include otherwise lawful activity such as “use of business cards (not held by tactical or security firms) for the purchase of arms / ammo,” “transfers to GiveSendGo or other crowdsourcing sites,” “purchasing of gift cards; Use of debit cards for Crypto,” and “transactions in or near capitols or state capitols at/around 1/6.”¹⁴¹

¹³⁸ HJCSWFG_0000454.PPTX. at 5.

¹³⁹ HJCSWFG_0000003 (email from FinCEN distributing slide to KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase); see also HJCSWFG_0000007.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*


A Strictly Confidential Customer Information

GFCD Intelligence & Analytics Data Insights and Analytics

Typologies for review as they relate to the events of 1/6/20

Scope: Transactions pulled from 11/3 – 1/12: ATM, CREDIT, DEBIT, with expanded reviews where needed.

#	Typology
1	MCC Codes that, when taken together, demonstrate travel: ex. hotel, rental car, & gas, AND Mileage increasingly further from cardholder's home
2	Cardholder purchases at gun-ammo, sporting goods stores, etc., that demonstrate increases in volume, value, or velocity above average and/or a high % relative to cardholder's available credit. Transactions that contain keyword list matches: a) potential target events, locations, or individuals b) names:
3	i: of those arrested at demonstrations / riots ii: of key leadership in organizations c) code terms and calls to action d) precursor elements to IEDs and firearms
4	Transactions in or near capitols or state capitols at/around 1/6
5	Multiple cards used by one person, for the purchasing of fire arms/ammo etc.
6	Use of business cards (not held by tactical or security firms) for the purchase of arms / ammo
9	Transfers to GiveSendGo or other crowdsourcing sites
10	Purchasing of gift cards; Use of debit cards for Crypto
11	Over/under invoicing for merchant codes at gun clubs with other vendor services (i.e., large transactions for an individual at a snack bar)



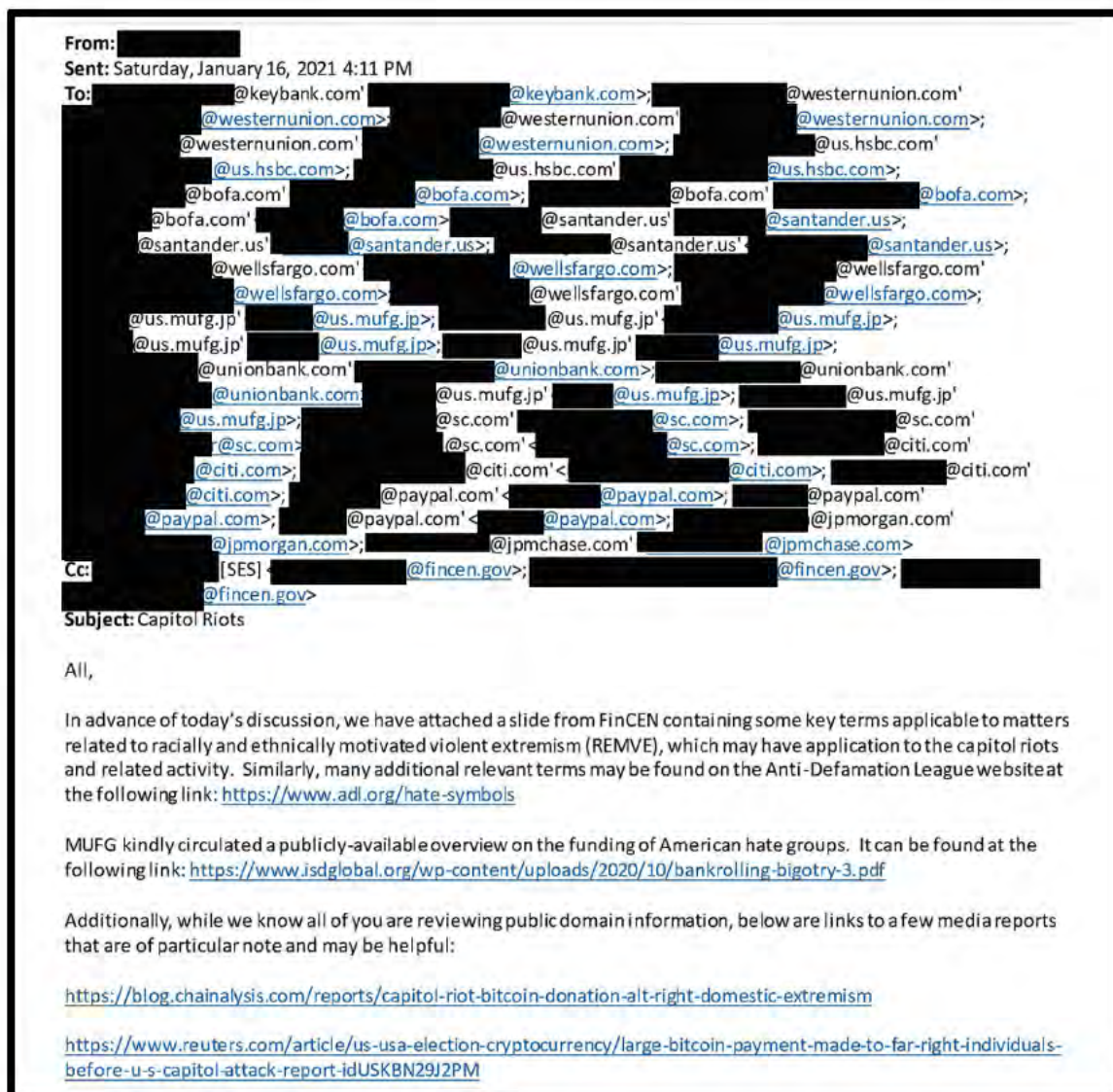
NOTE: DIA plans on looking at these typologies holistically, that is no single hit may warrant escalation but more than one could.
DIA plans on, where possible, pulling transaction details for Credit, ATM, and DEBIT card activity.
DIA will look to sort for these typologies via in person vs. online purchases
The condition and contents of data may dictate that DIA will have to alter these typologies, abandon these typologies, and / or adopt new typologies

Consequently, account information and transactions meeting any of the eleven “typology” criteria may have been flagged and shared with federal law enforcement as being “suspicious.” The slide is another clear example that these typologies were not necessarily evidence of criminal activity, but that were nonetheless scrutinized and potentially shared with federal law enforcement. Unfortunately, the use of MCC search parameters were not the only kinds of typologies and transactions that FinCEN was interested in. FinCEN also circulated politicized materials to financial institutions for monitoring their databases for certain “hate groups” and other “key terms.”¹⁴²

¹⁴² HJCSWFG_0000004 (email from FinCEN sharing hyperlinks to KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase).

b. FinCEN shared a “hate symbols” database and a report on the funding of American “hate groups” to financial institutions.

On January 16, 2021, FinCEN circulated another email to financial institutions “in advance of today’s discussion.”¹⁴³ That email included links to “key terms applicable to matters related to racially and ethnically motivated violent extremism, which may have application to the capitol riots and related activity.”¹⁴⁴ In addition, the email included a hyperlink to “relevant terms” from the Anti-Defamation League website and a hyperlink to a “publicly-available overview on the funding of American hate groups.”¹⁴⁵ The first hyperlink was to a database of “Hate Symbols” indexed by the Anti-Defamation League (ADL)—a notorious anti-conservative activist group—and the second was to a report authored by the Institute for Strategic Dialogue



¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

(ISD) titled “Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups.”¹⁴⁶

In recent years, ADL has become significantly more left-wing and taken an aggressively anti-conservative stance. For example, the “Hate Symbols” database maintained by ADL and circulated by FinCEN to financial institutions treats “Anti-Antifa Images,” the “Celtic Cross,” the “Okay Hand Gesture,” “Pepe the Frog,” and “White Lives Matter,” as hate symbols.¹⁴⁷ It should alarm Americans that FinCEN approved of and distributed a link to a database that considers symbols of faith such as the Christian Celtic Cross and other images opposing Antifa—a violent left-wing anarchist group—as hate symbols. This practice is reminiscent of the FBI’s disdain for “Radical Traditionalist Catholics,” and the FBI’s reliance on the Southern Poverty Law Center—another far-left activist group—as an authoritative source on the Catholic Church.¹⁴⁸



FinCEN also circulated a hyperlink to a report authored by the ISD. The ISD is a left-wing organization that holds itself out as an “independent” monitor of “disinformation” that promotes the censorship of speech it decries as false or extreme.¹⁴⁹ FinCEN’s distribution of the ISD report amounts to an approval of its content, its methods, and its conclusions. Such an endorsement is concerning because the ISD report labels and demonizes various right-of-center groups in America as “hate groups.”¹⁵⁰ For example, the ISD’s report incorrectly characterizes several conservative groups such as the Center for Immigration Studies, Numbers USA, the

¹⁴⁶ ADL, HATE ON DISPLAY™ HATE SYMBOLS DATABASE, <https://www.adl.org/resources/hate-symbols/search> (last visited Feb. 28, 2024); Institute for Strategic Dialogue, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, ISD at 9 (Oct. 27, 2020).

¹⁴⁷ ADL, HATE ON DISPLAY™ HATE SYMBOLS DATABASE, <https://www.adl.org/resources/hate-symbols/search> (last visited Feb. 28, 2024).

¹⁴⁸ See STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON THE FBI’S BREACH OF RELIGIOUS FREEDOM: THE WEAPONIZATION OF LAW ENFORCEMENT AGAINST CATHOLIC AMERICANS 5 (Comm. Print 2023).

¹⁴⁹ Institute for Strategic Dialogue, <https://www.isdglobal.org/about/> (last visited Feb. 28, 2024); see also Letter from Rep. Michael T. McCaul, Chairman, H. Foreign Aff. Comm., to Hon. Antony J. Blinken, Secretary of St. (May 1, 2023).

¹⁵⁰ Institute for Strategic Dialogue, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, ISD (Oct. 27, 2020).

Alliance Defending Freedom, along with several others, as “hate groups.”¹⁵¹ In fact, the ISD’s report draws a false equivalency between certain conservative civil society groups and the American Nazi Party and the Knights of the Ku Klux Klan, suggesting FinCEN views them equally.¹⁵² Still, FinCEN circulated the ISD report to some of the largest financial institutions in the world, including the very financial institutions that are likely responsible for providing financial services to many of the listed “hate groups,” without regard for the chilling effect it would have on protected speech and its potential to be weaponized against the groups by financial institutions.

¹⁵¹ *Id.* at 9.

¹⁵² *Id.*

Table 2 Overview of hate groups studied

<p>Anti-immigrant</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> Center for Immigration Studies Dustin Inman Society Federation for American Immigration Reform Numbers USA Oregonians for Immigration Reform ProEnglish The Remembrance Project We The People Rising <hr/> <p>Anti-LGBTQ+</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> Pass the Salt Ministries All Scripture Baptist Church Alliance Defending Freedom American College of Pediatricians American Family Association American Vision Center for Family and Human Rights Chalcedon Foundation Church Militant and St Michael's Media Eagle Forum Family Research Council Family Watch International Liberty Counsel MassResistance National Organization for Marriage New Independent Fundamental Baptist Network Pacific Justice Institute Ruth Institute Westboro Baptist Church World Congress of Families 	<p>Anti-Muslim</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> Act for America American Freedom Defense Initiative Center for Security Policy Clarion Project David Horowitz Freedom Center The United West <hr/> <p>Militia or street protest</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> American Patriots USA American Revolution 2.0 Patriot Prayer Patriot Wave Proud Boys Rise Above Movement Washington Three Percenters Oath Keepers <hr/> <p>White nationalist</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> America First Students American Freedom Party American Guard Groyppers – Nick Fuentes New Jersey European Heritage Association Patriot Front VDARE Identity Dixie League of the South 	<p>White supremacist</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> American Identity Movement (formerly Identity Evropa) American Nazi Party American Renaissance, website of New Century Foundation Atomwaffen Division Bowl Patrol or Bowl Gang Feuerkrieg Division (international) Keystone United Knights of the Ku Klux Klan Legion of St. Ambrose National Alliance National Socialist Movement National Justice Party Northwest Front NSC 131 Order 15 Shield Wall Network The Base Vorherrschaft Division Kingdom Identity Ministries <hr/> <p>Black supremacist</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> Nation of Islam <hr/> <p>Holocaust denial</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> Institute for Historical Review <hr/> <p>Misogynist</p> <hr/> <p>Organisations</p> <ul style="list-style-type: none"> A Voice for Men
--	--	--

C. FinCEN used financial institutions to monitor and report on accounts involved in crowdfunding for conservative events.

On January 18, 2021, FinCEN circulated a “list of crowdfunding sites” that “[p]eople have been observed using to post an event and sell tickets including bus tickets to the

casting the selling of “bus tickets to the demonstrations” as suspicious without articulating any basis for believing such demonstrations might be unlawful.¹⁵⁶ However, the weaponization of crowdfunding against conservative movements is not new.¹⁵⁷ For example, GoFundMe removed fundraisers associated with the “Freedom Convoy,” a group protesting COVID-19 mandates internationally, and removed fundraisers on its platform supporting the legal defense of Kyle Rittenhouse while leaving fundraisers for Antifa militants and Black Lives Matter rioters untouched on the platform.¹⁵⁸ FinCEN’s incursion into the crowdfunding space represents a trend in the wrong direction and a threat to American civil liberties.

D. FinCEN circulated a KeyBank-created “Appendix” of “Domestic Extremist Groups” to other financial institutions.

FinCEN also distributed an additional slide, prepared by another financial institution, via email to other financial institutions.¹⁵⁹ The slide is an “Appendix” that labels certain groups as “Domestic Extremist,” including “American Border Patrol,” “Anti-Abortion (violent),” “Anti-Government,” the “Center for Immigration Studies,” and the “Center for Security Policy,” among many others.¹⁶⁰ By sharing this slide prepared by KeyBank, FinCEN endorsed a listing of groups it considered “domestic extremist.”

CONCLUSION

The decline of cash and the rise of digital payments and e-commerce platforms has provided financial institutions with more insight and influence over the financial system than ever before. In fact, very little financial activity occurs beyond the purview of modern financial institutions. As a result, these financial institutions often act as arms of federal law enforcement as they work in coordination with federal law enforcement to identify what transactions and other information is “suspicious” enough to be reported. Other times, law enforcement uses backchannel discussions to commandeer financial institutions’ databases in order to collect Americans’ data and build a profile of any “typology” it deems “suspicious.” When working together, these two parties wield a tremendous amount of influence and power over the American financial system with almost no oversight of their partnership and no possibility for recourse when that system is abused at the cost of victims who have been wrongfully targeted by the secret information-sharing network.

As this investigation shows, greater scrutiny of the partnership between federal law enforcement and financial institutions is warranted. When “Big Banks” and “Big Government” collude to violate American civil liberties, Congress has a responsibility to step in. Thanks to the brave whistleblower testimony that brought it to light, what started as an investigation into alarming information-sharing between Bank of America and the FBI without legal process has

¹⁵⁶ *Id.*

¹⁵⁷ See, e.g., Ryan King, *Five times GoFundMe shut down conservative fundraisers*, WASH. EXAMINER (Feb. 7, 2022).

¹⁵⁸ See Douglas Blair, *GoFundMe’s Sordid History of Censorship of Conservative Causes*, DAILY SIGNAL (Feb. 9, 2022).

¹⁵⁹ HJCSWFG_0000549 (email from FinCEN sharing slide with KeyBank, Standard Chartered, Western Union, Wells Fargo, PayPal, Citibank, Bank of America, Santander, HSBC, MUFG, Union Bank, and JPMorgan Chase).

¹⁶⁰ HJCSWFG_0000550.PPTX.

exposed what appears to be an even greater state of financial surveillance and weaponization. From targeting customers and transactions that shop at Bass Pro Shop or Cabela's using MCCs, to profiling customers with "typologies" that cast the purchase of religious texts and other donations to organizations that promote "radicalism" as indicative of "Homegrown Violent Extremism," federal law enforcement has overstepped its bounds.

As this investigation continues, the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government will continue to conduct oversight of the state of financial surveillance, targeting, and the vulnerabilities of Americans' data. Secret information-sharing portals and backchannel discussions outside the normal course of legal process pose serious risks to the nation. Larger questions remain regarding how the information shared between federal law enforcement and financial institutions was acted upon, and the ongoing extent of the financial surveillance. The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government remain committed to answering those questions and upholding the civil liberties of Americans.

Appendix

Date: Friday, January 29 2021 08:31 PM

Subject: [EXTERNAL] Capitol Riots Investigations

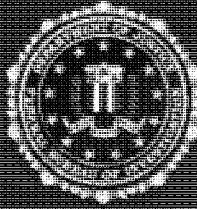
From: [REDACTED]@fbi.gov >
[REDACTED]@jpmchase.com > [REDACTED]@citi.com >; [REDACTED]
[REDACTED]@paypal.com > [REDACTED]@wellsfargo.com >
To: [REDACTED]@us.hsbc.com >; [REDACTED]@sc.com >; [REDACTED]
[REDACTED]@bofa.com >; [REDACTED]@usbank.com >; [REDACTED]
[REDACTED]@barclays.com >; [REDACTED]@jpmchase.com >
[REDACTED]@schwab.com >;
CC: [REDACTED]@fbi.gov >;

Good afternoon all,

For the past several months I have been working at our Washington Field Office under [REDACTED] who I believe most of you met while [REDACTED] was serving as the [REDACTED]. As the dust begins to settle here after the events of January 6th, [REDACTED] would like to hold a call with the goal of identifying the best approach to information sharing, both strategic and operational, related to the Capitol Riots. In the hopes of moving forward together quickly, we have set aside time at 2:30pm on Tuesday, February 2nd for this discussion. I will be sending out dial-in information first thing Monday and hope you, or someone from your team, is available to participate.

Thanks and have a great weekend!

[REDACTED]
[REDACTED]
Special Assistant to [REDACTED]
Federal Bureau of Investigation
Washington Field Office
[REDACTED]



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CROSS-SECTOR

17 January 2020

LIR 210117002

Domestic Violent Extremists Likely Emboldened in Aftermath of Capitol Breach

References in this LIR to any specific commercial product, process or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service or corporation on behalf of the FBI.

The Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and National Counterterrorism Center (NCTC) prepared this LIR to alert private sector partners that the 6 January 2021 violent breach by suspected domestic violent extremists (DVEs) into the U.S. Capitol Building may serve as a driver for a diverse set of DVEs.

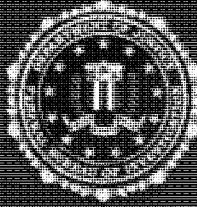
DVEs may exploit future lawful protests, rallies, demonstrations, and other gatherings to carry out ideologically motivated violence and criminal activity. The death of an individual directly engaged in the U.S. Capitol breach may serve to galvanize DVEs and increase collaboration between such diverse DVE groups.¹ These DVEs may also perceive the event as a step toward achieving their initiatives and consider the death of a perceived like-minded individual as an act of martyrdom.²

The belief in the existence of global or “deep state” actors who work to manipulate various social, political, and/or economic conditions of the United States likely serves as a driver of some DVE violence. Some rioters and DVEs’ view the 6 January event as a success and may exploit follow-on lawful gatherings; this perceived success may inspire some DVEs to target racial, ethnic, or religious minorities and institutions, the media, law enforcement, and government officials and buildings.

- An individual who traveled to Washington, D.C. engaged in lawful protests, illegally entered the U.S. Capitol Building, and was shot and killed by law enforcement personnel.
- Some participants at the Capitol displayed insignias used or adopted by a range of DVEs. Nooses and plastic restraints were carried or stationed at or near the Capitol by some rioters, possibly to demonstrate their intent to cause harm to government officials.
- During rioting on the Capitol grounds, individuals pursued and threatened journalists, according to open-source reporting. Rioters destroyed or stole cameras and other media equipment outside the Capitol, and the phrase, “Murder the media,” was found scratched into a door within the Capitol.

¹ The information in this LIR is provided to inform law enforcement of the referenced narratives and theories, which may play in mobilizing criminal actors and DVEs to violence. Generating, accessing, discussing, or otherwise interacting with content related to these theories, without engaging in violence or other criminal activity, is protected by the First Amendment. The FBI does not investigate, collect, or maintain information on U.S. persons solely for the purpose of monitoring First Amendment-protected activities.

² The perception that deaths of like-minded individuals at the hands of law enforcement were unjust has historically been a significant driver for DVEs. DVEs have seized on the deaths of two U.S. persons Vicki and Samuel Weaver at Ruby Ridge, Idaho in 1992; U.S. persons at the Branch Davidians compound at Waco, Texas in 1993; and U.S. person Duncan Lemp in 2020 to justify threats against law enforcement and government officials.



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

DVEs May Target Elected Officials and Government Buildings Following Political Shifts

Perceptions of fraud surrounding the outcome of the General Election and the change in control of the Presidency and Senate—when combined with long-standing DVE drivers such as perceived government or law enforcement overreach, and the anticipation of legislation perceived to oppose or threaten their beliefs— may lead to an increase in the DVE threat.

Narratives surrounding the perceived success of the breach of the U.S. Capitol will likely lead to an increased DVE threat towards federal, state, and local governments across the United States, particularly in the time period surrounding the 20 January Presidential Inauguration. The targeting of government buildings and officials is consistent with observed activity in 2020, when armed individuals, including DVEs, threatened elected officials and occupied state government buildings. Since the 6 January event, online rhetoric regarding the 20 January Presidential Inauguration has increased, with some calling for unspecified “justice” for the 6 January fatal shooting by law enforcement of an individual at the Capitol Building, and another posting that “many” armed individuals would return on 19 January, according to open-source reporting. The recent removal efforts by social media platforms used by DVEs may push some to revert to other platforms they perceive as more secure.

Range of DVE Actors Likely to Pose Increasing Threat at Lawful Protests, Rallies, Demonstrations, etc.

Throughout 2020, DVEs with differing goals and perspectives exploited such events to promote, organize, conspire, and plot against ideological opponents and other targets. DVEs’ efforts to engage in violence at lawful gatherings will probably increase throughout 2021, as some DVEs perceive increased socio-political pressures. Such perceived pressures may stem from, but not be limited to, one or more of the following factors:

- The potential for shifts in various policies many DVEs may perceive to oppose or threaten their ideological goals and agendas or feed into existing narratives many DVEs subscribe to regarding the U.S. government’s exercise of power, influence, and initiatives: possibly including firearm legislation, the easing of immigration restrictions, and new limits on the use of public land.
- Ongoing narratives by DVEs that the 2020 General Election was illegitimate, or fraudulent, and the subsequent belief its results should be contested or unrecognized.
- Some DVEs’ discontent with renewed measures to mitigate the spread of COVID-19, the ordered dissemination of COVID-19 vaccinations, and the efficacy and/or safety of COVID-19 vaccinations.

The FBI, DHS, and NCTC remain concerned about the potential for a loosely organized, sustained, and significant DVE population mobilizing to violence based on social media calls to target government infrastructure or officials. The shared narrative of election fraud and the opposition to the change in control of the executive and legislative branches of the federal government may lead some individuals to adopt the belief that there is no political solution to address their grievances and violent action is necessary. Additionally, in-person engagement between DVEs of differing ideological goals during the Capitol breach likely served to foster connections, which may increase DVEs’ willingness, capability, and motivation to attack and undermine a government they view as illegitimate.³

³ Targeted attacks on identified elected and party officials based upon their political opinions would be similar to attacks observed in the last five years including the 2017 attempted assassination of Republican members of Congress on a baseball field in Virginia, or two assassinations by violent extremists espousing a belief in white supremacy targeting a British member of Parliament, and a German political party official.



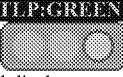



In the near term, DVEs could exploit upcoming events to engage in or justify violence, including events attended by MVEs and “boogaloo”⁴ adherents scheduled nationally from 16 to 20 January; the 20 January Presidential Inauguration and associated events in Washington, D.C.; and the impeachment and possible departure of the 45th President prior to the end of his term. The “boogaloo” is a concept most commonly used to reference an impending second civil war or insurgency against the U.S. Government. Calls for revolution may especially resonate with militia violent extremists (MVEs), who often justify violence based on their belief that they are guardians of the Constitution and the legacies of the American Revolution. While they may not necessarily share the partisan views of those who engaged in the 6 January breach, MVEs and other DVEs who adhere to the “boogaloo” concept and seek a politically motivated civil war, and racially motivated violent extremists who seek a race war, may exploit the aftermath of the Capitol breach in an attempt to create conflict in the United States.

If companies witness any suspicious activities related to potential domestic violent extremism, please report it to your FBI Private Sector Coordinator at your local FBI Field Office:
<https://www.fbi.gov/contact-us/field-offices>.

OPS’s Information Sharing and Analysis Unit disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:
<https://www.fbi.gov/contact-us/field-offices>.

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.
 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
 Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

⁴ According to open-source research, the original boogaloo meme references the 1984 film, *Breakin' 2: Electric Boogaloo*. Mainstream culture adopted the phrase “electric boogaloo” to comment on follow-on or repeat events in pop- and political-culture, such as re-elections. MVEs use the boogaloo derivative of the phrase to refer to a second Civil War, i.e. American Civil War 2: Electric Boogaloo. Proponents cultivated the meme by sharing images, videos, and rhetoric. “Big igloo,” “Big luau,” “Boog Bois,” “Boojahideen,” and other associated word-play in addition to imagery such as igloos, Hawaiian shirts, and leis, are used as coded references to the larger boogaloo phenomenon on-and offline.

From: [REDACTED] (FBI) [REDACTED]@fbi.gov]
Sent: 1/15/2021 9:56:49 AM
To: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
Subject: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

Ahead of next week's inauguration, I wanted to touch base on a couple things.

If either or both of you have time this morning to discuss SARs and a couple ideas, that would be great.

I will be on my cell this morning.

[REDACTED]

From: [REDACTED]@fbi.gov]
Sent: 1/15/2021 12:40:26 PM
To: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
Subject: Re: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

As always, thanks for the very quick communication/response over the phone this morning.

To recap our morning call, we [FBI] are prepared to action **[immediately]** the following thresholds:

- CTD/SPES/SEU is interested in all financial relationships that meet the following thresholds:
 - Customers confirmed as transacting, either through bank account [debit card] or credit card, Washington D.C. purchases between 1/5/21 and 1/6/21, with the additional [identifying] targeting thresholds:
 - Purchases made for hotel/airbnb RSVPs in the DMV area [the day before and during Inauguration Day] -----since 1/6/21.
 - ANY historical purchase [going back 6 months generally, for weapons or weapons related-vendor purchases].
 - Secondly, purchases made for returns to Washington, D.C. and the surrounding DMV area:
 - With Airline travel to DMV area for Inauguration Day
 - With no identified airline purchases for the DMV.**
- ** - SEU intends to capture, with its FI-partner concurrence, all customers who might be more strategic in carrying out attacks related to CTD interests; travel with weapons by vehicle and [not by] air, given the current threat and aftermath of the 6 Jan Capitol building incidents. The intention by SEU is to identify all potential networks of threats vs. individual threats to Inauguration Day and beyond.

[REDACTED]

From: [REDACTED] (FBI)
Sent: Friday, January 15, 2021 9:56 AM
To: [REDACTED]@bofa.com>; [REDACTED]@bofa.com>
Subject: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

Ahead of next week's inauguration, I wanted to touch base on a couple things.

From: [REDACTED]@bofa.com]
Sent: 1/17/2021 7:54:23 PM
To: [REDACTED]@fbi.gov'; [REDACTED]@fbi.gov]
CC: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
Subject: RE: [SecMail:] secmail:RE: Follow-up

[REDACTED] – you should have an email from [REDACTED]@bofa.com with our filing on the parameters you discussed with [REDACTED] last week.

Thanks,
[REDACTED]

[REDACTED]

From: [REDACTED]@fbi.gov [mailto:[REDACTED]@fbi.gov]
Sent: Saturday, January 16, 2021 11:26 AM
To: [REDACTED]@bofa.com>
Cc: [REDACTED]@bofa.com>; [REDACTED]@bofa.com>; [REDACTED]@fbi.gov
Subject: RE: secmail:RE: Follow-up

[REDACTED]

Great. Thanks. I will run with the info.

[REDACTED]

From: [REDACTED]
Sent: Sat, 16 Jan 2021 15:16:38 +0000
To: [REDACTED] (FBI)
Cc: [REDACTED]
Subject: Follow-up

Hi [REDACTED]

Following up from our conversation yesterday morning, we are doing some work around the parameters we discussed and should have something out before the end of the weekend.

To: [redacted]@keybank.com [redacted]@sc.com [redacted]
[redacted]@sc.com [redacted]@westernunion.com]; [redacted] Final Report 2050
[redacted]@westernunion.com [redacted]@wellsfargo.com [redacted]@wellsfargo.com
[redacted]@wellsfargo.com [redacted]@paypal.com];
[redacted]@paypal.com [redacted]@paypal.com [redacted]@citi.com];
[redacted]@citi.com [redacted]@bofa.com [redacted]@bofa.com];
[redacted]@santander.us [redacted]@santander.us [redacted]@us.hsbc.com
[redacted]@jpmorgan.com [redacted]@us.mufg.jp [redacted]@us.mufg.jp];
[redacted]@wellsfargo.com [redacted]@wellsfargo.com [redacted]@santander.us
[redacted]@us.mufg.jp]; [redacted]@citi.com [redacted]@us.hsbc.com];
[redacted]@bofa.com]; [redacted]@bofa.com]

Cc: [redacted]@fincen.gov]; [redacted]@fincen.gov]; [redacted]
[redacted]@fincen.gov]

From: [redacted]@fincen.gov]
Sent: Fri 1/15/2021 4:00:25 PM (UTC-05:00)
Subject: Compiled typologies in advance of 4:30 call
[Jan 15 2021 compiled typologies.docx](#)
[KeyBank Query Logic for Active Shooters v 01-15-2021.pptx](#)

All, in advance of the 4:30 call, please find attached indicators shared by two institutions, as well as indicators developed from prior FinCEN analysis on lone actors/homegrown violent extremists.

Talk to you shortly,
[redacted]

1) Bank submission:

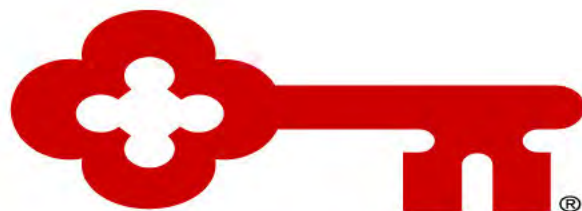
One of the things we've done is search Zelle payment messages for indications of involvement in the riots or potential violence. Here are the key words we used below to pull the data. [...] from our initial analysis "Storm the", "Capitol", "white power" and "Antifa" seem to be yielding the best results.

%PRESIDENT%
 %PREZ%
 %TRUMP%
 %KAMALA%
 %BIDEN%
 %DIE%
 %KILL%
 %SHOOT%
 %BLOW%
 %GUN%
 %DEATH%
 %MURDER%
 KRAKEN
 ANTIFA
 LAST SONS
 OATH KEEPER
 WHITE POWER
 CAPITOL
 STORM THE
 CIVIL WAR
 GROYPER ARMY
 CAMP AUSCHWITZ
 AMERICA FIRST
 THREEPERS
 MILITIA
 CAPITAL
 MAGA
 PATRIOT
 BOOGALOO
 PROUD B%
 CIVIL WAR
 PELOSI
 PENCE
 Schumer

2) Lone Actor/Homegrown Violent Extremism Indicators (developed from prior FinCEN analysis)

- ✓ Long periods of account inactivity, or show normal usage, but in the months or years preceding an attack, a sudden surge or change in activity type.
- ✓ Sudden purchase of firearms, firearm parts and accessories, ammunition, tactical gear at outdoor supply stores, and purchases at shooting ranges not commensurate with previously known customer behavior.

- ✓ Frequent cash deposits of unknown origin, followed by debit or credit card purchases at retailers not commensurate with previously known customer purchase activity.
- ✓ Frequent ATM withdrawals and wire transfers with no apparent economic or business purpose.
- ✓ Sudden account closings, asset liquidations, and disbursements in days or weeks leading up to attacks.
- ✓ Life insurance policy purchases not commensurate with typical behavior for the type of account holder.
- ✓ Transportation charges, such as bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose or not commensurate with the previous travel history of the customer, for example, travel to high-risk areas or indirect flightpaths for no apparent legitimate reason.
- ✓ Purchases that appear excessive or unusual for hobbyist or other legitimate use.
- ✓ The purchase of pre-cursor chemicals, fireworks, or potential bomb-making equipment, for example, ammonium nitrate, citric acid, aluminum powder, triacetone triperoxide [TATP], potassium nitrate, red iron oxide, tannerite, lengths of piping, BB pellets, cell phones, and others.
- ✓ Purchases of international calling cards not commensurate with previously known customer behavior.
- ✓ The purchase of books (including religious texts) and subscriptions to other media containing extremist views.
- ✓ Donations to organizations known to promote radicalism.



KeyBank's Query Logic for Active Shooters

[REDACTED]
SVP – Compliance Director - Financial Intelligence

[REDACTED]@keybank.com

Active Shooter Detection – Intent of Query

- Intends to detect potential active shooters, who may include dangerous International Terrorists / Domestic Terrorists / Homegrown Violent Extremists (“Lone Wolves”).
- Assumes individuals are creatures of habit and tend to frequent and/or shop at the same places when buying the same or similar items, rather than purchasing the same thing at multiple merchants or vendors.
 - Looks for purchases at multiple merchants or vendors who sell weapons and/or ammunition over a shorter period of time.
- Looks for “bursts” of potential suspicious purchase activity, especially when activity not seen previously.
 - Run query periodically, using a rolling lookback period of 60 days.
- Focuses on credit / debit card transaction activity with merchant / vendor counterparties.
 - Looks at specific counterparty Merchant Category Classification Codes (MCC Codes) and distinct merchant IDs.
 - MCC Codes are used by credit card companies to classify merchant businesses into market segments and industries, with each merchant / vendor location having a unique merchant ID.
 - No minimum dollar threshold for individual transactions.
 - Uses an iterative feedback loop process to build out and refine the exclusion and inclusion keyword lists (detailed in the next slides).
 - Limitations – Due to a lack of industry identifiers for counterparties for other transaction types, does not look at cash, check, ACH, or wire transactions at this time.
- SARs filed for public safety / law enforcement awareness purposes.
- **Alert Example – John Doe makes 5 credit card purchases at 4 different gun shops, plus makes 4 charges at 3 gun ranges, spending \$3,000 on weapons-related transactions over a 5 week period. Doe does not appear to have any previous firearms purchases.**



Active Shooter Detection – Methodology 1 – Keyword EXCLUSION (Broad Focus)

- **Transaction Population: Query for credit / debit card purchases involving any of the following MCC codes:**
 - **3484:** Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - **3489:** Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - **5091:** Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales)*
 - * Not universally recognized MCC code
 - **5099:** Durable Goods, Not Elsewhere Classified
 - **5933:** Pawn Shops
 - **5941:** Sporting Goods Stores (largest sellers of firearms and ammunition)
 - **5999:** Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - **7999:** Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)

- **Keyword EXCLUSION (Above transactions must EXCLUDE these keywords / Not exhaustive list):**

▪ Amazon	▪ Bowling	▪ Fitness	▪ Laundry	▪ Rod	▪ Tobacco
▪ Angler	▪ Canoe	▪ Food	▪ LifeVantage	▪ Scuba	▪ Tools
▪ Archery	▪ Card	▪ Football	▪ Linen	▪ Shoe	▪ Vape
▪ Bait	▪ Carquest	▪ Gift Shop	▪ Lodge	▪ Skate	▪ Vapor
▪ Baseball	▪ Cig	▪ Golf	▪ Lowe's	▪ Ski	▪ Victoriasecret
▪ Bath & Body	▪ Coffee	▪ Google	▪ Mercari (exact)	▪ Smoke	▪ Vitamin
▪ Beauty	▪ Comic	▪ Graze	▪ Mktplace	▪ Snorkel	▪ Volleyball
▪ Bicycle	▪ Communication	▪ Harris Teller	▪ Music	▪ Soccer	▪ Water
▪ Bike	▪ Danbury Mint	▪ Hockey	▪ Party	▪ Spirit Manufacturing	▪ Wish.com (exact)
▪ Billy Beez	▪ DirecTV	▪ Home Depot	▪ PayPal (unless it also includes "Gun")	▪ Square (exact)	▪ Yoga
▪ Bingo	▪ Dive	▪ Hoops	▪ Pizza	▪ Storage	▪ Zoo
▪ Boat	▪ Ebay	▪ Hospital	▪ Pool	▪ Swim	▪ Zulily (exact)
▪ Body	▪ Engineering	▪ Indeed	▪ Print	▪ Tackle	
▪ Body-Solid	▪ Escrow.com	▪ iTunes	▪ Quiver	▪ Tan	
▪ Boutique	▪ Farm	▪ Jewel	▪ Resort	▪ Tea	
▪ Bow	▪ Fish	▪ Johnson Hlth		▪ Tennis	

- **During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**
 - Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, **AND**
 - Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, **AND**
 - Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, **AND**
 - Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.



Active Shooter Detection – Methodology 2 – Keyword INCLUSION (Narrow Focus)

- **Transaction Population: Query for credit / debit card purchases involving any of the following MCC codes:**
 - **3484:** Small Arms (includes businesses generally manufacturing small arms and accessories having a bore less than 30 mm)*
 - **3489:** Ordnance and Accessories, Not Elsewhere Classified (includes businesses manufacturing firearms and accessories having a bore more than 30 mm)*
 - **5091:** Sporting and Recreational Goods and Supplies (includes retail ammunition and retail guns sales)*
 - * Not universally recognized MCC code
 - **5099:** Durable Goods, Not Elsewhere Classified
 - **5933:** Pawn Shops
 - **5941:** Sporting Goods Stores (largest sellers of firearms and ammunition)
 - **5999:** Miscellaneous and Specialty Retail Shops (includes firearms and ammunition dealers)
 - **7999:** Recreation Services, Not Elsewhere Classified (includes shooting facilities or shooting ranges)

- **Keyword INCLUSION (Above transactions must INCLUDE one of these keywords / Not exhaustive list):**

<ul style="list-style-type: none"> ▪ Academy.com ▪ Aero Precision ▪ AimSurplus ▪ AnarchyOutdoors.com ▪ Anderson Manufacturing ▪ AR-15.co ▪ AR15.com ▪ B & T Industries ▪ backcountry world ▪ Bass Pro Shop ▪ Blade HQ ▪ BladeOps.com ▪ BladePlay ▪ Botach.com ▪ BoydsGunstocks.com ▪ BravoCompanyUSA.com ▪ Brownells ▪ Browning 	<ul style="list-style-type: none"> ▪ Cabela's ▪ CaLegalMags.com ▪ CarrierComp.com ▪ ChattanoogaShooting.com ▪ CheaperThanDirt.com ▪ ClassicCollectionFirearms.com ▪ CopesDistributing.com ▪ DawsonPrecision.com ▪ DeltaDefense.com ▪ DeltaTeamTactical.com ▪ Dick's Sporting Goods ▪ DillonPrecision.com ▪ DLTTrading.com ▪ DSG (Dick's Sporting Goods) ▪ Dunkelbergers.com ▪ E-Sarcolnc.com 	<ul style="list-style-type: none"> ▪ Edge-Works Manufacturing ▪ EKnife Supply ▪ EKnifeWorks.com ▪ EliteDefense.com ▪ FreedomMunitions.com ▪ Gander Mountain ▪ Geissele.com ▪ GhostGuns.com ▪ GhostRunner.com ▪ Glock ▪ Govx.com ▪ GPKnives.com ▪ GrabAGun.com ▪ Grindworx.com ▪ GunBroker.com ▪ GunPartsCorp.com ▪ GunSprings.com 	<ul style="list-style-type: none"> ▪ HarrisBipods.com ▪ ImpactGuns.com ▪ JP Enterprises ▪ JPRifles.com ▪ JSESurplus.com ▪ KAKIindustry.com ▪ Karambit.com ▪ KingsFirearmsAndMore.com ▪ KingsFirearmsOnline.com ▪ MidwayUSA.com ▪ MGMTargets.com ▪ Mike Gibson Manufacturing ▪ MikesGunShop.net ▪ Mike's Gun and Pawn ▪ MileHighShooting.com ▪ NewFrontierArmory.com 	<ul style="list-style-type: none"> ▪ NorthShoreFirearms.com ▪ Noveske.com ▪ NTCTrading.net ▪ Numrich Gun Parts ▪ OpticsPlanet.com ▪ OregonRifleworks.com ▪ ParkerMountainMachine.com ▪ RobertsonTradingPost.com ▪ Ruger ▪ Sarcolnc.com ▪ ShootingTargets7.com ▪ SIG Sauer ▪ SilencerShop.com ▪ Silent Precision ▪ SMKW.com ▪ SniperCentral.com 	<ul style="list-style-type: none"> ▪ SOG International ▪ SouthernOhioGun.com ▪ SpikesTactical.com ▪ SportsmansGuide.com ▪ STIGuns.com ▪ STI International ▪ Taccom ▪ Taccom3G.com ▪ TaccomCanada.com ▪ TargetSportUSA.com ▪ WC Wolff Co. ▪ WideOpenSpaces.com ▪ WinthropHolsters.com ▪ WittMachine.net
---	--	--	---	--	--

- **During the 60-Day Rolling Lookback Period, Query Run Periodically (SME Adjustable Parameters):**
 - Involves 5 or more distinct and different merchants / vendors of the above population set by the customer, AND
 - Aggregate purchase transactions totaling \$2,500 or more from the above MCC codes by the customer, AND
 - Number of transactions at the above MCC codes > 50% of total number of transactions by the customer, AND
 - Aggregate purchase amount at the above MCC codes > 50% of total purchases by the customer.



Active Shooter Detection – Additional Red Flags to Consider

When Investigators are reviewing financial accounts, besides alerted transactions, other factors Investigators may wish to consider:

- Is the alerted transaction activity consistent with previous activity, or has it begun recently?
- Unexplained travel transactions, or unexplained transactions with a high-risk jurisdiction?
- Any recent purchases of counter-surveillance equipment?
- Any recent purchases of covert / secure communications equipment?
 - Virtual private networks (VPNs), online gaming, prepaid phones / calling cards, etc. transactions?
- Any recent rental of storage facilities?
- Other excessive transactions, especially if not consistent with previous activity?
 - Hardware, beauty supply, auto parts, electronics, machinist / engineering, gym / martial arts, political donations / materials, religious donations / materials, work uniforms, etc.
- Excessive ATM, Prepaid Cards, Person-to-Person (P2P), or Virtual Currency transactions?
- Any recent life insurance purchases and/or bank account closures?
- Any life stressor indicators?
 - Recent excessive legal / medical expenses (legal / family status or health challenges)?
 - No payroll deposits? Unemployed? Recently fired or laid off?
 - Delinquent / excessive debt?
- Any social media posts of concern?



GFGD Intelligence & Analytics Data Insights and Analytics

A Strictly Confidential
Customer Information

Typologies for review as they relate to the events of 1/6/20

Scope: Transactions pulled from 11/3 – 1/12: ATM, CREDIT, DEBIT, with expanded reviews where needed.

#	Typology
1	MCC Codes that, when taken together, demonstrate travel: ex. hotel, rental car, & gas, AND Mileage increasingly further from cardholder's home
2	Cardholder purchases at gun-ammo, sporting goods stores, etc., that demonstrate increases in volume, value, or velocity above average and/or a high % relative to cardholder's available credit.
3	Transactions that contain keyword list matches: a) potential target events, locations, or individuals b) names: i: of those arrested at demonstrations / riots ii: of key leadership in organizations c) code terms and calls to action d) precursor elements to IEDs and firearms
4	Transactions in or near capitols or state capitols at/around 1/6
5	Multiple cards used by one person, for the purchasing of fire arms/ammo etc.
6	Use of business cards (not held by tactical or security firms) for the purchase of arms / ammo
9	Transfers to GiveSendGo or other crowdsourcing sites
10	Purchasing of gift cards; Use of debit cards for Crypto
11	Over/under invoicing for merchant codes at gun clubs with other vendor services (i.e., large transactions for an individual at a snack bar)

1



NOTE: DIA plans on looking at these typologies holistically, that is no single hit may warrant escalation but more than one could.

DIA plans on, where possible, pulling transaction details for Credit, ATM, and DEBIT card activity.

DIA will look to sort for these typologies via in person vs. online purchases

The condition and contents of data may dictate that DIA will have to alter these typologies, abandon these typologies, and / or adopt new typologies

[REDACTED]@jpmorgan.com>; [REDACTED]@jpmchase.com' <[REDACTED]@jpmchase.com>
Cc: [REDACTED] [SES] <[REDACTED]@fincen.gov>; [REDACTED] <[REDACTED]@fincen.gov>; [REDACTED]
<[REDACTED]@fincen.gov>
Subject: RE: Capitol Riots

All, Key Bank circulated this very helpful list of key terms.

Regards,
[REDACTED]

From: [REDACTED]
Sent: Saturday, January 16, 2021 4:11 PM
To: [REDACTED]@keybank.com' <[REDACTED]@keybank.com>; [REDACTED]@westernunion.com'
[REDACTED]@westernunion.com' <[REDACTED]@westernunion.com>; [REDACTED]@westernunion.com>;
[REDACTED]@westernunion.com' <[REDACTED]@westernunion.com>; [REDACTED]@us.hsbc.com'
<[REDACTED]@us.hsbc.com>; [REDACTED]@us.hsbc.com' <[REDACTED]@us.hsbc.com>;
[REDACTED]@bofa.com' <[REDACTED]@bofa.com>; [REDACTED]@bofa.com' <[REDACTED]@bofa.com>;
[REDACTED]@bofa.com' <[REDACTED]@bofa.com>; [REDACTED]@santander.us' <[REDACTED]@santander.us>;
[REDACTED]@santander.us' <[REDACTED]@santander.us>; [REDACTED]@santander.us' <[REDACTED]@santander.us>;
[REDACTED]@wellsfargo.com' <[REDACTED]@wellsfargo.com>; [REDACTED]@wellsfargo.com'
<[REDACTED]@wellsfargo.com>; [REDACTED]@wellsfargo.com' <[REDACTED]@wellsfargo.com>;
[REDACTED]@us.mufg.jp' <[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp' <[REDACTED]@us.mufg.jp>;
[REDACTED]@us.mufg.jp' <[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp' <[REDACTED]@us.mufg.jp>;
[REDACTED]@unionbank.com' <[REDACTED]@unionbank.com>; [REDACTED]@unionbank.com'
<[REDACTED]@unionbank.com>; [REDACTED]@us.mufg.jp' <[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
<[REDACTED]@us.mufg.jp>; [REDACTED]@sc.com' <[REDACTED]@sc.com>; [REDACTED]@sc.com'
<[REDACTED]@sc.com>; [REDACTED]@sc.com' <[REDACTED]@sc.com>; [REDACTED]@citi.com'
<[REDACTED]@citi.com>; [REDACTED]@citi.com' <[REDACTED]@citi.com>; [REDACTED]@citi.com'
<[REDACTED]@citi.com>; [REDACTED]@paypal.com' <[REDACTED]@paypal.com>; [REDACTED]@paypal.com'
<[REDACTED]@paypal.com>; [REDACTED]@paypal.com' <[REDACTED]@paypal.com>; [REDACTED]@jpmorgan.com'
<[REDACTED]@jpmorgan.com>; [REDACTED]@jpmchase.com' <[REDACTED]@jpmchase.com>
Cc: [REDACTED] [SES] <[REDACTED]@fincen.gov>; [REDACTED] <[REDACTED]@fincen.gov>; [REDACTED]
<[REDACTED]@fincen.gov>
Subject: Capitol Riots

All,

In advance of today's discussion, we have attached a slide from FinCEN containing some key terms applicable to matters related to racially and ethnically motivated violent extremism (REMVE), which may have application to the capitol riots and related activity. Similarly, many additional relevant terms may be found on the Anti-Defamation League website at the following link: <https://www.adl.org/hate-symbols>

MUFG kindly circulated a publicly-available overview on the funding of American hate groups. It can be found at the following link: <https://www.isdglobal.org/wp-content/uploads/2020/10/bankrolling-bigotry-3.pdf>

Additionally, while we know all of you are reviewing public domain information, below are links to a few media reports that are of particular note and may be helpful:

<https://blog.chainalysis.com/reports/capitol-riot-bitcoin-donation-alt-right-domestic-extremism>

<https://www.reuters.com/article/us-usa-election-cryptocurrency/large-bitcoin-payment-made-to-far-right-individuals-before-u-s-capitol-attack-report-idUSKBN29J2PM>



**FINANCIAL SURVEILLANCE IN THE UNITED STATES:
HOW THE FEDERAL GOVERNMENT WEAPONIZED THE BANK SECRECY ACT
TO SPY ON AMERICANS**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



December 6, 2024

EXECUTIVE SUMMARY

Financial data can tell a person’s story, including one’s “religion, ideology, opinions, and interests”¹ as well as one’s “political leanings, locations, and more.”² Because of this data’s usefulness, federal law enforcement agencies increasingly coordinate with financial institutions to secure even greater access to Americans’ private financial information, often without legal process, and use federal laws like the Bank Secrecy Act (BSA) to do so. This interim report continues the oversight of the Committee on the Judiciary and its Select Subcommittee on the Weaponization of the Federal Government into financial surveillance in the United States. Based on nonpublic documents, this report sheds new light on the decaying state of Americans’ financial privacy and the federal government’s widespread, warrantless surveillance programs.

The Committee and Select Subcommittee began this investigation into government-led financial surveillance after a whistleblower disclosed that following the events of January 6, 2021, Bank of America (BoA), voluntarily and without legal process, provided the Federal Bureau of Investigation (FBI) with a list of names of all individuals who used a BoA credit or debit card in the Washington, D.C. region around that time.³ In response to these allegations and corroborating testimony from FBI officials, the Committee and Select Subcommittee requested documents from BoA and six other national financial institutions about the provision of Americans’ private financial information to federal law enforcement without legal process.⁴ On March 6, 2024, the Committee and Select Subcommittee released an interim report revealing that federal law enforcement had used sweeping search terms like “MAGA” and “TRUMP” to target Americans and even treated purchases of religious texts or firearms as indicators of “extremism.”⁵ That report detailed how federal law enforcement derisively viewed American citizens—treating Americans who expressed opposition to firearm regulations, open borders, COVID-19 lockdowns, vaccine mandates, and the “deep state” as potential domestic terrorists.⁶

Following these revelations, the Committee and Select Subcommittee requested additional documents and communications from seventeen different entities, including national banks, crowdfunding sites, money service businesses, and the U.S. Treasury Department, to further examine the federal government and financial institutions’ information-sharing relationship and to determine whether the federal government was abusing its access to Americans’ sensitive financial information.⁷ To date, the Committee and Select Subcommittee have reviewed over 48,000 pages of documents and conducted three additional transcribed interviews.

¹ *California Bankers Association v. Shultz*, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting).

² Nicholas Anthony, *What Does Financial Privacy Mean for Liberty?*, CATO Institute (Jul. 10, 2023).

³ Transcribed Interview of Mr. George Hill, former Supervisory Intelligence Analyst, FBI at 74-75 (Feb. 7, 2023).

⁴ *See, e.g.*, Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer, Bank of Am. Corp. (May 25, 2023); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Jamie Dimon, Chief Exec. Officer, JPMorgan Chase & Co. (Jun. 12, 2023).

⁵ *See* STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print 2024).

⁶ *Id.*

⁷ *See generally, e.g.*, Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Brian Moynihan, Chief Exec. Officer, Bank of Am. Corp. (Apr. 24, 2024).

The information obtained during the Committee and Select Subcommittee’s investigation, and detailed in this report, is concerning. Documents show that federal law enforcement increasingly works hand-in-glove with financial institutions, obtaining virtually unchecked access to private financial data and testing out new methods and new technology to continue the financial surveillance of American citizens.

- The FBI has manipulated the Suspicious Activity Report (SAR) filing process to treat financial institutions as *de facto* arms of law enforcement, issuing “requests,” without legal process, that amount to demands for information related to certain persons or activities it considers “suspicious.”**⁸ With narrow exception, federal law does not permit law enforcement to inquire into financial institutions’ customer information without some form of legal process.⁹ The FBI circumvents this process by tipping off financial institutions to “suspicious” individuals and encouraging these institutions to file a SAR—which does not require any legal process—and thereby provide federal law enforcement with access to confidential and highly sensitive information.¹⁰ In doing so, the FBI gets around the requirements of the Bank Secrecy Act (BSA), which, per the Treasury Department, specifies that “it is . . . *a bank’s responsibility*” to “file a SAR whenever *it* identifies ‘a suspicious transaction relevant to a possible violation of law or regulation’”¹¹ While at least one financial institution requested legal process from the FBI for information it was seeking,¹² all too often the FBI appeared to receive no pushback. In sum, by providing financial institutions with lists of people that it views as generally “suspicious” on the front end, the FBI has turned this framework on its head and contravened the Fourth Amendment’s requirements of particularity and probable cause.¹³
- In the days and weeks after January 6, 2021, the FBI coordinated with the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) to encourage financial institutions across the country to scour their data and file SARs on hundreds of Americans, if not more, without any clear criminal nexus.**¹⁴ Documents reveal that at least one financial institution took the initiative and reached out to FinCEN with an idea that would “support the Bureau’s efforts to address the acute threat of

⁸ See, e.g., Transcribed Interview of Mr. Peter Sullivan at 29 (Apr. 9, 2024) (discussing the FBI’s sharing of fact-based patters with financial institutions to identify potential threats); see also, e.g., Email from Peter Sullivan, FBI, to FBI employee and Bcc’d recipient [Redacted] at Santander (Jan. 15, 2021 3:25 PM) (SBNA_HJC_0001084); Email from Peter Sullivan, FBI, to FBI employee and Bcc’d recipients (Jan. 15, 2021 10:25 AM) (SCB-00002713).

⁹ See, e.g., 12 U.S.C. § 3413(g).

¹⁰ See Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of the Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (“SARs contain personally identifiable information about individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation . . .”)

¹¹ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2, 4 (Feb. 9, 2024) (emphasis added) (citing 31 U.S.C. § 5318(g)(1)).

¹² See, e.g., Email from [Redacted], Standard Chartered, to Peter Sullivan, FBI, and FBI employee (Apr. 20, 2021, 2:52 PM) (SCB-00002923).

¹³ See U.S. CONST. amend. IV.

¹⁴ See Transcribed Interview of Mr. Peter Sullivan at 31-32, 34-35 (Apr. 9, 2024).

domestic terrorism.”¹⁵ That financial institution encouraged FinCEN to use SARs as the basis for issuing Patriot Act 314(a) requests, which allows FinCEN “to canvas the nation’s financial institutions for potential lead information” from “more than 37,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering.”¹⁶

- **The government’s access to Americans’ private financial data is widespread and virtually unchecked.** In 2023, financial institutions filed 4.6 million SARs and 20.8 million Currency Transaction Reports (CTRs) with FinCEN, which are accessible to government officials for querying and downloading via various programs.¹⁷ According to FinCEN, at least 25,000 authorized users across federal, state, and local government have warrantless access to these filings, known as BSA data, through the FinCEN Query program.¹⁸ In 2023, government officials ran 3,362,735 searches of the filings in the FinCEN Query program.¹⁹ In addition to the FinCEN Query program, approximately 27,000 federal officials have access to BSA data through the Agency Integrated Access (AIA) program that allows certain federal agencies to download the data onto their own systems.²⁰ In total, according to FinCEN, “472 federal, state, and local law enforcement, regulatory, and national security agencies have access to BSA reports”²¹
- **Financial institutions and FinCEN are expanding their capacity to surveil Americans through new, confidential projects and emerging technologies.** Officially, the Bank Secrecy Act Advisory Group (BSAAG) serves as an advisory body to the Treasury Department on issues related to the BSA.²² However, in practice, documents obtained by the Committee and Select Subcommittee indicate that it is also a tool for federal law enforcement and financial institutions to monitor the private, financial data of American citizens.²³ Previously confidential BSAAG documents indicate that it is advancing plans that would require Americans to have a digital identification to access financial services, testing artificial intelligence to surveil Americans’ financial activity, and working towards even closer coordination between financial institutions and federal law enforcement.

¹⁵ See Email from [Redacted], MUFG, to FinCEN employee (Jan. 13, 2021, 6:41 PM) (MUFG-0000248-249).

¹⁶ FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN’S 314(A) FACT SHEET (Feb. 26, 2019).

¹⁷ FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).

¹⁸ *Id.* at 3.

¹⁹ Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (Apr. 25, 2024, 5:03 PM).

²⁰ Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024, 2:44 PM). FinCEN “does not have an exact contemporaneous count of the number of [government] users” with AIA access. See Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (Apr. 25, 2024, 5:03 PM).

²¹ FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).

²² Bank Secrecy Act Advisory Group; Solicitation of Application for Membership, 88 Fed. Reg. 9329 (Financial Crimes Enforcement Network Feb. 13, 2023).

²³ FINANCIAL CRIMES ENFORCEMENT NETWORK, CHARTER OF THE BANK SECRECY ACT ADVISORY GROUP, <https://www.fincen.gov/sites/default/files/shared/charter.pdf> (last visited Oct. 10, 2024).

All Americans should be disturbed by how their financial data is collected, made accessible to, and searched by federal and state officials, including law enforcement and regulatory agencies. With the rise in e-commerce and the widespread adoption of cash alternatives like credit cards or peer-to-peer payment services, the future leaves very little financial activity beyond the purview of modern financial institutions or the government's prying eyes. This is because, as a condition of participating in the modern economy, Americans are forced to disclose details of their private lives to a financial industry that has been too eager to pass this information along to federal law enforcement.

The Committee's and Select Subcommittee's investigation makes clear that federal law enforcement has taken advantage of this dynamic by deploying financial institutions as arms of federal law enforcement, directing financial institutions to profile Americans using the typologies it distributes or urging financial institutions to identify any "suspicious activity" an individual may have engaged in.²⁴ As promoted by the BSAAG, this surveillance will be catalyzed by even greater government entanglement with financial institutions as they begin to integrate new technology to more effectively track their customers' financial habits. Absent renewed safeguards, the federal government and financial institutions will continue to siphon off Americans' sensitive financial data, place it into the hands of bureaucrats, and erode any remaining semblance of financial privacy in the United States.

²⁴ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print 2024).

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
THE BSA REGIME INVITES EVER-INCREASING FINANCIAL SURVEILLANCE	6
A. The reporting requirements of the Bank Secrecy Act (BSA) turn financial institutions into confidential informants that are required to secretly report Americans’ financial activities to the federal government.....	6
i. Financial institutions report millions of Americans’ transactions to the federal government as part of the BSA’s excessive reporting requirements.....	8
ii. In order to effectuate the BSA, banks must engage in mass surveillance of Americans’ transactions.	12
B. The BSA and related programs provide law enforcement officials with broad, warrantless access to Americans’ data.....	15
i. Thousands of law enforcement officials have warrantless access to Americans’ financial information through a vast and searchable system.....	16
ii. FinCEN provides federal law enforcement agencies the ability to copy and transfer entire BSA data sets from FinCEN, onto their own systems, and access it without a warrant.	17
iii. In addition to law enforcement’s access to Americans’ financial information, some financial institutions use third-party contractors to monitor and report on their customers’ transactions.	18
iv. FinCEN appeared to have registered an individual with no affiliation to BoA into the 314(b) information-sharing system.	19
FEDERAL LAW ENFORCEMENT AND ITS PARTNERS ABUSE THE BSA’S INFORMATION SHARING REGIME.....	22
A. Federal law enforcement has broad discretion in what it considers “suspicious” financial activity and often shares that information with financial institutions to review their customers’ transactions and file SARs accordingly.....	23
B. FinCEN solicits customer transaction information from financial institutions, on behalf of the FBI, even if the transaction activity lacks a clear nexus to criminal activity.....	33
C. The federal government, through the BSAAG advisory group, is increasing its coordination with financial institutions and pushing them to adopt new and invasive technologies that increase their ability to surveil Americans.....	39
i. BSAAG documents indicate that Big Banks and Big Government are advancing the implementation of a national digital ID system.....	39
ii. The federal government encouraged financial institutions to incorporate new technologies, including artificial intelligence and machine learning, into their systems to more aggressively track Americans.....	42
POTENTIAL LEGISLATIVE REFORMS	44
CONCLUSION.....	46

THE BSA REGIME INVITES EVER-INCREASING FINANCIAL SURVEILLANCE

Documents obtained by the Committee and Select Subcommittee demonstrate that federal law enforcement increasingly relies on financial institutions for highly sensitive information about Americans without legal process. Federal law enforcement has effectively deputized financial institutions to advance its investigations and to gain access to the information that financial institutions possess. As financial institutions' capacity to track and gather data on Americans continues to increase, federal law enforcement will continue to be incentivized to rely on banks for easy access to sensitive information about Americans' private lives.

A. The reporting requirements of the Bank Secrecy Act turn financial institutions into confidential informants that are required to secretly report Americans' financial activities to the federal government.

Enacted by Congress in 1970, the Bank Secrecy Act (BSA)²⁵ and succeeding legislation are “the primary U.S. anti-money laundering (AML) law[s]’ regulating financial institutions,”²⁶ and that authorize the Treasury Department to impose far-reaching reporting obligations on businesses and financial institutions.²⁷ The BSA is primarily enforced by the Treasury Department’s Financial Crimes Enforcement Network (FinCEN).²⁸ According to FinCEN, its mission “is to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security”²⁹ Consistent with that mission, the BSA is touted as the “principal U.S. law for the prevention of money laundering, terrorist financing and proliferation, and other forms of illicit financial activity.”³⁰

Pursuant to the BSA and other anti-money laundering laws, covered financial institutions operating in the United States—like banks—are required to file certain reports, such as Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs), with the federal government reflecting their customers’ information and their financial activities.³¹ A financial institution is required to file a CTR on any person who conducts a transaction over \$10,000 or multiple transactions that amount to over \$10,000 in a single day.³² Likewise, the BSA “requires that a bank or other financial institution file a SAR whenever it identifies ‘a suspicious transaction *relevant to a possible violation of law or regulation.*’”³³ The BSA also grants broad

²⁵ Pub. L. No. 91-508 (1970).

²⁶ JAY B. SYKES, CONG. RESEARCH SERV., R45076, TRENDS IN BANK SECRECY ACT/ANTI-MONEY LAUNDERING ENFORCEMENT (2018) (internal citation omitted).

²⁷ See, e.g., FINANCIAL CRIMES ENFORCEMENT NETWORK, THE BANK SECRECY ACT.

²⁸ FINANCIAL CRIMES ENFORCEMENT NETWORK, WHAT WE DO.

²⁹ FINANCIAL CRIMES ENFORCEMENT NETWORK, MISSION.

³⁰ Review of Bank Secrecy Act Regulations and Guidance, 86 Fed. Reg. 238 (Financial Crimes Enforcement Network Dec. 15, 2021).

³¹ See, e.g., 31 U.S.C. §§ 5313, 5314; see also Transcribed Interview of Mr. Jimmy Kirby at 46, 51 (July 18, 2024).

³² 31 U.S.C. § 5313; 31 C.F.R. § 1010.330; see also FIN. CRIMES ENFORCEMENT NETWORK, NOTICE TO CUSTOMERS: A CTR REFERENCE GUIDE, <https://www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf> (last visited Sept. 26, 2024).

³³ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (emphasis added).

immunity to “[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency”³⁴

The BSA’s reporting requirements are also extremely broad and are not limited to potentially criminal conduct.³⁵ When a financial institution files a SAR, it must make sensitive information available to the Treasury Department, including “personally identifiable information about individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation.”³⁶ These filings are ostensibly subject to “strong confidentiality protections” that purport to limit access to the highly sensitive information they contain.³⁷ However, despite these protections, the Treasury Department estimates that tens of thousands of government officials have warrantless access to these filings.³⁸

The BSA regime creates strong incentives for financial institutions to over-file SARs about American citizens—at the cost of Americans’ financial privacy. In a transcribed interview with the Committee and Select Subcommittee, FinCEN Deputy Director Jimmy Kirby explained:

There’s the mandatory requirement and then there’s the ability to voluntarily file, as the statutory construct laid out by Congress really is to encourage filing. So . . . there’s the ones you’re required to file, but there’s also very much an encouragement for people to voluntarily file beyond what they’re required to file.³⁹

In addition to the voluntary filing option, financial institutions have a further incentive to over-file because failing to file a SAR can result in large monetary penalties.⁴⁰ As a consequence, financial institutions often file defensively, even when there is little reason to do so.⁴¹ This dynamic is compounded by the BSA’s broad grant of immunity which protects “[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency.”⁴² Financial institutions are also placed under a *de facto* gag order prohibiting the revelation of “any information that would reveal that the transaction has been

³⁴ 31 U.S.C. 5318(g)(3).

³⁵ Transcribed Interview of Mr. Jimmy Kirby at 46 (July 18, 2024) (explaining it could involve civil law violations).

³⁶ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024).

³⁷ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024).

³⁸ See Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024, 2:44 PM).

³⁹ Transcribed Interview of Mr. Jimmy Kirby at 46 (July 18, 2024).

⁴⁰ See, e.g., FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN PENALIZES U.S. BANK OFFICIAL FOR CORPORATE ANTI-MONEY LAUNDERING FAILURES (Mar. 4, 2020) (noting that FinCEN assessed \$450,000 civil penalty against U.S. Bank Official for “failure to prevent violations of the Bank Secrecy Act” and \$185 million civil penalty against U.S. Bank for “willfully violating the BSA’s requirements”).

⁴¹ *Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI): Hearing Before the H. Comm. on Financial Services*, 118th Cong. 4 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.).

⁴² 31 U.S.C. 5318(g)(3).

reported.”⁴³ Viewing this framework together, financial institutions frequently err on the side of over-filing.⁴⁴

During his transcribed interview with the Committee and Select Subcommittee, Peter Sullivan, former FBI Senior Private Sector Partner for Outreach within the Strategic Partner Engagement Section, acknowledged how useful sensitive financial data can be to law enforcement.⁴⁵ He explained that “financial intelligence can illuminate a lot of deliberate information . . . it could tell the pattern of life.”⁴⁶ Now, decades removed from the BSA’s enactment, financial institutions are able to collect and report more granular financial data than ever, heightening privacy concerns for Americans and casting renewed doubt on the BSA’s constitutionality.⁴⁷

i. Financial institutions report millions of Americans’ transactions to the federal government as part of the BSA’s excessive reporting requirements.

The BSA’s reporting requirements have gone far beyond providing the government with reports and records that will be “highly useful in ‘criminal, tax, or regulatory investigations or proceedings.’”⁴⁸ Instead, the BSA has become a dragnet that forces financial institutions to report millions of transactions to the federal government each year for potentially “suspicious activity” without any clear nexus to unlawful behavior.⁴⁹ The staggering number of these filings demonstrate the breadth of the BSA’s reporting requirements and, with it, the number of Americans’ transactions that are increasingly swept up by its reach. Indeed, according to Sullivan, the reach of one single SAR can be enormous. He testified that he has seen “many SARs that have more than one individual on the SAR . . . I have seen thousands.”⁵⁰

According to FinCEN, it received over 25.4 million BSA reports from 294,000 separate financial institutions and other entities in fiscal year 2023.⁵¹ Among those filings, FinCEN reported that it received an average of 57,000 CTRs per day.⁵² Given the threshold for the reporting requirement, the volume of CTR filings should not come as a surprise. In a letter to FinCEN, the American Bankers Association (ABA) explained the absurdity of the CTR filing

⁴³ 31 U.S.C. 5318(g)(2).

⁴⁴ See *Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligences (TFI): Hearing Before the H. Comm. on Financial Services*, 118th Cong. 4 (Feb. 12, 2024) (statement for the record of Brian Knight, Senior Research Fellow, George Mason Univ.).

⁴⁵ See Transcribed Interview of Mr. Peter Sullivan at 41 (Apr. 9, 2024).

⁴⁶ *Id.*

⁴⁷ See Norbert Michel, *Experts Agree That Financial Privacy Needs A Revamp*, FORBES (Sept. 16, 2024); see also Brian Knight, *Is the Bank Secrecy Act Vulnerable to Constitutional Challenge over post January 6th Data Collection?*, FINREGRAG (Feb. 26, 2024).

⁴⁸ *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Govt. of the H. Comm. on the Judiciary*, 118th Cong. 6 (2024) (testimony of Norbert Michel, Vice President and Director, CATO).

⁴⁹ See *id.* at 10.

⁵⁰ Transcribed Interview of Mr. Peter Sullivan at 100 (Apr. 9, 2024).

⁵¹ FINANCIAL CRIMES ENFORCEMENT NETWORK, *FINCEN YEAR IN REVIEW FOR FY 2023* (June 2024) (noting that in addition to financial institutions, individuals, companies, corporations, etc. are required to report cash payments of over \$10,000).

⁵² FINANCIAL CRIMES ENFORCEMENT NETWORK, *FINCEN YEAR IN REVIEW FOR FY 2023* (June 2024).

threshold, stating, decades “after the inception of this threshold, \$10,000 is no longer an unusually large transaction.”⁵³ If adjusted for inflation, the \$10,000 threshold—which was set more than 50 years ago—would be nearly \$75,000 today.⁵⁴ The ABA observed, “CTR reports have proliferated exponentially and . . . are no longer inherently tied to combating financial crime.”⁵⁵ To further illustrate, if a consumer purchased a car, furniture, jewelry, art, or made a tuition payment totaling more than \$10,000, a CTR was likely filed containing the consumer’s information despite there being no evidence of any suspicious activity.⁵⁶

With respect to SAR filings, the trend is the same. FinCEN reported receiving a daily average of 12,600 SAR filings, totaling more than 4.6 million in 2023.⁵⁷ FinCEN reported “Other Suspicious Activities” as the most cited reason why a financial institution filed a SAR in 2023, making up an overwhelming portion of the annual filings—totaling 3.174 million.⁵⁸ By comparison, “money laundering” accounted for just 1.629 million reports and “terrorist financing” accounted for only 1,500 filings—the least reported reason for why a SAR was filed.⁵⁹ These data confirm that FinCEN is using the BSA and its SAR reporting requirements to collect far more than “highly useful” reports on transactions that may be related to money laundering and terrorist financing. Instead, FinCEN regularly receives information about private transactions concerning “Other Suspicious Activities” that Americans may be engaged in, completely disconnected from FinCEN’s stated mission or the stated purpose of the BSA.

⁵³ American Bankers Association, *Letter to FinCEN on Information Collection Requirements relating to Currency Transaction Reports* (Apr. 5, 2024).

⁵⁴ See Nicholas Anthony, *How Inflation Erodes Financial Privacy*, CATO (June 10, 2022).

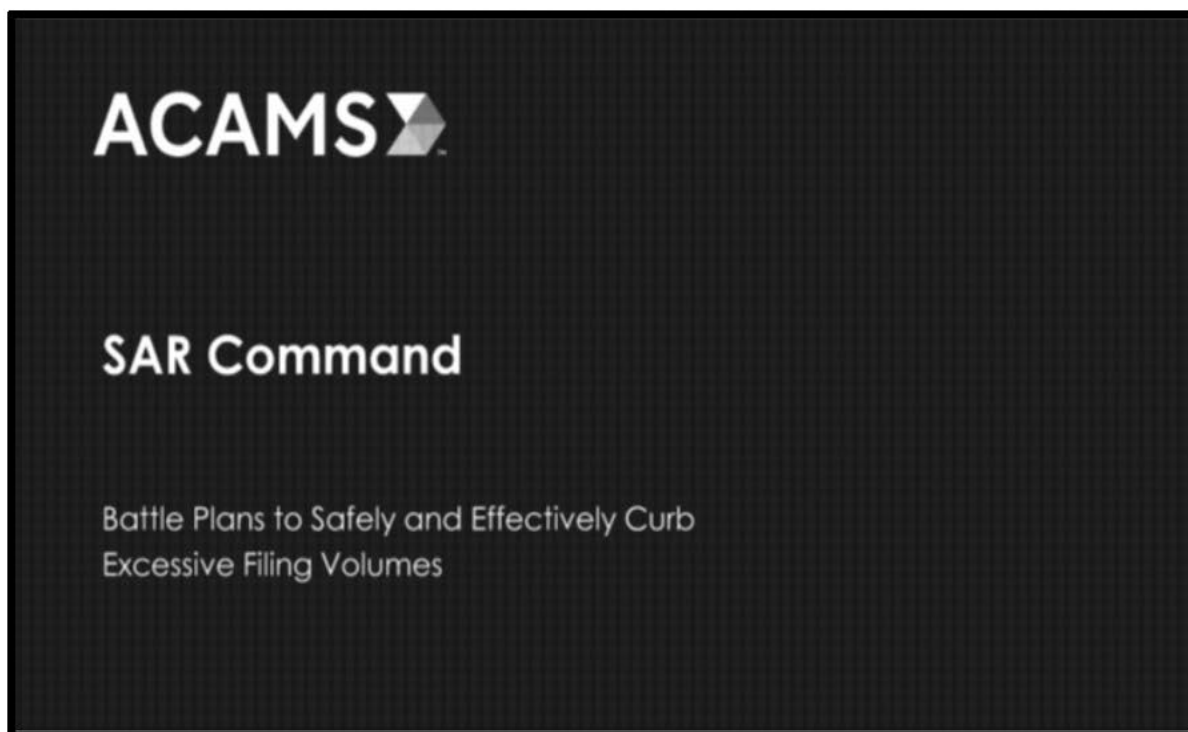
⁵⁵ American Bankers Association, *supra* note 53.

⁵⁶ INTERNAL REVENUE SERVICE, UNDERSTAND HOW TO REPORT LARGE CASH TRANSACTIONS (FEB. 2021).

⁵⁷ FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).

⁵⁸ *Id.*

⁵⁹ *Id.*; see also *Special Report: suspicious activity reports surge; 2023 filings on pace for another record*, THOMSON REUTERS (June 9, 2023).



ACAMS slideshow on curbing Excessive SAR Filing Volumes that implicate Americans.
 —Association of Certified Anti-Money Laundering Specialists

The explosion of BSA-required filings has become a topic of discussion in the industry. One of the purported leading groups in the financial crimes space is the Association of Certified Anti-Money Laundering Specialists (ACAMS), which describes itself as “the largest international membership organization for Anti-Financial Crime professionals”⁶⁰ and provides “the global gold standard in AML [Anti-Money Laundering] certifications.”⁶¹ A slideshow obtained by the Committee and Select Subcommittee shows that even ACAMS believes that SAR over-filing is a problem.⁶² According to these documents, on May 9, 2023, ACAMS hosted a panel titled, “SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes.”⁶³ In the description of the panel, “[l]ed by seasoned compliance veterans,” ACAMS observed: “To paraphrase a saying about the weather, everybody complains about high SAR volumes, but nobody does anything about it,” and explained that the panel’s discussion would focus on “the current climate of escalating SAR filing volumes.”⁶⁴ One slide from the presentation showed a 118-percent surge in SAR filings over the last decade.⁶⁵

⁶⁰ ACAMS, *About Us*, <https://www.acams.org/en/about#about-us-c4ffaef2> (last visited Sept. 27, 2024).

⁶¹ ACAMS, <https://www.acams.org/en> (last visited Sept. 27, 2024).

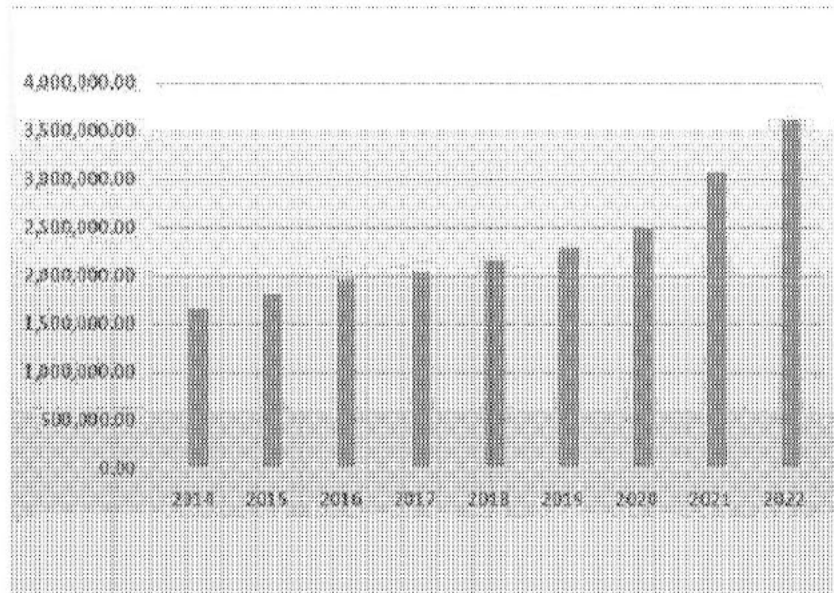
⁶² *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002809).

⁶³ Wintrust Financial Corp., Truist Financial Corp., HSBC, NICE Actimize, *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS (May 9, 2023) (118HJC_00005985).

⁶⁴ Wintrust Financial Corp., Truist Financial Corp., HSBC, NICE Actimize, *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS (May 9, 2023) (118HJC_00005985).

⁶⁵ *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002806).

Annual SAR Filings Increased by 118% since 2014



ACAMS

© 2023 ACAMS. All Rights Reserved. 7

SAR Filings increased by 118% from 2014 to 2022.
 —Association of Certified Anti-Money Laundering Specialists

Another slide from the panel’s discussion on “curb[ing] excessive filing volumes” touched on “the need to change” the BSA regime.⁶⁶ According to ACAMS, SAR numbers are increasing, despite law enforcement having “[l]imited success” in using SARs as part of their criminal investigations.⁶⁷ The ACAMS slide aptly described the over-filing problem, by inquiring “do[es] law enforcement want to know everything or do they want intelligent SARs?”⁶⁸ Under the current BSA regime, law enforcement appears to want to know everything. As this report details, financial institutions are filing millions of SARs on Americans’ transactions in the hopes that it will appease law enforcement’s appetite to “know everything.”

⁶⁶ *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002805).

⁶⁷ *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002805).

⁶⁸ *SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes*, ACAMS, Slideshow (TFC002805).

The need to change how we file SAR's

- o Increasing SAR numbers
- o Increasing financial crime proceeds
- o Limited success of law enforcement

SARs need to inform law enforcement, not just tick a box

- o What does law enforcement need to know
 - o 5WH (Who, What, Where, When, Why and How!)
- o How do we as FIs get that information?
- o What does law enforcement need our help with?
- o A decision needs to be made, do law enforcement want to know everything or do they want intelligent SARs?

ACAMS

© 2023 ACAMS. All Rights Reserved 16

“Do[es] law enforcement want to know everything or do they want intelligent SARs?”
—Association of Certified Anti-Money Laundering Specialists

ii. In order to effectuate the BSA’s requirements, financial institutions must engage in mass surveillance of Americans’ private transactions.

To comply with the BSA and related requirements, banks must establish a “BSA/AML [Anti-Money Laundering] compliance program” that includes “proper monitoring and reporting processes” to “identify unusual activity” and monitor “suspicious activity.”⁶⁹ These “[m]onitoring systems typically include . . . transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.”⁷⁰ With so much data collected by financial institutions, this monitoring is becoming increasingly widespread.

In a July 2022 presentation about these compliance programs, the ABA explained how financial institutions “identify[] the suspicious activity” using a technique called “surveillance monitoring.”⁷¹ To reinforce the point, a picture on the slide showed a figure monitoring several one-way video feeds for “suspicious” activities.⁷² The slide explained that “surveillance monitoring” programs “are designed to capture a wide range of account activity, such as cash activity, fund transfers, automated clearing house (ACH) transfers, and ATM transactions and include rule-based and intelligent systems to detect unusual or higher-risk transactions.”⁷³ With the assistance of technology, the slide noted, these systems are becoming increasingly

⁶⁹ FED. FIN. INST. EXAMINATION COUNCIL, ASSESSING COMPLIANCE WITH BSA REGULATORY REQUIREMENTS, <https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04> (last visited Oct. 1, 2024).

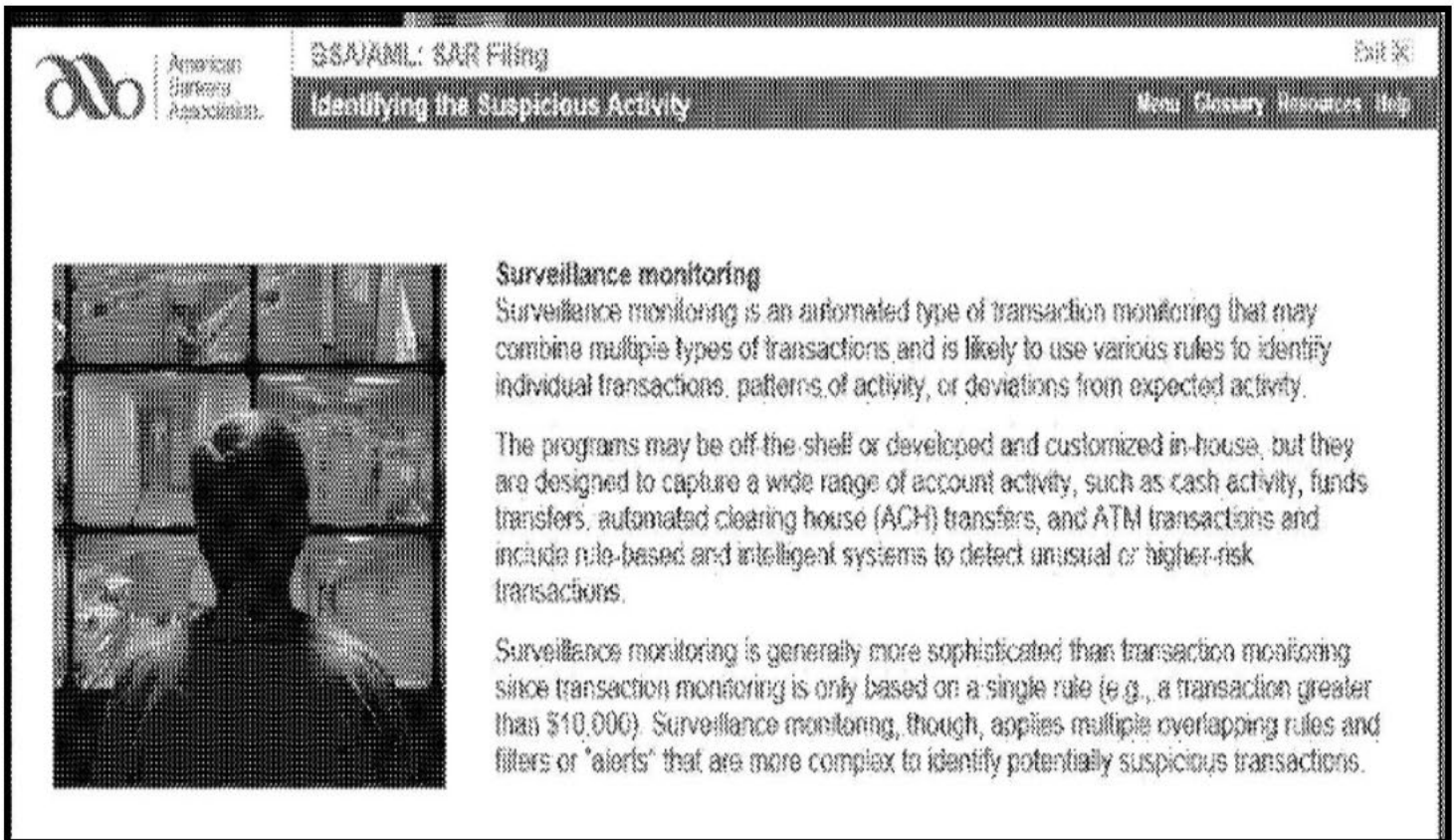
⁷⁰ *Id.*

⁷¹ *BSA/AML: SAR Filing*, American Bankers Association (July 2022) (SBNA_HJC_0000727).

⁷² *Id.*

⁷³ *Id.*

intelligent.⁷⁴ One report on BSA/AML compliance also noted that while “regulators do not require the use of any particular technology or system, they encourage (and expect) use of innovative technology to increase the efficacy of BSA/AML programs.”⁷⁵



BSA/AML: SAR Filing Exit X

Identifying the Suspicious Activity How Doesy Monitor the

Surveillance monitoring

Surveillance monitoring is an automated type of transaction monitoring that may combine multiple types of transactions and is likely to use various rules to identify individual transactions, patterns of activity, or deviations from expected activity.

The programs may be off-the-shelf or developed and customized in-house, but they are designed to capture a wide range of account activity, such as cash activity, funds transfers, automated clearing house (ACH) transfers, and ATM transactions and include rule-based and intelligent systems to detect unusual or higher-risk transactions.

Surveillance monitoring is generally more sophisticated than transaction monitoring since transaction monitoring is only based on a single rule (e.g., a transaction greater than \$10,000). Surveillance monitoring, though, applies multiple overlapping rules and filters or “alerts” that are more complex to identify potentially suspicious transactions.

“Surveillance monitoring is an automated type of transaction monitoring . . . to identify individual transactions [and] patterns of activity. . . .”

—American Bankers Association Slideshow

Americans should be rightly skeptical of a federal regime like the BSA that requires unaccountable financial institutions, on behalf of federal law enforcement, to build out a surreptitious and highly sophisticated surveillance system for monitoring and secretly flagging Americans’ transactions as “suspicious” or “unusual.” As the former Director of the Office of Stakeholder Integration and Engagement in the Strategic Operations Division at FinCEN explained, a bank’s surveillance system is “[l]egal and required” under federal law.⁷⁶ He testified:

Q. . . . And [are there] investigators in, particularly the banks that are large enough to have multiple employees and entire

⁷⁴ *Id.*

⁷⁵ *BSA/AML and International Trade Enforcement And Compliance Annual Update*, Gibson Dunn 97 (Feb. 7, 2024).

⁷⁶ Transcribed Interview of the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 54 (May 14, 2024).

compliance units, whose job it is to search and monitor their customers' financial records for suspicious activity that must be reported?

A. Yes.

Q. And based on your experience both at a financial institution and at FinCEN, that type of monitoring by a bank, by a financial institution of its own customers' data, that's entirely legal, correct?

A. Legal and required.

Q. Legal and required?

A. Yeah.

Q. No subpoenas required, no—no warrant is required?

A. Correct.⁷⁷

The mass monitoring by financial institutions opens the door for federal law enforcement to spy on Americans' constitutionally protected activity. For example, on September 28, 2022, Peter Sullivan and a representative from Wells Fargo presented at an ABA webinar, titled "Domestic Terrorism: A Threat to the Financial System."⁷⁸ Their presentation included a slide titled "Radicalization & Warning Signs."⁷⁹ The slide illustrated how banks should review a customer's transactions, explaining the transition from a "sympathizer" of a cause (which the ABA concedes is legal), to an "activist" (which is also labeled as legal), to an "extremist" (which begins the shift from "legal to illegal"), and, ultimately, to engaging in illegal "terrorist" activities.⁸⁰ While the presentation included a disclaimer that "[b]anks don't want to interfere with customers' First Amendment rights,"⁸¹ by highlighting transactions related to First and Second Amendment activity as an early sign of radicalization, the slide seemed to encourage financial institutions to begin tracking Americans' transactions even when they are engaged in constitutionally-protected activity. For example, the "warning signs" that the ABA suggests banks should look for include customers making "payments related to extremist political activity or donations to the cause," "more financial commitment to the cause," and the "purchase [of] weapons, gear, literature & other inflammatory propaganda," which the ABA concedes are all

⁷⁷ *Id.*

⁷⁸ Domestic Terrorism: A Threat to the Financial System, American Bankers Association (Sept. 28, 2022) (HJC118_00000502-503).

⁷⁹ *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000521).

⁸⁰ *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000521).

⁸¹ *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000522).

“legal” activities.⁸² In effect, the ABA appears to be indicating that tracking Americans’ political donations, the literature they purchase, and the firearms they buy, are all a necessary prerequisite to identifying potential extremist or illegal activity.

Radicalization & Warning Signs

- Sympathizer (interest in cause) → *legal*
 - Mindset
 - Payments related to extremist political activity or donations to the cause
- Activist (engagement in cause) → *legal*
 - Lifestyle change
 - More financial commitment to the cause
 - Capacity development
 - Purchase weapons, gear, literature & other inflammatory propaganda
- Extremist (as passion & commitment grow, escalates from non-violent to violent) → *from legal to illegal*
 - Concealment of activities
 - Realization that law enforcement might be looking at them (financial activity)
 - Operational planning & preparation
 - Plan, surveil, select targets, travel & other activity leading them toward action
- Terrorist → *illegal*
 - Personal preparation
 - Finalize their personal preparation, settle their business & move into action

aba.com1-800-BANKERS

20



ABA slide illustrating when financial institutions should begin tracking customers’ transactions, including when engaged in “legal” activity.
—American Bankers Association Slideshow

In effect, the BSA requires financial institutions to engage in mass surveillance of Americans’ transactions and report en masse their personal information and financial activities to the federal government. Once filed, federal officials, through multiple programs, have warrantless access to search through the SARs and CTRs filed on Americans.

B. The BSA and Treasury Department programs provide law enforcement officials with broad, warrantless access to Americans’ financial data.

The Treasury Department claims that access to confidential BSA documents is limited in part because SARs “contain personally identifiable information, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation.”⁸³

⁸² *Domestic Terrorism: A Threat to the Financial System*, American Bankers Association (Sept. 28, 2022) (HJC118_00000521).

⁸³ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 1 (July 31, 2024).

Therefore, BSA “documents or the information therein should not be disclosed to, accessed by, or disseminated to unauthorized individuals in any fashion.”⁸⁴ However, despite these sensitivities, tens of thousands of government personnel have widespread and warrantless access to BSA data, like SARs and CTRs, through FinCEN programs, and, in some circumstances, programs that leave FinCEN and Congress in the dark about how BSA data is used once it is accessed.

i. Thousands of law enforcement officials have warrantless access to Americans’ financial information through a vast and searchable system.

A Treasury Department program known as the FinCEN Query system grants thousands of federal, state, and local law enforcement officials the ability to “easily and quickly access, query, and analyze” BSA data through a Memorandum of Understanding (MOU) with each entity.⁸⁵ FinCEN also provides access to this program, through MOUs, to employees from intelligence agencies and other external financial regulatory agencies “to conduct official agency business.”⁸⁶ According to the Office of Inspector General (OIG) of the Treasury Department, FinCEN has “475 MOUs with external LE [law enforcement], intelligence, and regulatory agencies.”⁸⁷ Once a “partner agenc[y]” reaches an MOU agreement with FinCEN it “identif[ies] employees for access to the system” and, once identified, the agency provides those users with a “unique login” to access the FinCEN Query system and begin running searches.⁸⁸ Users can search “first and last names or parts of addresses,” as well as other “keywords” and “search terms” to “scan across all text fields.”⁸⁹ Searches conducted in the FinCEN Query system are logged by FinCEN in an audit log.⁹⁰

During his transcribed interview, FinCEN Deputy Director Kirby described how the query system works. Using his name as an example, Kirby testified that a search for “Jimmy Kirby” would reveal any “SARs that have been filed on [Jimmy Kirby] . . . to the extent a bank has filed currency transaction reports or a non-bank has filed a Form 8300 on [Jimmy Kirby], you would see those” and “any of the other BSA forms that involve [Jimmy Kirby], you would be able to see those,” it would be the “universe of . . . what has been filed on [Jimmy Kirby].”⁹¹ Indeed, because these reporting “obligations apply to U.S. financial institutions,” Kirby explained, it is safe to assume that a “substantial portion,” if not the “majority of the filings,” involve “U.S. persons.”⁹² Thousands of law enforcement personnel can generally conduct these searches on the FinCEN Query system without ever needing a warrant or any legal process.⁹³

⁸⁴ *Id.*

⁸⁵ See FINANCIAL CRIMES ENFORCEMENT NETWORK, FACT SHEET FINCEN QUERY; *see also* Transcribed Interview of Mr. Jimmy Kirby at 72, 73-74 (July 18, 2024); FINANCIAL CRIMES ENFORCEMENT NETWORK, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2023 (2024).

⁸⁶ U.S. DEP’T OF TREASURY, OFF. OF INSPECTOR GEN., AUDIT OF FINCEN’S MANAGEMENT OF BSA DATA – USER ACCESS REPORT 4 (Aug. 1, 2024).

⁸⁷ U.S. DEP’T OF TREASURY, OFF. OF INSPECTOR GEN., AUDIT OF FINCEN’S MANAGEMENT OF BSA DATA - SUPPRESSION REPORT 4 (Aug. 31, 2023).

⁸⁸ Transcribed Interview of Mr. Jimmy Kirby at 73 (July 18, 2024).

⁸⁹ FINANCIAL CRIMES ENFORCEMENT NETWORK, FACT SHEET FINCEN QUERY.

⁹⁰ Transcribed Interview of Mr. Jimmy Kirby at 73 (July 18, 2024).

⁹¹ *Id.* at 74-75.

⁹² *Id.* at 78.

⁹³ *Id.* at 72, 74-76.

FinCEN informed the Committee and Select Subcommittee that, in 2023, there were 14,415 registered and authorized users with access to the FinCEN Query system.⁹⁴ That year, users conducted 3,362,735 million searches of the database without a warrant or legal process, amounting to an average of 9,212 searches per day.⁹⁵

However, the FinCEN Query system, including its searches and authorized users, do not reflect a complete picture of government officials' access to, or their searches, of Americans' financial data. In fact, according to FinCEN, "FinCEN Query users represent only a fraction of users who access" BSA data.⁹⁶ In other words, the number of government searches that FinCEN reported of its BSA data, and the number of government officials with access to the BSA data, is likely much higher. Another FinCEN program, called Agency Integrated Access, provides an additional avenue for federal officials to transfer, access, and use BSA data with little to no oversight from FinCEN.

ii. FinCEN provides federal law enforcement agencies the ability to copy and transfer entire BSA data sets from FinCEN, onto their own systems, and access it without a warrant.

FinCEN's Agency Integrated Access (AIA) program provides approved federal agencies the "ability to ingest the BSA data that is filed with FinCEN" if the agency has an MOU in place with FinCEN.⁹⁷ The Treasury OIG describes AIA as the "transfer of entire copy sets of FinCEN BSA data to an external agency" by "downloading an encrypted file daily from [the] FinCEN Portal"⁹⁸ From then on, FinCEN Deputy Director Kirby explained, "those agencies control the access to that data on their systems."⁹⁹ Once a partnered agency imports the BSA data onto their system, FinCEN does not maintain "visibility" into how the agency uses the data.¹⁰⁰

FinCEN informed the Committee and Select Subcommittee that "because the agencies manage [their AIA] user accounts, FinCEN does not have an exact contemporaneous count of the number of [government] users" with AIA access.¹⁰¹ However, as of September 2023, FinCEN reported "approximately 27,000 authorized agency users who had access to BSA data through AIA agencies," comprising nine federal law enforcement and national security agencies, including the FBI, Internal Revenue Service (IRS), National Security Agency (NSA), United States Secret Service (USSS), Immigration and Customs Enforcement (ICE), Organized Crime and Drug Enforcement Task Forces (OCDETF), National Counterterrorism Center (NCTC), and

⁹⁴ Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (Apr. 8, 2024 10:48 AM).

⁹⁵ *Id.*

⁹⁶ U.S. DEP'T OF TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN YEAR IN REVIEW FOR FY 2022.

⁹⁷ Transcribed Interview of Mr. Jimmy Kirby at 72, 81 (July 18, 2024).

⁹⁸ U.S. DEP'T OF TREASURY, OFF. OF INSPECTOR GEN., AUDIT OF FINCEN'S MANAGEMENT OF BSA DATA - SUPPRESSION REPORT 1, 5 (Aug. 31, 2023).

⁹⁹ Transcribed Interview of Mr. Jimmy Kirby at 72 (July 18, 2024).

¹⁰⁰ *Id.* at 72, 81.

¹⁰¹ Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024 2:44 PM).

one other agency whose involvement is classified.¹⁰² With this access, these federal agencies download the “same BSA filings” onto their own systems instead of using the auditable FinCEN Query system.¹⁰³

The very existence of the AIA program—which allows certain federal agencies to download the same data already made available through FinCEN Query—suggests that its purpose is to provide federal agencies with the ability to access and use BSA data outside the scope of the FinCEN Query system. Given that AIA access does not provide FinCEN with the “same degree of visibility” as FinCEN Query and grants the receiving agency “control [of] the access to that data,” federal law enforcement appears to operate in a regulatory blind spot in its use of Americans’ financial data and in an environment ripe for federal surveillance.¹⁰⁴

iii. In addition to law enforcement’s access to Americans’ financial information, some financial institutions use third-party contractors to monitor and report on their customers’ confidential transactions.

According to documents obtained by the Committee and Select Subcommittee, some financial institutions also appear to be sharing confidential BSA data with “third party vendors.”¹⁰⁵ On February 5, 2024, the Bank Secrecy Act Advisory Group (BSAAG) shared a draft white paper with its members that “addresse[d] unique issues that arise with BSA data and third-party relationships” and “to communicate . . . clear, consistent, cross-industry guidance/practices for information security and confidentiality when sharing BSA data with third parties.”¹⁰⁶ This white paper illustrates the concerning practice of third-party vendors with access to confidential BSA data and that are responsible for “monitoring” Americans’ banking activity.

The white paper discussed “Third Party BSA Data Sharing,” a practice in which financial institutions contract with vendors that offer “Financial Crimes Management” solutions, such as “transaction monitoring, customer due diligence, and other features”¹⁰⁷ It explained how financial institutions may use these vendors “to augment their BSA staffing” and to “assign[] tasks in the review of transaction monitoring alerts, unusual activity investigation, or even [the] SAR preparation process” despite the fact that regulators “have not addressed the question of whether information subject to SAR confidentiality rules may be shared with business relationship partners”¹⁰⁸ Still, financial institutions appear to be contracting with vendors

¹⁰² Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 2, 2024 2:44 PM); Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 10, 2024 11:10 AM); Email from Staff of Office of the Dir., Financial Crimes Enforcement Network, to Staff of H. Comm. on the Judiciary and H. Comm. on Financial Services (May 29, 2024 10:47 AM).

¹⁰³ Transcribed Interview of Mr. Jimmy Kirby at 72, 80 (July 18, 2024).

¹⁰⁴ *Id.* at 72, 81-82.

¹⁰⁵ Email from BSAAG to BSAAG and personnel at MUFJ and Golden 1 (Feb. 5, 2024, 8:42 AM) (SCHWAB_HJC_00002945).

¹⁰⁶ Email from BSAAG to BSAAG and personnel at MUFJ and Golden 1 (Feb. 5, 2024, 8:42 AM) (SCHWAB_HJC_00002945).

¹⁰⁷ *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002947).

¹⁰⁸ *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002947-2948, 2952).

that offer “solutions in which BSA data, including Suspicious Activity Report (SAR) data, is stored on the business relationship partner’s platform.”¹⁰⁹ However, these practices may be violating the BSA.

As the white paper acknowledged, “Federal Functional Regulators (FFRs) and FinCEN have not issued comprehensive rules or guidance relating to sharing BSA data with third parties” and that “it is not entirely clear to what extent [a financial institution] may use [a third party’s] contract resources to perform these functions consistent with SAR confidentiality rules and guidance.”¹¹⁰ The white paper observed the tension between keeping BSA data confidential and sharing the same information with third-party contractors:

The sharing of BSA data with third parties carries elevated risks, beyond data privacy and security risks related to all third-party relationships. Most BSA data, by definition, is highly confidential and sensitive . . . An FI subject to BSA regulation can run afoul of the law and prudent practice by over delegating BSA-related functions to a business-relationship partner or agent without sufficient supervision, training, and oversight.¹¹¹

Despite the legal uncertainty, security risks, and privacy concerns that sharing BSA data with third-party vendors presents for Americans’ private financial data, financial institutions appear to continue doing so with the tacit approval of the federal government.

iv. FinCEN appeared to have provided an individual with unauthorized access to a financial information-sharing system.

Section 314(b) of the USA Patriot Act “permits financial institutions, upon providing notice to the United States Department of Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.”¹¹² As of 2020, the 314(b) program included over 7,000 financial institutions.¹¹³ In 2020, 17,384 SAR narratives, which consist of a summary of the suspicious activity, referenced use of the 314(b) program, indicating that financial institutions actively collaborated to share information concerning potentially suspicious activity.¹¹⁴ The 314(b)

¹⁰⁹ *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002947).

¹¹⁰ *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002950-2952).

¹¹¹ *Sharing BSA Data with Third Parties: Guidance and Recommendations*, BSAAG Information Security and Confidentiality Subcommittee, Draft Paper (Aug. 25, 2023) (SCHWAB_HJC_00002959).

¹¹² U.S. DEP’T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, SECTION 314(B).

¹¹³ U.S. DEP’T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, INFORMATION SHARING INSIGHTS: 314(B) PARTICIPATION AND REPORTING.

¹¹⁴ U.S. DEP’T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, INFORMATION SHARING INSIGHTS: 314(B) PARTICIPATION AND REPORTING; *see also* FIN. CRIMES ENFORCEMENT NETWORK, GUIDANCE ON PREPARING A COMPLETE & SUFFICIENT SUSPICIOUS ACTIVITY REPORT NARRATIVE (explaining SAR narratives).

program requires participating financial institutions to “protect the security and confidentiality of all information . . . and only use such information for the purposes laid out” in the statute.¹¹⁵

According to nonpublic documents, it appears that in at least one instance, an individual with “no connection” to a financial institution was mistakenly able to register with FinCEN as the bank’s program representative and received access to the sensitive data of customers’ and their transactions in this program.¹¹⁶ On May 5, 2021, a BoA employee emailed the former Director of the Office of Stakeholder Integration and Engagement at FinCEN explaining that there was “a 314(b) registration issue” involving BoA.¹¹⁷ He wrote:

I have a 314(b) registration issue that I want to discuss with someone of appropriate seniority within FinCEN to make sure you are aware. It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America’s 314(b) contact. I’d be happy to pull up with you to share what we know or if you want to direct me somewhere else that would be fine too.¹¹⁸

The fact that an unauthorized representative appeared to have gained access to FinCEN’s 314(b) program raises the question of whether FinCEN is adequately protecting the sensitive financial data under its control and properly screening and vetting all individuals with access to this information. After BoA flagged the issue, the FinCEN employee agreed that the unauthorized access was “troubling” and would “escalate this immediately.”¹¹⁹

¹¹⁵ U.S. DEP’T OF TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, SECTION 314(B) FACT SHEET (Dec. 2020) (citing 31 CFR 1010.540(b)(4)(i)-(ii)).

¹¹⁶ Email from personnel at Bank of America to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN (May 5, 2021, 1:09 PM) (424HJUD00006301).

¹¹⁷ Email from personnel at Bank of America to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN (May 5, 2021, 1:09 PM) (424HJUD00006301).

¹¹⁸ Email from personnel at Bank of America to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN (May 5, 2021, 1:09 PM) (424HJUD00006301).

¹¹⁹ Email from the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, to personnel at Bank of America (May 5, 2021, 5:30 PM) (424HJUD00006301).

From: [REDACTED]@fincen.gov]
 Sent: 5/5/2021 5:30:59 PM
 To: [REDACTED]@bofa.com]
 Subject: RE: 314(b) related escalation

[REDACTED] that's obviously troubling. I will escalate this immediately and revert once we have a path for further discussion.

Regards,
 [REDACTED]

[REDACTED]
 Director, Office of Stakeholder Integration and Engagement
 Strategic Operations Division
 Financial Crimes Enforcement Network (FinCEN)
 U.S. Department of the Treasury
 [REDACTED] (mobile)

From: [REDACTED]@bofa.com>
 Sent: Wednesday, May 5, 2021 1:09 PM
 To: [REDACTED]@fincen.gov>
 Subject: [EXTERNAL] 314(b) related escalation

[REDACTED] – I have a 314(b) registration issue that I want to discuss with someone of appropriate seniority within FinCEN to make sure you are aware. It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America's 314(b) contact. I'd be happy to pull up with you to share what we know or if you want to direct me somewhere else that would be fine too.

Thanks,
 [REDACTED]

“It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America’s 314(b) contact.”
 —May 5, 2021, email from Bank of America personnel to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN

Given the amount of information that can be gleaned by viewing financial data, a bad actor who gains access to the 314(b) program could use it to view, target, or disclose Americans' sensitive information. It is concerning to learn that FinCEN could mistakenly register someone with no affiliation to the bank as their representative for the 314(b) program and seemingly gain unauthorized access to the data.

* * *


The threat of potential financial surveillance is expanding. Financial institutions are filing an ever-increasing number of confidential BSA reports like SARs and CTRs on Americans and, at the same time, the federal government is providing tens of thousands of federal, state, and local officials with warrantless access to this information and using it in undisclosed ways. As a

consequence, more people than ever before have access to Americans' sensitive financial information.


**FEDERAL LAW ENFORCEMENT AND ITS PARTNERS ABUSE THE BSA'S INFORMATION-SHARING
REGIME**

The FBI treats the SARs filed by financial institutions as a valuable resource. The FBI has told at least one financial institution that it “data min[es]” SARs as part of its investigations and that “all cases are required to search FinCEN data including SARs/CTRs.”¹²⁰ The FBI even asked financial institutions to include “as much . . . biographical info in SARs as possible: email address, phones, IP addresses, App data (cookies / push tokens, etc.) **EVEN OLD DATA!**”¹²¹ It also directed financial institutions to “[p]ut as many key words in the SAR write-up as possible.”¹²²

UNCLASSIFIED//FOUO



Info for BSA / AML Teams



- SARS ARE SO IMPORTANT TO LAW ENFORCEMENT!
 - Today, tomorrow, next year...in 10 Years
 - Data mining by FBI
 - All cases are required to search FinCEN data including SARs/CTRs
- What can financial institutions do to help Law Enforcement?
 - Include as much IT biographical info in SARs as possible: email address, phones, IP addresses, App data (cookies / push tokens, etc.) **EVEN OLD DATA!**
 - Include location info for branches and activity (can help with venue)
 - Back up docs are great; continual/reoccurring SARs for updates
 - Put as many key words in the SAR write-up as possible. Think “What words would LE data mine that would hit on this SAR.”
- Why can't Agents tell bank investigators more? If you did, we could help you more...
 - Classification issues
 - Careful Agents
- Shift from NSLs to Other Legal process: Subpoenas and 2703d Court Orders
 - Legal requirement for organizations to comply (IT company issues)
 - Need a Non-Disclosure Court Order anyways (IT company issues)
 - Unclassified use

(side comment—IT companies are typically VERY responsive and helpful with Emergency Disclosures)
- **We use the data—and thank you for your help! (and Law Enforcement STINKS at telling investigators this!)**

UNCLASSIFIED//FOUO

“What words would [Law Enforcement] data mine that would hit on this SAR.”
—FBI Charlotte Division Joint Terrorism Task Force Slideshow

¹²⁰ *International Terrorism*, FBI Charlotte Division Joint Terrorism Task Force (424HJUD00004507).

¹²¹ *Id.* (emphasis in original).

¹²² *Id.*

In his transcribed interview with the Committee and Select Subcommittee, the former Director of the Office of Stakeholder Integration and Engagement at FinCEN acknowledged that the SAR process sweeps in much more information than just suspicious activity.¹²³ He testified:

So, again, it's instead of looking for that needle in a haystack in millions of transactions, it's let's take a narrow subset that fits certain characteristics and look at those to evaluate whether they are suspicious. . . . Are we going to be overly inclusive in looking at things that we decide are not suspicious? Absolutely. But it makes it manageable.¹²⁴

The issue with FinCEN's "overly inclusive" approach, however, is that it subjects innocent Americans and their highly sensitive information to potential FBI scrutiny or other law enforcement investigations. The customer's information is never deleted and the customer never learns whether a financial institution has filed a SAR on them.¹²⁵

A. Federal law enforcement has broad discretion in what it considers "suspicious" financial activity and urges financial institutions to review their customers' transactions and file reports on the activity they consider "suspicious."

In 2021, Congress codified a new program called the FinCEN Exchange "to facilitate the sharing of information between law enforcement, FinCEN, and financial institutions" to include the sharing of "typologies," "trends," and other information that financial institutions "could consider incorporating into their existing AML/CFT [Anti-Money Laundering / Countering the Financing of Terrorism] programs" in order to "identify indicia of suspicious activity."¹²⁶ FinCEN Deputy Director Kirby described the FinCEN Exchange as "probably our premier public-private partnership, and it's a way for the private sector and different parts of government to come together and share information on priority topics."¹²⁷

Financial institutions review the typologies, trends, and other criteria provided to them through the FinCEN Exchange and subsequently review their own customers' transactions to determine if there is reportable suspicious activity.¹²⁸ This exchange of information creates a feedback loop between the government and financial institutions that, when used appropriately, may help the government and financial institutions detect and deter fentanyl distribution, human trafficking, or terrorist financing.¹²⁹ However, as Peter Sullivan, the former FBI Senior Private

¹²³ Transcribed Interview of the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 141 (May 14, 2024).

¹²⁴ *Id.*

¹²⁵ See Transcribed Interview of Mr. Jimmy Kirby at 78 (July 18, 2024); see also 31 U.S.C. 5318(g)(2) (prohibiting notification that a transaction has been reported).

¹²⁶ Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 3-4 (Feb. 9, 2024).

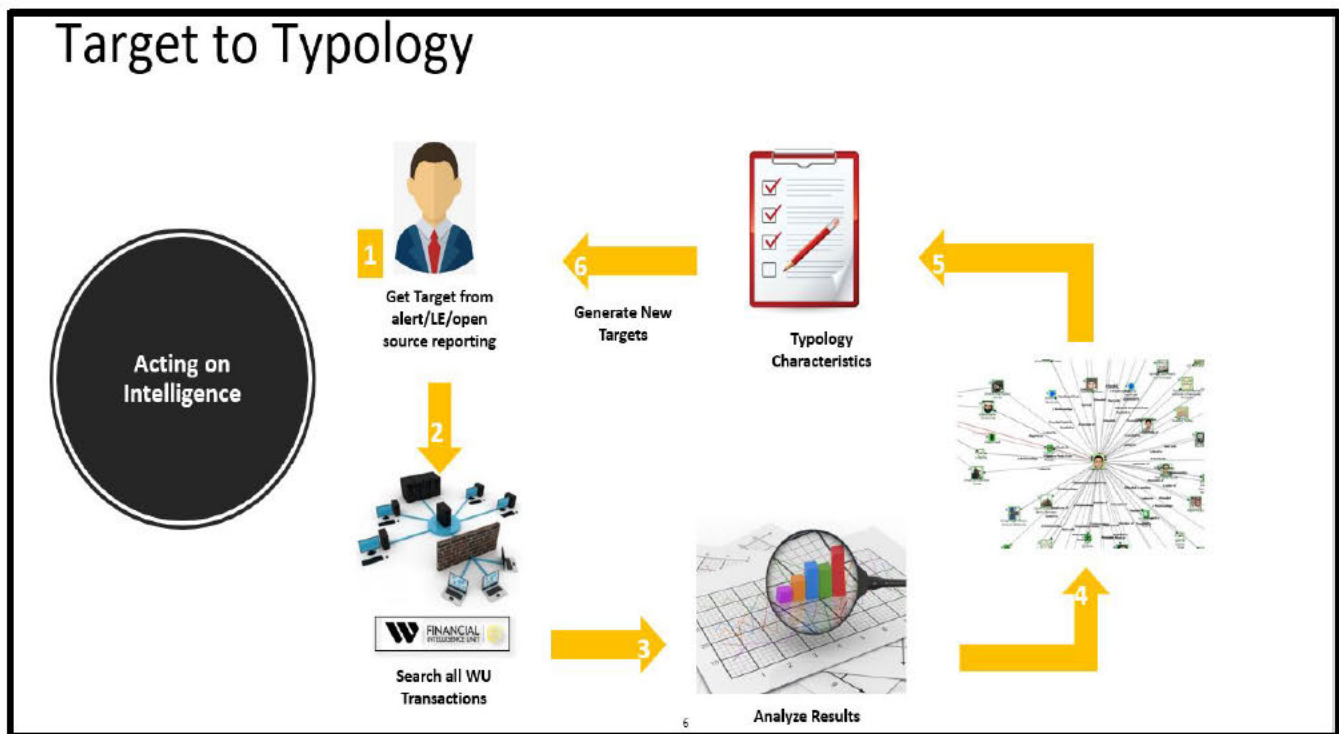
¹²⁷ Transcribed Interview of Mr. Jimmy Kirby at 15-16 (July 18, 2024).

¹²⁸ See Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (quoting 31 U.S.C. § 5318(g)(1)).

¹²⁹ See Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2-3 (Feb. 9, 2024); see also, e.g., Transcribed Interview of Mr. Jimmy Kirby at 16 (July 18, 2024).

Sector Partner for Outreach within the Strategic Partner Engagement Section noted during his transcribed interview, the FBI is not limited in the kind of transactions it can suggest to financial institutions as potentially suspicious. He testified:

- Q. Are there limits in terms of the kind of transactions that you can express an interest as being possibly suspicious?
- A. From my law enforcement standpoint, there [are] various things that we can discuss and brainstorm. So, in that sense, you know, it varies. It's a pretty wide scope.¹³⁰



Slide detailing the feedback loop between the government and financial institutions.
 —March 2024 presentation from Western Union Financial Intelligence Unit.¹³¹

While “it is ultimately a bank’s responsibility to determine when—consistent with the BSA and its implementing regulations—a bank must file a SAR,”¹³² when federal law enforcement and Treasury Department regulators share information with banks for them to “consider incorporating into their existing AML/CFT programs,”¹³³ financial institutions have a massive incentive to act on the intelligence they receive from government officials and

¹³⁰ Transcribed Interview of Mr. Peter Sullivan at 139 (Apr. 9, 2024).

¹³¹ Western Union, Using Strategic Intelligence to Combat Financial Crime at 6 (2023) (PowerPoint presentation) (WesternUnion-0004941.PPTX).

¹³² Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 4 (Feb. 9, 2024) (emphasis added).

¹³³ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 3 (Feb. 9, 2024) (emphasis added).

regulators. If the banks fail to file SARs that they should have, or otherwise fail to comply with the BSA by maintaining effective AML programs, they could incur civil penalties that could total hundreds of millions of dollars.¹³⁴ This is the incentive framework in which financial institutions are forced to operate.

Federal law enforcement has regularly abused the information sharing process in order to deploy financial institutions as *de facto* arms of federal law enforcement. For example, following the events of January 6, 2021, federal law enforcement and FinCEN deputized the entire financial sector to identify anyone who may have been present at the U.S. Capitol.¹³⁵ This collaboration included sharing information and developing typologies that clearly targeted Americans with conservative views—gun owners, those concerned with illegal immigration, and those opposed to COVID mandates, to name a few.¹³⁶ The FBI exploited its relationships with financial institutions by asking them to file SARs based on specific typologies crafted by FinCEN and the FBI to ostensibly identify potential threats to Inauguration Day.¹³⁷ Yet, even after Inauguration Day had concluded and any potential threats to the event had passed, the FBI still sent financial institutions specific names, requesting that they search their database for those individuals and file SARs on any potential suspicious activity.¹³⁸

On January 8, 2021, FinCEN convened a call with Peter Sullivan, representing the FBI’s Counterterrorism Division, and approximately thirty to fifty financial institutions.¹³⁹ On this call and others, “FinCEN asked [the FBI] to discuss different fact-based patterns that would help institutions look at their data, review their data for anything . . . that would help the institutions understand if they had any threats”¹⁴⁰ Following the January 8, 2021, conversation, BoA reached out to Sullivan directly to discuss the FinCEN call.¹⁴¹ On January 15, 2021, Sullivan and BoA representatives “brainstorm[ed]” potential indicators and thresholds that could be used by BoA to file a SAR related to the events at the Capitol on January 6, 2021, and to identify potential threats to Inauguration Day.¹⁴² Sullivan memorialized this call in an email to BoA with

¹³⁴ See, e.g., FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN PENALIZES U.S. BANK OFFICIAL FOR CORPORATE ANTI-MONEY LAUNDERING FAILURES (Mar. 4, 2020) (noting that FinCEN assessed \$450,000 civil penalty against U.S. Bank Official for “failure to prevent violations of the Bank Secrecy Act” and \$185 million civil penalty against U.S. Bank for “willfully violating the BSA’s requirements”).

¹³⁵ See Transcribed Interview of Mr. Peter Sullivan at 66-67 (Apr. 9, 2024); see also Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002) (including thresholds confirming customers transacting in Washington, D.C. or purchasing hotel reservations in Washington, D.C.).

¹³⁶ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS 17 (Comm. Print 2024).

¹³⁷ See Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002); see also Transcribed Interview of Mr. Peter Sullivan at 29 (Apr. 9, 2024) (Sullivan testified that the FBI shared “fact-based patterns” with financial institutions to “help the institutions understand if they had any threats that may help cover down on the threat to Inauguration Day”).

¹³⁸ See, e.g., Email from Peter Sullivan, FBI, to FBI employee and Bcc’d recipient [Redacted] at Santander (Jan. 15, 2021, 3:25 PM) (SBNA_HJC_0001084); Email from Peter Sullivan, FBI, to FBI employee and bcc’d financial institutions (Jan. 15, 2021, 10:25 AM) (SCB-00002713).

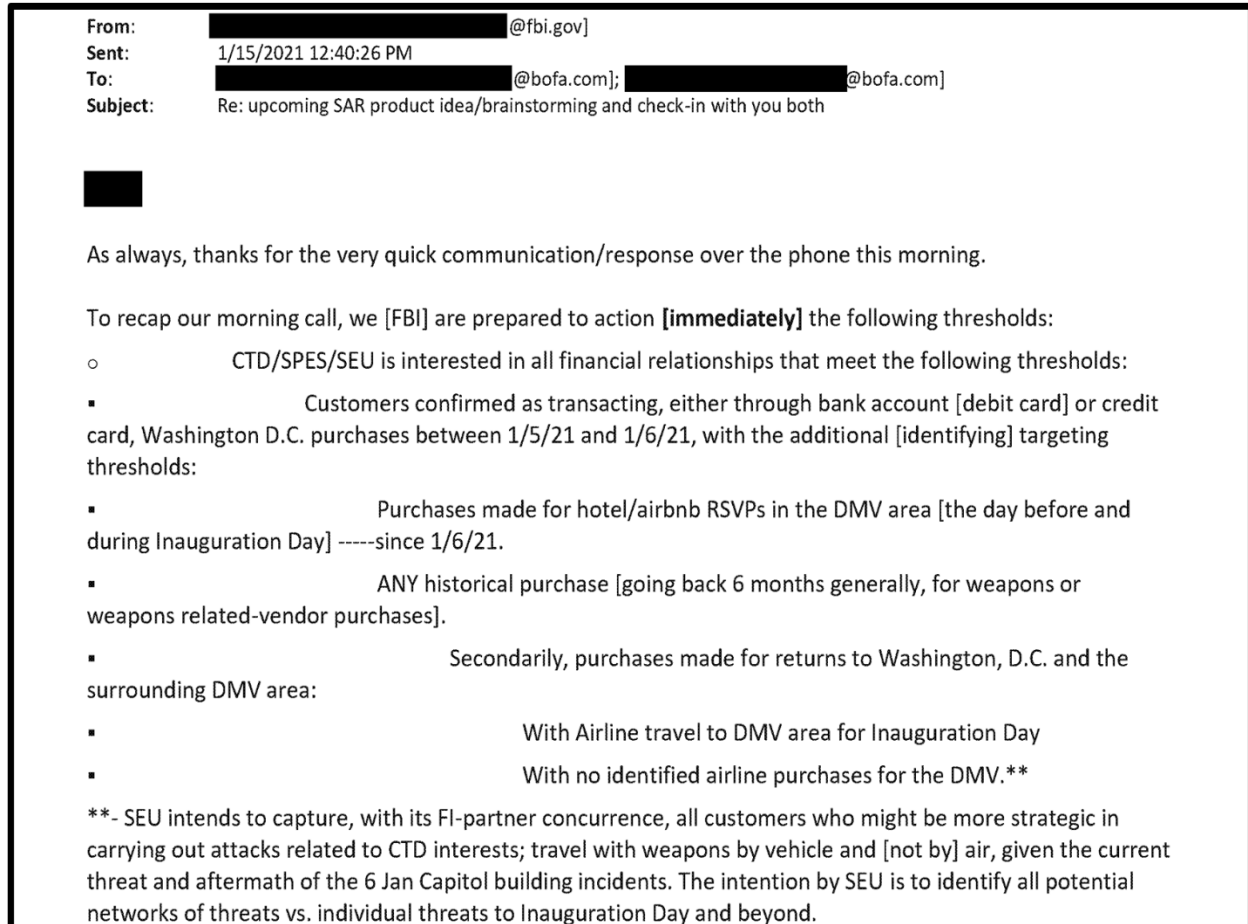
¹³⁹ Transcribed Interview of Mr. Peter Sullivan at 27, 29, 80, 92 (Apr. 9, 2024) (noting that the FinCEN call occurred on January 8, 2021).

¹⁴⁰ *Id.* at 29.

¹⁴¹ *Id.* at 28.

¹⁴² *Id.* at 28-30.

a list of thresholds the FBI was “prepared to action.”¹⁴³ According to these thresholds, the FBI sought information on any BoA customer who transacted in the Washington, D.C., area and who made “ANY historical purchase” of a firearm or who had made a hotel, Airbnb, or airline reservation within a given date range in January 2021.¹⁴⁴



*“[W]e [FBI] are prepared to action **[immediately]** the following thresholds . . . Washington D.C. purchases between 1/5/21 and 1/6/21 . . . [p]urchases made for hotel/Airbnb RSVPs in the DMV area . . . ANY historical purchase [going back 6 months generally, for weapons or weapons related-vendor purchases]”*

—Jan. 15, 2021, email from FBI personnel to Bank of America personnel

Ultimately, according to Sullivan, BoA filed a SAR based on these FBI-provided thresholds. Sullivan testified:

Q. And did Bank of America’s production of the SAR and information that was in the SAR, did it correlate with these thresholds?

¹⁴³ Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BoFA-HJUD-00000002).

¹⁴⁴ *Id.*

A. It did.

* * *

Q. Do you recall how many individuals then were identified in that SAR?

A. My recollection is that there were 211 individuals that met the three thresholds that you can see within the email.¹⁴⁵

Sullivan’s interactions, however, were not limited to only BoA. He testified that, “my engagement was not just with Bank of America. My engagement was with all [of the] finance sector. And so that covered banks, fintech, it covered neobanks, cryptocurrency, I mean, you name it.”¹⁴⁶ Sullivan stated that “a handful” of those financial institutions, like BoA, filed SARs based on thresholds developed by the FBI and FinCEN and that, at times, he even received SARs that were “handpicked” for him directly by executives at financial institutions.¹⁴⁷ He testified:

Q. Do you know, approximately, how many other banks . . . did, in fact, send you information complying with those three criteria like Bank of America did[?]

A. Yeah, there were between 40 and 60 representatives on the first FinCEN [call], which probably spanned 30 to 50 financial institutions. So I received a lot of SARs related to the Capitol riots and the unknown threat to Inauguration Day.¹⁴⁸

Following the January 8 phone call between FinCEN, the FBI, and financial institutions, FinCEN “created a tag for all SARs related to the Capitol riots”¹⁴⁹ and financial institutions swiftly complied with FinCEN’s and the FBI’s requests, directing their employees to expedite SARs related to the events of January 6, 2021.¹⁵⁰ In an email from a Citigroup Senior Vice President, employees received direction that “for any SAR filings related to the Capitol Riots, the following reference should be included in SAR Field 2 (Filing Institution Note to FinCEN) and in the narrative of the SAR: ‘**FIN-2021-DE01.**’”¹⁵¹ It further directed, “[a]s a reminder, all SARs related to the Capitol Riots should be **expedited.**”¹⁵²

¹⁴⁵ Transcribed Interview of Mr. Peter Sullivan at 34 (Apr. 9, 2024).

¹⁴⁶ *Id.* at 31-32.

¹⁴⁷ *Id.* at 22, 80.

¹⁴⁸ *Id.* at 80.

¹⁴⁹ *Id.* at 77-78.

¹⁵⁰ *Id.* at 91; *see also* Email from personnel at Citigroup to personnel at Citigroup (Jan. 15, 2021, 4:10 PM) (HJCSWFG_0000648).

¹⁵¹ Email from personnel at Citigroup to personnel at Citigroup (Jan. 15, 2021, 4:10 PM) (HJCSWFG_0000648) (emphasis in original).

¹⁵² *Id.* (emphasis in original).

Despite stating that the SAR filing process was voluntary, Sullivan could not recall a single financial institution that declined to produce a SAR after the FBI sent the thresholds for banks to use in compiling SARs. Sullivan testified:

Q. [I]s it voluntary for Bank of America to file a SAR after discussing the very thresholds that were subsequently filed by Bank of America with you?

A. Under BSA, it would be up to the bank exclusively whether or not they met [the] SAR thresholds[.]

Q. Anyone not respond? . . . Any financial institutions you sent similar requests to, like you did [with] Bank of America, and Bank of America sent you back information, including documentation that included 211 American customer names, any other financial institutions you sent similar stuff to, did they not respond?

* * *

A. I can't recall any financial institution that didn't produce SARs during that time.¹⁵³

While the FBI frequently claims that financial institutions voluntarily produce SARs, this information raises questions about whether financial institutions truly have a choice to file SARs when the FBI solicits them.

Ultimately, the FBI's focus shifted from sending thresholds and typologies to financial institutions to soliciting information on specific individuals potentially under investigation.¹⁵⁴ On January 15, 2021, Sullivan sent an email to various financial institutions with the subject line "[a]dditional names/selectors for SAR purposes only at your [financial institution's] discretion."¹⁵⁵ The email included names and other selectors "linked to the 6 Jan Capitol building incidents . . . for SARs purposes only."¹⁵⁶ In other words, Sullivan, on behalf of the FBI, provided a list of Americans to financial institutions suggesting that the companies search their databases to find additional information and potentially file SARs on those individuals.

¹⁵³ Transcribed Interview of Mr. Peter Sullivan at 90-91 (Apr. 9, 2024).

¹⁵⁴ See, e.g., Email exchange between Peter Sullivan at FBI, FBI employee, personnel at Union Bank and MUFG (Apr. 16, 2021) (MUFG-0000075-76).

¹⁵⁵ Email from Peter Sullivan, FBI, to FBI employee and bcc'd recipient [Redacted] at Santander (Jan. 15, 2021, 3:25 PM) (SBNA_HJC_0001084); see also Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (Jan. 15, 2021, 10:25 AM) (SCB-00002713-2714) (similarly providing names and selectors).

¹⁵⁶ Email from Peter Sullivan, FBI, to FBI employee and bcc'd recipient [Redacted] at Santander (Jan. 15, 2021, 3:25 PM) (SBNA_HJC_0001084).

#External Sender# Additional names/selectors for SAR purposes only at your FI's discretion

From: [REDACTED] (CTD) (FBI)" [REDACTED]@fbi.gov>
 To: [REDACTED] (CTD) (FBI)" [REDACTED]@fbi.gov>
 Bcc: [REDACTED]@santander.us>
 Date: Fri, 15 Jan 2021 15:25:25 +0000
 Attachments: List of names and selectors for SAR purposes only.docx (25.37 kB)

Folks,

SEU has been working hard over the last week to get you additional names/selectors linked to the 6 January Capitol incident and the current threat environment leading up to Inauguration Day.

Please see the attached list of names/selectors linked to the 6 Jan Capitol building incidents and review at the discretion of your own investigation/compliance teams---for SARs purposes only.

If you chose to publish a SAR, SEU will be interested to review and disseminate to the appropriate FBI operations personnel immediately.

To be clear, none of the names on this list are part of our SEU's code Yellow/Red/Equity Check outreach tool. But this list is being provided as a collective effort by SEU to help your investigations/compliance teams in your normal course of value-added SAR production.

SEU requests that nothing in the attached be considered a higher priority than SEU's current [pending and future] outreach code YELLOWS/REDS/Equity Checks.

[REDACTED]
 Senior Private Sector Partner Outreach
 Strategic Partner Engagement Section
 [REDACTED]

“SEU has been working hard over the last week to get you additional names/selectors . . . this list is being provided as a collective effort by SEU to help your investigations/compliance teams in your normal course of value-added SAR production.”

—Jan. 15, 2021, email from Peter Sullivan, FBI, to FBI employee, and bcc'd financial institutions

However, despite Sullivan's assurance to financial institutions that his information sharing was a part of the “normal course of value-added SAR production,”¹⁵⁷ the FBI's provision of specific names and selectors was a manipulation of the SAR-filing process, which “requires that a bank or other financial institution file a SAR whenever it identifies ‘a suspicious transaction relevant to a possible violation of law or regulation.’”¹⁵⁸ Indeed, as Deputy Director Kirby testified in his transcribed interview, “[W]ith a suspicious activity report it's the bank who's investigating or monitoring their customers and then flagging for FinCEN and law enforcement what they deem to be suspicious.”¹⁵⁹ By sending specific names to financial institutions and requesting any SARs related to those individuals, however, the FBI is turning the SAR process on its head, suggesting for the banks that certain people could be suspicious and impliedly urging financial institutions to examine them more closely.

¹⁵⁷ *Id.*

¹⁵⁸ Letter from Corey Tellez, Acting Assistant Sec'y, Office of Legislative Affairs, U.S. Dep't of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 2 (Feb. 9, 2024) (emphasis added).

¹⁵⁹ Transcribed Interview of Mr. Jimmy Kirby at 98-99 (July 18, 2024).

In a similar exchange months later, on April 16, 2021, Sullivan shared with various financial institutions a “name and selectors . . . for your discretionary SAR purposes only.”¹⁶⁰ In response, an MUFG employee asked “[d]oes this mean you are not looking for a response from us except to notify you if we happen to file something based on this?”¹⁶¹ Sullivan replied that the FBI “will take any SARs you decide to file on.”¹⁶² In his transcribed interview, Sullivan explained that he received, on behalf of the FBI, “a hundred SARs” each year that are “handpicked” directly “from an executive at a financial institution.”¹⁶³

From: Sullivan, Peter (CTD) (FBI) [mailto: [REDACTED]@fbi.gov]
Sent: Friday, April 16, 2021 5:19 PM
To: [REDACTED] (CTD) (FBI)
Subject: [External: [REDACTED]] - selectors provided for SAR purposes only

***** External email: Please be careful when opening attachments or clicking links. *****

Folks,

The name and selectors linked to the [REDACTED] are being provided to you below for your discretionary SAR purposes only.

At this time, this is NOT being treated as a Code RED.

-Pete

Name: [REDACTED]
DOB: [REDACTED]
SS#: [REDACTED]
Address: [REDACTED]
Driver's License: [REDACTED]

“[S]electors . . . are being provided to you below for your discretionary SAR purposes only . . . this is NOT being treated as a Code RED.”

—Email from Peter Sullivan, FBI, to bcc'd financial institutions

¹⁶⁰ Email from Peter Sullivan, FBI, to FBI employee and bcc'd financial institutions (Apr. 16, 2021, 5:19 PM) (MUFG-0000075-76).

¹⁶¹ Email from personnel at MUFG to Peter Sullivan, FBI, FBI employee, and personnel at Union Bank (Apr. 16, 2021 5:46 PM) (MUFG-0000075-76).

¹⁶² Email from Peter Sullivan, FBI, to personnel at MUFG, Union Bank, and FBI employee (Apr. 16, 2021, 9:55 PM) (MUFG-0000075).

¹⁶³ See Transcribed Interview of Mr. Peter Sullivan at 21-22 (Apr. 9, 2024).

Message

From: [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov
Sent: 4/16/2021 9:55:51 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7 [REDACTED]; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov
CC: [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]unionbank.com]; [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]unionbank.com]; [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]unionbank.com]
Subject: [External] RE: [REDACTED] selectors provided for SAR purposes only

*** External email: Please be careful when opening attachments or clicking links. ***

[REDACTED]

This may turn into a code red, but in the interim we wanted to push you selectors we confirmed on the ops side. So yes, for now, we have not confirmed we have GJS' teed up for all results from our normal "code red" protocol --but we will take any SARs you decide to file on.

If this turns into a code red over the weekend, you will hear it from me first.

Hope this helps.

Hope you all have a safe weekend with your families.

[REDACTED]

From: [REDACTED]@us.mufg.jp>
Sent: Friday, April 16, 2021 5:46 PM
To: [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov>
Cc: [REDACTED]@unionbank.com>; [REDACTED]@unionbank.com>; [REDACTED]@unionbank.com>
Subject: [EXTERNAL EMAIL] - RE: [REDACTED] - selectors provided for SAR purposes only

Hi [REDACTED], happy Friday. Does this mean you are not looking for a response from us except to notify you if we happen to file something based on this?

From: [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov
Sent: Friday, April 16, 2021 5:19 PM
To: [REDACTED] (CTD) (FBI)
Subject: [External] [REDACTED] - selectors provided for SAR purposes only

*** External email: Please be careful when opening attachments or clicking links. ***

Folks,

"We will take any SARs you decide to file on."

—Apr. 16, 2021, Email from Peter Sullivan, FBI, to Union Bank personnel

In at least two instances, one financial institution replied to Sullivan’s emails and sought legal process from the FBI before it would turnover more detailed financial records. Sullivan pushed back on those requests. On April 20, 2021, Sullivan sent an email to Standard Chartered employees, requesting information on various names “in response to a **CODE YELLOW**.”¹⁶⁴ Standard Chartered responded to Sullivan and informed him that its search registered a “positive hit” but stated that “[i]f additional information is required, we ask that you send a subpoena.”¹⁶⁵ Sullivan responded, asking for a phone call, explaining that “typically for Code Reds and Yellows, we get more on the front end than ‘positive’ only” and affirmed that “because this outreach name on [redacted] was a code yellow, we’d like to get something additional.”¹⁶⁶ He contrasted this request with “Equity Checks” that require a response of “‘positive’ only with no other info offered because Equity Checks are priority investigations but have no . . . emergency-related nexus.”¹⁶⁷

In a similar exchange, on May 24, 2021, Sullivan requested that Standard Chartered “run the following name and associated selectors in response to an Equity Check.”¹⁶⁸ Standard Chartered responded, acknowledging that it had identified transactions “with an exact name match,” but again asked for legal process, writing, “If additional information is required, we ask that you send a subpoena.”¹⁶⁹ Two days later, on May 26, 2021, Sullivan replied to Standard Chartered asking, “I wanted to revisit our conversation on your two cents if we could discuss next steps to try to get more information on name matches”¹⁷⁰ Sullivan and the Standard Chartered employee scheduled a call for the next day.¹⁷¹ Sullivan also sought a “pre-call” with the Standard Chartered employee to see if the bank planned to have “compliance or someone else on the call” so that Sullivan could “make sure at a minimum” that he was on “the same page” as the Standard Chartered employee regarding these requests.¹⁷² This apparent effort to avoid any legal process to obtain the sensitive information of a bank’s customer is concerning, but does not appear uncommon.

The FBI clearly recognizes the usefulness of Americans’ financial data and frequently contacts financial institutions to request information for the FBI’s investigations. While avoiding making outright demands for this information, documents show that the FBI avoids requests for legal process and routinely operates on the edge of what is permissible information sharing under

¹⁶⁴ Email from Peter Sullivan, FBI, to FBI employee and bcc’d financial institutions (Apr. 19, 2021, 5:43 PM) (SCB-00002923) (emphasis in original).

¹⁶⁵ Email from personnel at Standard Chartered Bank to Peter Sullivan at FBI, FBI employee, and personnel at Standard Chartered Bank (Apr. 20, 2021, 2:52 PM) (SCB-00002923).

¹⁶⁶ Email from Peter Sullivan, FBI, to personnel at Standard Chartered Bank and FBI employee (Apr. 20, 2021, 4:46 PM) (SCB-00002922).

¹⁶⁷ *Id.*

¹⁶⁸ Email from Peter Sullivan, FBI, to FBI employee and bcc’d financial institutions (May 24, 2021, 11:58 AM) (SCB-00003013).

¹⁶⁹ Email from personnel at Standard Chartered Bank to Peter Sullivan, FBI, FBI employee, and personnel at Standard Chartered Bank (May 24, 2021, 4:04 PM) (SCB-00003012).

¹⁷⁰ Email exchange between Peter Sullivan, FBI, to personnel at Standard Chartered Bank (May 26, 2021) (SCB-00003012).

¹⁷¹ Email from personnel at Standard Chartered Bank to Peter Sullivan, FBI (May 26, 2021, 3:40 PM) (SCB-00003018).

¹⁷² Email from Peter Sullivan, FBI, to personnel at Standard Chartered Bank (May 26, 2021, 8:19 PM) (SCB-00003018).

the BSA. By soliciting financial institutions for SAR filings directly, the FBI is treating financial institutions as arms of law enforcement charged with investigating whether a customer has engaged in any “suspicious activity” on the FBI’s behalf.

B. FinCEN solicits customer transaction information from financial institutions, on behalf of the FBI, even if the transaction activity lacks a clear nexus to criminal activity.

FinCEN also serves as an active partner of the FBI by collecting Americans’ financial data on its behalf. During his transcribed interview, the former Director of the Office of Stakeholder Integration and Engagement in the Strategic Operations Division at FinCEN, stated that “if the FBI said, hey, we’re desperate; you know, something major is happening . . . we need you to jump, we would jump.”¹⁷³ This closeness played out following January 6, 2021, when FinCEN coordinated with the FBI to share hordes of information with financial institutions to assist in the FBI’s investigation. The Committee and Select Subcommittee’s investigation has revealed that FinCEN provided financial institutions with politicized search terms and typologies that cast certain ideologies, namely conservatives, as potentially dangerous or extreme.¹⁷⁴ New documents reveal that, as it sought to assist the FBI in its January 6-related investigations, FinCEN cast such a wide net that it inevitably caused financial institutions to flag ordinary Americans’ transactions as suspicious.

One example that demonstrates the problem with casting such a wide net, is a list that FinCEN circulated to financial institutions that included hundreds of shops and vendors that any traveler would have made at D.C.-area airports, train stations, and bus stops, including purchases from major nationwide food and retail chains.¹⁷⁵ On January 22, 2021, after the presidential inauguration, an employee from MUFUG sent FinCEN an email with an excel sheet that included “a compilation of vendors at the 3 major DMV airports (Reagan, Dulles, BWI), Union Station (rail), and Bus Stops.”¹⁷⁶ A FinCEN employee responded to MUFUG, saying, “this is terrific. Thank you both.”¹⁷⁷

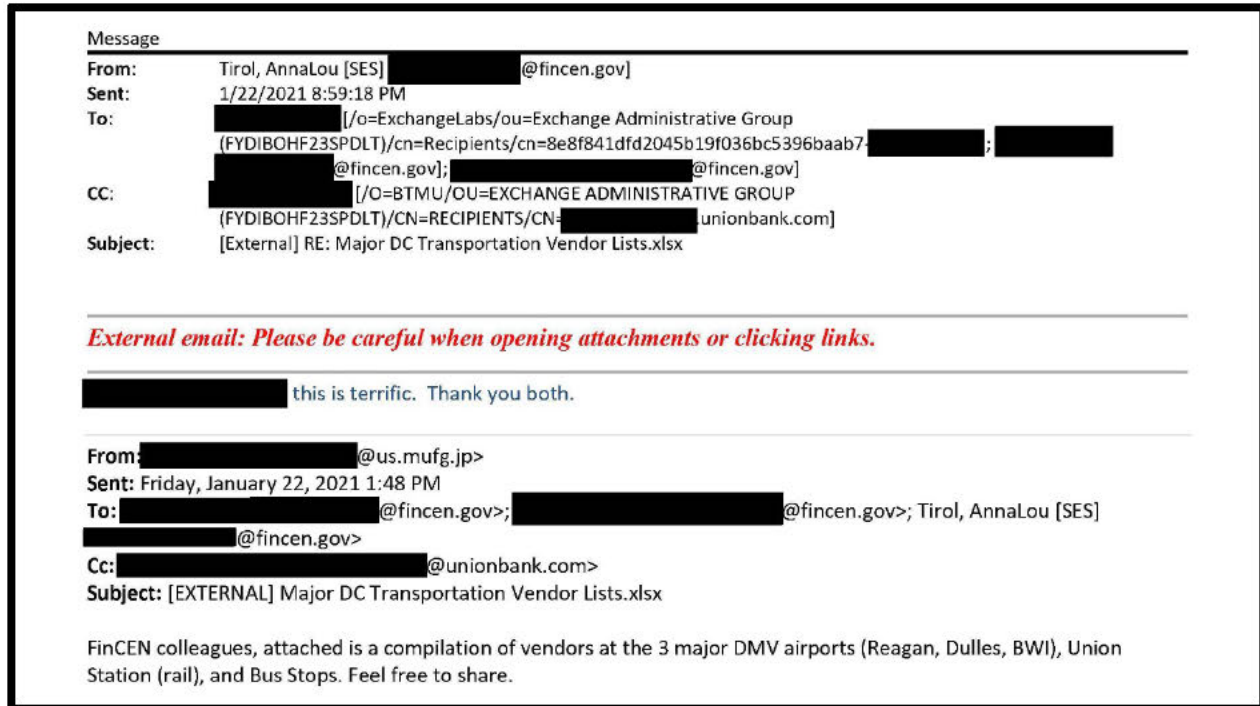
¹⁷³ Transcribed Interview of the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 21-22 (May 14, 2024).

¹⁷⁴ See STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS 21-22 (Comm. Print 2024).

¹⁷⁵ List of airport and bus stop vendors in the Washington, D.C. area (MUFUG-0000417.XLSX).

¹⁷⁶ Email from personnel at MUFUG to the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, FinCEN employee, and AnnaLou Tirol, FinCEN, and personnel at Union Bank (Jan. 22, 2021 1:48 PM) (MUFUG-0000806).

¹⁷⁷ Email from AnnaLou Tirol, FinCEN, to personnel at MUFUG, the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, FinCEN employee, and personnel at Union Bank (Jan. 22, 2021 8:59 PM) (MUFUG-0000806).



“[A]ttached is a compilation of vendors at the 3 major DMV airports (Reagan, Dulles, BWI), Union Station (rail), and Bus Stops. Feel free to share.”
 —Email from MUFG personnel to FinCEN personnel

FinCEN shared this compilation of vendors with financial institutions.¹⁷⁸

¹⁷⁸ Email from the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, to personnel at KeyBank, Western Union, HSBC, Bank of America, Santander, Wells Fargo, MUFG, Union Bank, MUFG, Standard Chartered Bank, Citibank, PayPal, JPMorgan Chase, and AnnaLou Tirol at FinCEN, and FinCEN personnel (Jan. 22, 2021 4:03 PM) (WesternUnion-0000646).

From: [REDACTED]
Sent: Friday, January 22, 2021 4:03 PM
To: [REDACTED]@keybank.com'; [REDACTED]@westernunion.com';
[REDACTED]@westernunion.com>; [REDACTED]@westernunion.com'; [REDACTED]@westernunion.com>;
[REDACTED]@westernunion.com'; [REDACTED]@westernunion.com>; [REDACTED]@us.hsbc.com'
[REDACTED]@us.hsbc.com>; [REDACTED]@us.hsbc.com'; [REDACTED]@us.hsbc.com>;
[REDACTED]@bofa.com'; [REDACTED]@bofa.com>; [REDACTED]@bofa.com'
[REDACTED]@bofa.com>; [REDACTED]@bofa.com'; [REDACTED]@bofa.com>; [REDACTED]@santander.us'
[REDACTED]@santander.us>; [REDACTED]@santander.us'; [REDACTED]@santander.us>; [REDACTED]@santander.us'
[REDACTED]@santander.us>; [REDACTED]@wellsfargo.com'; [REDACTED]@wellsfargo.com>;
[REDACTED]@wellsfargo.com'; [REDACTED]@wellsfargo.com>; [REDACTED]@wellsfargo.com>;
[REDACTED]@wellsfargo.com>; [REDACTED]@us.mufg.jp'; [REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'; [REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@unionbank.com'; [REDACTED]@unionbank.com>;
[REDACTED]@unionbank.com'; [REDACTED]@unionbank.com>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'; [REDACTED]@us.mufg.jp>; [REDACTED]@sc.com'
[REDACTED]@sc.com>; [REDACTED]@sc.com'; [REDACTED]@sc.com>; [REDACTED]@sc.com'
[REDACTED]@sc.com>; [REDACTED]@citi.com'; [REDACTED]@citi.com>; [REDACTED]@citi.com'
[REDACTED]@citi.com>; [REDACTED]@citi.com'; [REDACTED]@citi.com>; [REDACTED]@paypal.com'
[REDACTED]@paypal.com>; [REDACTED]@paypal.com'; [REDACTED]@paypal.com>; [REDACTED]@paypal.com'
[REDACTED]@paypal.com>; [REDACTED]@jpmorgan.com'; [REDACTED]@jpmorgan.com>;
[REDACTED]@jpmorgan.com'; [REDACTED]@jpmorgan.com>;
Cc: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov>; [REDACTED]@fincen.gov>; [REDACTED]
[REDACTED]@fincen.gov>; [REDACTED]@fincen.gov>
Subject: RE: Capitol Riots

All,
With thanks to our MUFG colleagues, please find attached a compilation of vendors at the three major DMV-area airports, Union Station, and various bus stops.
Regards,

“With thanks to our MUFG colleagues, please find attached a compilation of vendors at the three major DMV-area airports, Union Station, and various bus stops.”

—Jan. 22, 2021, Email from the former Director of the Office of Stakeholder Integration and Engagement, FinCEN, to financial institutions and FinCEN personnel

In his transcribed interview, the former Director of the Office of Stakeholder Integration and Engagement stated that FinCEN shares typologies or red flags with financial institutions to provide guidance for their AML/CFT programs.¹⁷⁹ Therefore, by sharing a compilation of vendors at the major Washington, D.C. area transit facilities, it appears that FinCEN expected banks to use the list to identify people or transactions made at those vendors that may be suspicious and merit a SAR filing. This dragnet, suspicious treatment of purchases at vendors around the DMV area, coincided with the FBI soliciting BoA to search its database for any individuals seeking to travel to the Washington, D.C. area around January 6, 2021, and January 20, 2021, and FinCEN’s distribution of a PowerPoint slideshow explaining how financial institutions could search through Americans’ transactions using MCC codes and other keywords

¹⁷⁹ Transcribed Interview of former Director of the Office of Stakeholder Integration and Engagement, FinCEN, at 50 (May 14, 2024).

like “Bass Pro Shop” and “Dick’s Sporting Goods” to scrutinize their purchases.¹⁸⁰ These kinds of sprawling requests have an extremely limited nexus, if any, to individualized criminal conduct. Despite the lack of a criminal nexus, the Treasury Department acknowledged in a letter to the Committee that FinCEN was sharing this kind of information with financial institutions for them to “consider incorporating into their existing AML/CFT programs.”¹⁸¹

Documents obtained by the Committee and Select Subcommittee indicate that federal law enforcement was not the only entity that was abusing the information-sharing process. Deployed as arms of law enforcement, financial institutions seemingly assumed their role and sought ways to manipulate FinCEN’s existing authorities in order to expand the amount of financial data that could be turned over to the FBI.

As an email between MUFG and FinCEN shows, MUFG suggested using the USA PATRIOT Act’s Section 314(a) process to notify other financial institutions about what would otherwise be confidential SAR information. The 314(a) process gives investigators the ability “to canvas the nation’s financial institutions for potential lead information” from “more than 37,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering.”¹⁸² MUFG suggested to FinCEN that it should issue 314(a) requests, based on SAR filings, in order to trigger other financial institutions into conducting a review of their databases for any positive matches and presumably file SARs with law enforcement, “assuming [FinCEN has] the authority.”¹⁸³ But, according to FinCEN, “Section 314(a) provides lead information only and is not a substitute for a subpoena or other legal process.”¹⁸⁴ As Deputy Director Kirby testified, this process is “essentially a hand-raising exercise for whether [the financial institutions] have responsive accounts” in response to a law enforcement inquiry, but the response “does not include the actual financial records.”¹⁸⁵ Yet, the strategy concocted by MUFG would appear to be a substitute for the Section 314(b) legal process, which already exists so that “financial institutions . . . [can] share information with one another in order to identify and report . . . money laundering or terrorist activity” after notifying the Treasury Department.¹⁸⁶ Though Section 314(b) allows financial institutions to share information with one another, according to FinCEN, the 314(b) process “does not relax the prohibition against SAR disclosures” and financial institutions “remain prohibited from disclosing a SAR or any information that would reveal the existence of a SAR notwithstanding

¹⁸⁰ See Email from [Redacted] at FBI to personnel at Bank of America (Jan. 15, 2021 12:40 PM) (BofA-HJUD-00000002); see also STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS 27 (Comm. Print 2024).

¹⁸¹ Letter from Corey Tellez, Acting Assistant Sec’y, Office of Legislative Affairs, U.S. Dep’t of The Treasury, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary at 3-4 (Feb. 9, 2024); As the Treasury Department makes clear, “FinCEN and banks shared information about methodologies that banks could consider using as part of their AML/CFT programs to identify indicia of suspicious activity relevant to the January 6 attack on the Capitol or threats of violence in connection with the then-upcoming presidential inauguration.” *Id.* at 3-4.

¹⁸² FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN’S 314(A) FACT SHEET.

¹⁸³ Email exchange between AnnaLou Tirol, FinCEN, and personnel at MUFG (Jan. 14, 2021) (MUFG-0000248-249).

¹⁸⁴ FINANCIAL CRIMES ENFORCEMENT NETWORK, FINCEN’S 314(A) FACT SHEET.

¹⁸⁵ Transcribed Interview of Mr. Jimmy Kirby at 98 (July 18, 2024).

¹⁸⁶ FINANCIAL CRIMES ENFORCEMENT NETWORK, SECTION 314(B).

Section 314(b).¹⁸⁷ MUFG apparently proposed the “idea” to “support the Bureau’s efforts to address the acute threat of domestic terrorism.”¹⁸⁸

From: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov]
Sent: 1/14/2021 4:23:40 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7-[REDACTED]]
Subject: [External] RE: Bouncing an Idea off You

External email: Please be careful when opening attachments or clicking links.

Terrific - I'll call you at 1. Thanks!

-----Original Message-----

From: [REDACTED]@us.mufg.jp>
Sent: Thursday, January 14, 2021 11:10 AM
To: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov>
Subject: [EXTERNAL] RE: Bouncing an Idea off You

Terrific. If you're able to give me a time, just shoot me an email and I'll re-arrange meetings to be available. I'm free right now from 1-2 but as I said, can shift stuff around if need be.

-----Original Message-----

From: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov]
Sent: Thursday, January 14, 2021 8:34 AM
To: [REDACTED]
Subject: [External] Re: Bouncing an Idea off You

External email: Please be careful when opening attachments or clicking links.

Hi [REDACTED]
It's great to hear from you, and thank you for reaching out with this interesting idea. I will give you a call to chat more, hopefully around midday. I look forward to talking more.
I hope you are safe and well,
AnnaLou

From: [REDACTED]@us.mufg.jp<mailto:[REDACTED]@us.mufg.jp>>
Date: Wednesday, January 13, 2021 at 6:41:53 PM
To: "Tirol, AnnaLou [SES]" [REDACTED]@fincen.gov<mailto:[REDACTED]@fincen.gov>>
Subject: [EXTERNAL] Bouncing an Idea off You

Confidential

AnnaLou, I hope you are well. We live in interesting times. As you might imagine, our bank, and I expect many others, are thinking hard about how we can support the Bureau's efforts to address the acute threat of domestic terrorism we are facing at the moment.

I wanted to bounce an idea off you. Would FinCEN have an appetite (assuming you feel you have the authority) to, in SARs filed in relation to the current acute threat of domestic terrorism, identify whether the suspicious activity being reported involves a customer of another institution in the U.S. and, if so, make a 314(a) request, perhaps under a specific code, for such subjects? In other words, Bank A files a SAR for suspicious transactions involving John Doe, a customer of Bank B (an FI in the US). However, Bank B is unaware of the concern surrounding its customer (unless Bank A utilized 314(b) authorities—but even then, the delay would be unworkable when addressing an acute terror threat). FinCEN, by doing a 314(a) request for that subject, will trigger an internal review in Bank B (most banks will open an investigation following a 314(a) match). If the 314(a) request is coded under a project name, all the better.

I'm happy to explain myself more in a call. [REDACTED] I'm also curious if FinCEN is planning anything independently (i.e., red flags circular). I'm sure that BSAAG members would be happy to contribute thoughts and ideas that could be shared more broadly – even with other BSAAG members.

Anyhow, we are open to assisting however we can, within the existing authorities. Take care and say hi to Ken and congratulations to you both on the passage of the NDAA. That's a big accomplishment!

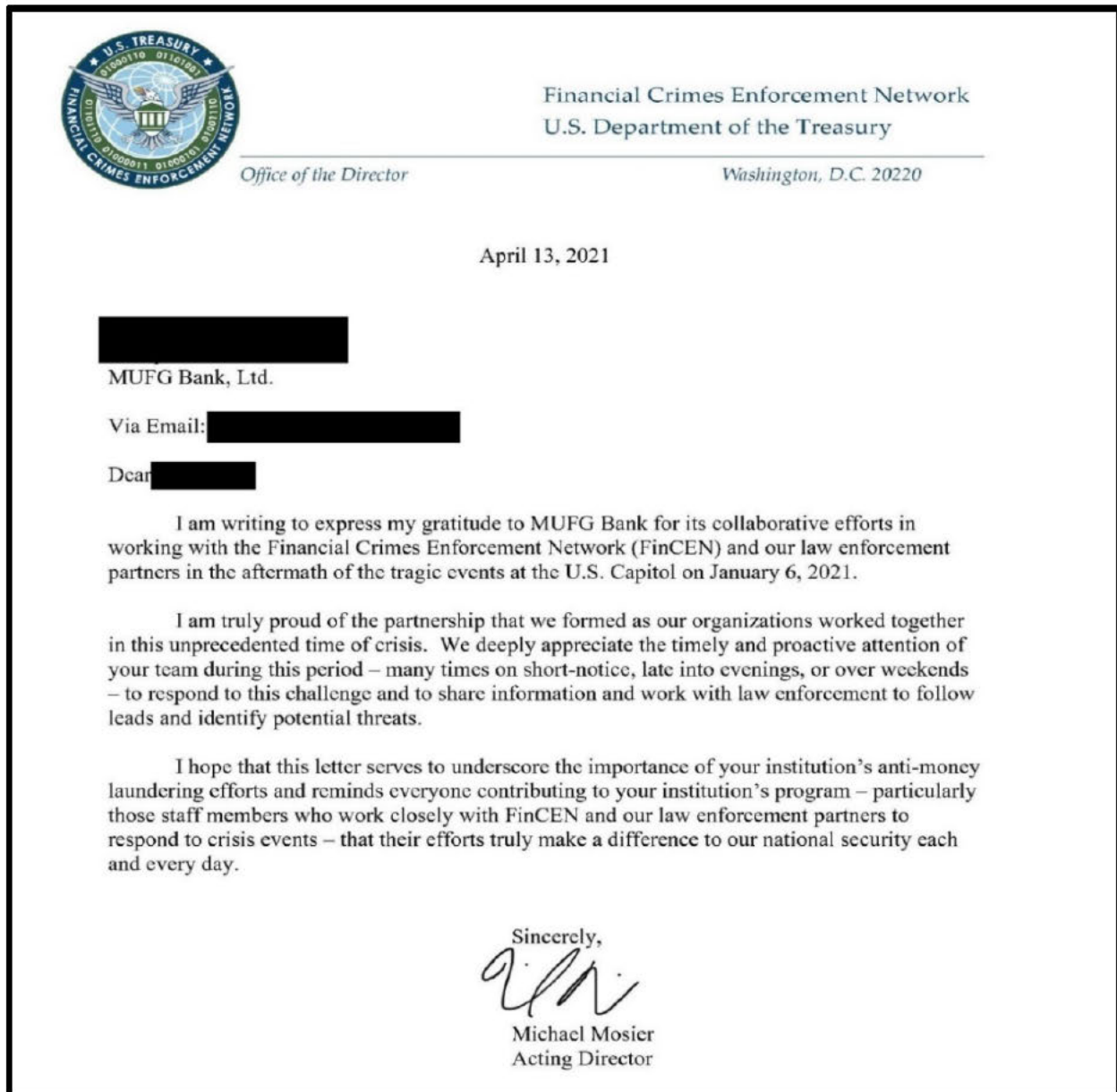
“I wanted to bounce an idea off you. Would FinCEN have an appetite . . . to, in SARs filed in relation to the current acute threat of domestic terrorism, identify whether the suspicious activity being reported involves a customer of another institution in the U.S. and, if so, make a 314(a) request . . . ?”

—Jan. 13, 2021, email exchange between MUFG personnel and AnnaLou Tirol, FinCEN

¹⁸⁷ FINANCIAL CRIMES ENFORCEMENT NETWORK, SECTION 314(B) FACT SHEET.

¹⁸⁸ Email exchange between AnnaLou Tirol, FinCEN, and personnel at MUFG (Jan. 14, 2021) (MUFG-0000248-249).

MUFG’s and other financial institutions’ efforts to assist FinCEN and federal law enforcement’s investigative efforts did not go unnoticed. On April 13, 2021, FinCEN Acting Director Michael Mosier sent a thank you letter to various financial institutions for “the timely and proactive attention of your team during this period – many times on short-notice, late into evenings, or over weekends – to respond to this challenge and to share information and work with law enforcement to follow leads and identify potential threats.”¹⁸⁹



“I am writing to express my gratitude to MUFG Bank for its collaborative efforts in working with [FinCEN] and our law enforcement partners in the aftermath of the tragic events at the U.S. Capitol on January 6, 2021 . . . I am truly proud of the partnership that we formed”
 —Apr. 13, 2021, Michael Mosier, FinCEN, to MUFG personnel

¹⁸⁹ Michael Mosier, FinCEN, to personnel at MUFG, Apr. 13, 2021 (MUFG-0001196).

This letter exemplifies FinCEN and law enforcement’s expectation that financial institutions work to assist the federal government whenever the government calls.

C. The federal government, through the BSAAG advisory group, is increasing its coordination with financial institutions and pushing them to adopt new and invasive technologies that augment the ability to surveil Americans.

Established by the Annunzio-Wylie Anti-Money Laundering Act of 1992,¹⁹⁰ the Bank Secrecy Act Advisory Group (BSAAG) advises the Treasury Department on issues related to the BSA.¹⁹¹ The BSAAG includes representatives from government agencies like the Treasury and Justice Departments, national financial institutions, trade associations, and other businesses subject to the reporting requirements of the BSA.¹⁹² Documents obtained by the Committee and Select Subcommittee indicate that the federal government, through the BSAAG, is pushing financial institutions to integrate new technologies, such as AI and digital ID requirements, that will expand the access to and surveillance of Americans’ data.

i. BSAAG documents indicate that Big Banks and Big Government are advancing the implementation of a national digital ID system.

As the world becomes increasingly digitized, there has been a global push toward requiring digital identification systems.¹⁹³ These systems, under the guise of modernizing identity verification, are designed to authenticate a claimed identity with the real-life existence of the individual “us[ing] electronic means to assert and prove a person’s official identity online.”¹⁹⁴ Traditionally, verifying a person’s identity has relied on physical documents like driver’s licenses and passports.¹⁹⁵ However, in the United States and around the globe, interest groups comprised of financial institutions, influential global organizations, and various governmental bodies are pushing the integration of a national “digital ID” system into financial and public services.¹⁹⁶ Troublingly, the Committee and Select Subcommittee obtained a confidential BSAAG Working Group White Paper, titled “Brick & Mortar to Bits & Bytes: Adapting the U.S. AML/CFT Regime for Digital Identity,” which indicates that a push for a national digital ID requirement in the United States appears to be underway and that financial services may be the vehicle for its adoption.¹⁹⁷

¹⁹⁰ Pub. L. No. 102-550, 106 Stat. 3672 (1992).

¹⁹¹ See Bank Secrecy Act Advisory Group; Solicitation of Application for Membership, 88 Fed. Reg. 9329 (Feb. 13, 2023).

¹⁹² CHARTER OF THE BANK SECRECY ACT ADVISORY GROUP, FINCEN.

¹⁹³ See, e.g., Ash Johnson, *The Path to Digital Identity in the United States*, Information Technology & Innovation Foundation (Sept. 23, 2024).

¹⁹⁴ Financial Action Task Force, *Guidance on Digital Identity* ¶ 57 (Mar. 2020).

¹⁹⁵ See *id.* at ¶ 109.

¹⁹⁶ See Kanwaljit Singh, Digital IDs are an effective tool against poverty, Bill & Melinda Gates Foundation, <https://www.gatesfoundation.org/ideas/articles/mosip-digital-id-systems> (Aug. 15, 2024); see also WORLD BANK, *Digital ID to Enhance Financial Inclusion: A Toolkit for Regulatory Authorities* (Dec. 2021), <https://documents1.worldbank.org/curated/en/099650005162214653/pdf/P16477001277440f10b8080dc6f51daf2dc.pdf>.

¹⁹⁷ *Brick & Mortar to Bits & Bytes: Adopting the U.S. AML/CFT Regime for Digital Identity*, BSAAG FinTech/RegTech Working Group (SCHWAB_HJC_00000717).

In the white paper, the BSAAG Working Group acknowledged “the reality that there is [a] deep political and cultural skepticism of, or even hostility to, a national ID system in the U.S.,” and that the “national ID system will face unique political challenges and structural hurdles in the U.S. . . .”¹⁹⁸ Despite this public skepticism, the BSAAG Working Group recommended that “U.S. financial institutions . . . support digital identity proofing and/or authentication for AML/CFT efforts (customer identification/verification at on-boarding and ongoing due diligence and transaction monitoring) . . .”¹⁹⁹ The white paper also discussed how the biometric information and digital signals enabled by the use of digital ID could be repurposed for “broader KYC [Know-Your-Customer] and transaction monitoring purposes,” mentioning, in particular the use of:

- “geolocation, MAC and IP addresses,”
- “biophysical biometric attributes (e.g., fingerprints, iris patterns, voiceprints, facial recognition),”
- “biomechanical patterns (e.g., keystroke mechanics, typing cadence, or device angle compared with known patterns),”
- “behavioral attributes (e.g., expected log-in channels, email/text message patterns, file access log, time of log-in, etc. compared with historical behavior), email age, patterns of website interaction (e.g., expected progression through product offering and account opening), frequency and type of usage . . .”²⁰⁰

¹⁹⁸ *Id.*

¹⁹⁹ *Id.* at 00000718-719 (internal quotations omitted).

²⁰⁰ *Id.* at 00000736.

IV. Progressive Identity and the Customer Journey

- A. Encourage the use of information associated with digital identification for broader KYC and transaction monitoring purposes

Financial institutions (and their examiners) should take the FATF’s cue and expand their view of traditional KYC information to include those “anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts [like] customer identification/verification at onboarding *and ongoing due diligence and transaction monitoring*.”⁶⁰ Depending on the purpose and stage of the relationship, these “digital signals” may include: geolocation, MAC and IP addresses, biophysical biometric attributes (e.g., fingerprints, iris patterns, voiceprints, facial recognition), biomechanical patterns (e.g., keystroke mechanics, typing cadence, or device angle compared with known patterns), behavioral attributes (e.g., expected log-in channels, email/text message patterns, file access log, time of log-in, etc. compared with historical behavior), email age, patterns of website interaction (e.g., expected progression through product offering and account opening), frequency and type of usage, among others.

“Encourage the use of information associated with digital identification for broader [Know-Your-Customer] and transaction monitoring purposes”

—BSAAG FinTech/RegTech Working Group

The white paper also noted that successful digital ID implementation would have “potentially profound policy implications and benefits” by “focusing financial institutions on behavioral risk” and “leveraging the digital signals” financial institutions would gain from digital ID to better surveil its customers for behavior that the bank considers risky.²⁰¹ This includes expanding and utilizing a concept called “progressive identity” which “recognizes that digital ID is not simply a new method for static identification and verification, but can facilitate the ‘customer journey’ through which customers increase their digital footprint”²⁰² If digital ID and the concept of “progressive identity” are integrated into American financial regulation, government surveillance is likely to pervade even deeper into Americans’ financial activities as the “digital footprint” of Americans increase.

The BSAAG document explicitly stated, “*First*, the U.S. AML regime should create the conditions for digital ID practices to take root in the U.S. financial industry by expanding and updating the existing customer identification program (CIP) rules”²⁰³ In doing so, digital ID is sold as a portable and secure way of determining the validity of an individual’s credentials;²⁰⁴ however, in reality, digital ID can be a potential Trojan horse. It can be a governmental tool used

²⁰¹ *Id.* at 00000720.

²⁰² *Id.* at 00000720, 736.

²⁰³ *Id.* at 00000719.

²⁰⁴ See NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Digital Identity Guidelines: Enrollment and Identity Proofing (2017), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>; see also *Digital Identity: Why It Matters and Why It’s Important We Get It Right*, WORLD ECONOMIC FORUM (Jan. 26, 2018), <https://www.weforum.org/press/2018/01/digital-identity-why-it-matters-and-why-it-s-important-we-get-it-right/>.

to regulate access to banking services and can lead to constant surveillance, as every transaction becomes associated with a digital ID. Some proponents maintain that individuals will have control over their information and the ability to voluntarily participate in the system, but, in practice, digital ID often becomes mandatory, leaving individuals with no choice but to surrender their privacy.²⁰⁵

Indeed, the BSAAG document speaks to the consequences of refusing to comply with digital ID signals, “if a customer uses a VPN [Virtual Private Network] or blocks location permissions—both legitimate privacy-based decisions—the progressive identity of the customer will be hampered . . . as the financial institution may likely have to resort to more traditional KYC [Know-Your-Customer] techniques or *limit the customer’s access to its services*.”²⁰⁶ In other words, making “legitimate privacy-based decisions” may result in a different reality: either accept these tools of surveillance and digital ID, or risk being debanked.

ii. The federal government encouraged financial institutions to incorporate new technologies, including artificial intelligence and machine learning, into their systems to more aggressively track Americans.

Incorporating artificial intelligence (AI) and machine learning (ML) into financial institutions’ AML programs also appears to be a priority of the BSAAG. In April of 2022, Himamauli Das, the then-Acting Director of FinCEN, testified before the House Committee on Financial Services that “we can envision consideration of efforts involving artificial intelligence or machine learning-driven transaction monitoring . . . digital identity tools . . . and automating the adjudication and filing of SARs related to certain types of activity.”²⁰⁷ Confidential BSAAG documents obtained by the Committee and Select Subcommittee reveal that digital identity tools, along with AI and ML solutions, may already be being used to monitor Americans’ financial activity.

On June 23, 2022, the BSAAG Innovation and Technology Subcommittee held a meeting in which one item on the agenda was “AI/Machine Learning—new focus area.”²⁰⁸ Following this meeting, FinCEN and financial institutions exchanged ideas on how to incorporate and utilize AI to further track and report suspicious customer activity.²⁰⁹ On September 19, 2023, a FinCEN

²⁰⁵ See NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DIGITAL IDENTITY GUIDELINES: ENROLLMENT AND IDENTITY PROOFING (2017), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST DRAFTS REVISED GUIDELINES FOR DIGITAL IDENTIFICATION IN FEDERAL SYSTEMS (Dec. 16, 2022), <https://www.nist.gov/news-events/news/2022/12/nist-drafts-revised-guidelines-digital-identification-federal-systems>. See also Jay Stanley, *TSA Shouldn’t Force a Bad Digital ID System on America*, ACLU (Oct. 31, 2023); Brett Solomon, *Digital IDs Are More Dangerous Than You Think*, WIRED (Sep. 28, 2018).

²⁰⁶ *Brick & Mortar to Bits & Bytes: Adopting the U.S. AML/CFT Regime for Digital Identity*, BSAAG FinTech/RegTech Working Group (SCHWAB_HJC_00000737) (emphasis added).

²⁰⁷ *Oversight of the Financial Crimes Enforcement Network: Hearing Before the H. Comm. on Fin. Serv.*, 117th Cong. (2022) (statement of Himamauli Das, Acting Director, Fin. Crimes Enf’t Network).

²⁰⁸ BSAAG Innovation and Technology Subcommittee Meeting (June 23, 2022, 2:00 PM) (JPM_HJC_0001917).

²⁰⁹ See Email from personnel at Promontory Financial Group to BSAAG, FDIC employee, FinCEN liaison, and personnel at HSBC and Barclays (Aug. 18, 2022 1:58 PM) (118HJC_00005933).

liaison sent an email to the AI and ML working group calling for volunteers to draft a white paper on its risks and benefits.²¹⁰

As the Committee and Select Subcommittee have discussed in other reports, the growth and expansion of AI present major risks to Americans’ civil liberties.²¹¹ For example, the Committee and Select Subcommittee uncovered AI being used to censor “alleged misinformation regarding COVID-19 and the 2020 election”²¹² Those concerns are not hypothetical. Some AI systems developed by Big Tech companies have been programmed with biases; for example, Google’s Gemini AI program praised liberal views while refusing to do the same for conservative views, despite claiming to be “objective” and “neutral.”²¹³ With financial institutions seemingly adopting AI solutions to monitor Americans’ transactions, a similarly biased AI program could result in the systematic flagging or censoring of transactions that the AI is trained to view as “suspicious.”²¹⁴ Given that financial institutions and federal law enforcement previously worked together to flag transactions using biased search terms like “TRUMP” or “MAGA,” in addition to FinCEN sharing typologies that treated purchases of “religious texts” or “donations to organizations known to promote radicalism,” as “indicators” of “homegrown violent extremism,” concerns over biased AI transaction monitoring are well-founded.²¹⁵ If financial institutions are using a biased AI to spy on Americans’ transactions, they may begin flagging purchases associated with conservative views such as lawful firearm purchases, tickets to conservative political rallies, or even Bibles—all constitutionally-protected activities.

The BSAAG appears to support using AI and other innovative technologies to monitor customers’ transactions. Another document drafted by a BSAAG working group noted that “[e]ncouraging the adoption of innovative technologies is a priority for industry, law enforcement and regulators to increase the efficiency and effectiveness of AML/CFT programs”²¹⁶ The BSAAG document proposed, among other things, using “[s]uspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence” to monitor Americans’ transactions surreptitiously, without human input.²¹⁷ The white paper also encouraged “[b]ig data infrastructures . . . that can enable financial institutions to ingest, store, index, and analyze information”²¹⁸

²¹⁰ Email from FinCEN liaison, to BSAAG AI/ML Working Group members (Sept. 19, 2023, 2:24 PM) (SCHWAB_HJC_00001209).

²¹¹ See, e.g., STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON THE WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION: HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO CENSOR ONLINE SPEECH “AT SCALE” AND TRYING TO COVER UP ITS ACTIONS (Comm. Print 2024).

²¹² *Id.* at 1.

²¹³ Timothy Carney, *Gemini, Google’s AI, tells very familiar lies*, THE WASHINGTON EXAMINER (Feb. 26, 2024).

²¹⁴ April Levin, *How AI is Revolutionizing Financial Crime Prevention in Banking*, SUPERIOR PRESS (June 4, 2024), <https://www.superiorpress.com/blog/ai-financial-crime>.

²¹⁵ STAFF OF H. COMM. ON THE JUDICIARY, 118TH CONG., REP. ON FINANCIAL SURVEILLANCE IN THE UNITED STATES: HOW FEDERAL LAW ENFORCEMENT COMMANDEERED FINANCIAL INSTITUTIONS TO SPY ON AMERICANS (Comm. Print 2024).

²¹⁶ BSAAG Innovation and Adoption Working Group Recommendations (JPM_HJC_0002612).

²¹⁷ *Id.*

²¹⁸ *Id.*

II. TECHNOLOGY EXAMPLES AND CHALLENGES TO ADOPTION

Technologies either being used or developed/contemplated by financial institutions or vendors include:

- Suspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence.
- Technologies that extract, capture, and analyze structured and unstructured data (e.g., text, speech, voice, image, video, metadata) to identify unusual or suspicious patterns.
- Technologies which review, digitize, and interpret new and existing regulatory intelligence (e.g., rules, regulations, enforcement actions, no-action letters, advisories).
- Big data infrastructures (e.g., cloud computing, data lakes, knowledge graphs) that can enable financial institutions to ingest, store, index, and analyze information within their organizations more quickly and make faster data connections.
- e-Know Your Customer ("KYC") and Know Your Business ("KYB") utilities that leverage distributed ledgers and cryptography to create trusted networks managed by a central provider that stores data that is made available to a larger group via personalizing access per user.
- Use of automated verification tools (e.g., using biometrics, computer vision, deep learning) that speeds up and increases security during remote onboarding.
- Use of distributive ledger platforms to enhance transaction monitoring and enable comprehensive investigations across financial institutions and jurisdiction (e.g., enclave-supporting data sharing).

“Technologies either being used or developed/contemplated by financial institutions or vendors include: [s]uspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence.”

—BSAAG Innovation and Adoption Working Group

In other words, the BSAAG document explored how financial institutions can make greater use of Americans’ financial data and extract additional information on behalf of law enforcement and sought greater collaboration with “law enforcement, regulators, financial service providers, vendors, and technology companies” in order to “facilitat[e] the adoption of new technologies”²¹⁹

Unfortunately, the BSAAG document glosses over any real concern for Americans’ financial privacy and makes no mention of civil liberties, and, instead, prioritizes the interests of the financial industry, law enforcement, and new technologies designed to provide them with even greater insight into Americans’ financial habits and their pattern of life. Documents uncovered in this investigation reveal that the financial information-sharing regime continues to grow alongside the financial institutions’ capacity to surveil Americans.

POTENTIAL LEGISLATIVE REFORMS

Congress enacted the BSA and other relevant pieces of Anti-Money Laundering legislation with the stated goal of curbing money laundering, terrorist financing, and detecting and deterring other crimes.²²⁰ However, the aims of that legislation has fallen short, while

²¹⁹ *Id.* at 0002613.

²²⁰ *See* FED. DEPOSIT INSURANCE CORP., BANK SECRECY ACT / ANTI-MONEY LAUNDERING (BSA/AML).

needlessly sacrificing Americans' financial privacy. Based upon the Committee's and Select Subcommittee's findings, Congress should act to protect Americans' financial privacy.

The Financial Reporting Threshold Modernization Act proposes, among other things, raising the CTR threshold from the \$10,000 mark—set more than 50 years ago—to \$60,000.²²¹ The original \$10,000 CTR threshold, was set “to identify unusually large currency transactions that exceed the legitimate and customary conduct of a bank’s customers, and produce information highly useful to combat financial crime[;]” however, if the CTR threshold were adjusted for inflation, it would be nearly \$75,000 today.²²² For that reason, the \$10,000 threshold actually makes the program less effective as the sheer number of CTR reports—20.8 million in 2023—transforms the CTR from being about criminal activity into a government surveillance program. If inflation trends continue, the number of transactions passing the \$10,000 threshold will continue to increase, resulting in even more CTR filings and greater surveillance of Americans' finances.

Congress could also consider reforming the SAR filing process. Under the current BSA framework, financial institutions are required to act as confidential informants on their customers, reporting them to the federal government without any recourse or notice available to the customer. Congress could amend the BSA to require that banks, after a certain period of time, give notice to the customer that a SAR was filed, provide a justification, and offer an opportunity for the customer to respond to allegations they engaged in “suspicious activity.” Other reforms propose establishing “a private right of action for Americans and financial institutions harmed by illicit government activity.”²²³

Finally, Congress could restore Fourth Amendment protections to Americans' financial records. In order to end warrantless surveillance, Congress could require a warrant before law enforcement can gain access to Americans' private financial information. Senator Mike Lee's Saving Privacy Act proposes bolstering the warrant requirement under the Right to Financial Privacy Act of 1978.²²⁴ Americans should not have to choose between having a bank account and worrying that the federal government may have warrantless access to their personal financial decisions and other revealing details about their pattern of life, interests, faith, politics, and more.

²²¹ Financial Reporting Threshold Modernization Act, H.R.8686, 118th Cong. (2024).

²²² American Bankers Association, *Letter to FinCEN on Information Collection Requirements relating to Currency Transaction Reports* (Apr. 5, 2024); see also Nicholas Anthony, *How Inflation Erodes Financial Privacy*, CATO (June 10, 2022).

²²³ See Press Release, Sen. Mike Lee, Lee Introduces the Saving Privacy Act to Protect Americans' Financial Data (Sept. 25, 2024); see also Saving Privacy Act, S. 5242, 118th Cong. (2024).

²²⁴ S. 5242 (2024).

CONCLUSION

The Committee and Select Subcommittee opened this investigation to determine how and to what extent the federal government and financial institutions weaponized financial surveillance to monitor the private lives of American citizens. The result of the investigation reveals that financial surveillance goes far beyond the targeting of one political ideology and is more pervasive than one act of criminal conduct. The information-sharing apparatus, designed by Congress and implemented by the Executive Branch and financial institutions, has been warped into a tool designed to constantly monitor the activities of millions of Americans.

Federal law enforcement has shown that it will leverage any opportunity to operate outside the bounds of the statutes that govern access to Americans' financial data. Because the existence of a SAR and other BSA filings may never be revealed to a customer, Americans may never know the extent to which their finances are being tracked. The most egregious abuses of this system occurred in the days after January 6, 2021, in which seemingly anyone with any possible connection to Washington, D.C., was potentially subjected to warrantless government surveillance and SAR filings. It is very likely that, without intervention or reform, federal law enforcement will abuse this system again in the future.

Indeed, the information gathered by the Committee and Select Subcommittee shows that the federal government continues to exploit the laws governing financial data and is deputizing financial institutions as arms of law enforcement. By sharing typologies and even specific names with financial institutions, federal law enforcement has shown its willingness to manipulate the SAR filing process. Although the FBI and FinCEN claim that financial institutions have the choice to act upon the information federal law enforcement shares, the reality is different. When federal law enforcement demands something, it is difficult—if not impossible—for banks to say no.

As the federal government and financial institutions adjust to modern finance, there will come a time when almost no financial activity will occur outside of the watchful eye of the federal government. And as the federal government and the financial sector explore integrating new technologies like digital ID and the use of AI to monitor transactions, every financial movement of every American could soon be automatically recorded and scrutinized. With the documented abuses of AI technology already mounting, these new tools pose a threat of biased enforcement.

Absent adequate congressional oversight and legislative reforms, it is likely that countless more Americans will be subject to financial surveillance and potentially federal investigation, all without ever knowing about it. The Committee and Select Subcommittee will continue to investigate the coordination between Big Banks and Big Government to protect Americans' civil liberties.

Appendix

1

2

3

4

5 COMMITTEE ON THE JUDICIARY,

6 U.S. HOUSE OF REPRESENTATIVES,

7 WASHINGTON, D.C.

8

9

10

11

12 INTERVIEW OF: PETER SULLIVAN

13

14

15

Tuesday, April 9, 2024

16

17

Washington, D.C.

18

19

20 The interview in the above matter was held in room 2237, Rayburn House Office

21 Building, commencing at 10:01 a.m.

22

Present: Representative Jordan.

1 Appearances:

2

3

4

5 For the COMMITTEE ON THE JUDICIARY:

6

7 [REDACTED] PROFESSIONAL STAFF MEMBER

8 [REDACTED] COUNSEL

9 [REDACTED] SPECIAL COUNSEL

10 [REDACTED] DEPUTY CHIEF COUNSEL FOR OVERSIGHT

11 [REDACTED] MINORITY OVERSIGHT COUNSEL

12 [REDACTED] MINORITY CHIEF OVERSIGHT COUNSEL

13 [REDACTED] MINORITY OVERSIGHT COUNSEL

14 [REDACTED] MINORITY STAFF ASSISTANT

15 [REDACTED] MINORITY OVERSIGHT COUNSEL

16 [REDACTED] MINORITY PROFESSIONAL STAFF MEMBER

17

18

19 For the SUBCOMMITTEE ON CRIME AND

20 FEDERAL GOVERNMENT SURVEILLANCE:

21

22 [REDACTED] MINORITY DETAILEE

1 For the FEDERAL BUREAU OF INVESTIGATION:

2

3 [REDACTED] ASSISTANT GENERAL COUNSEL,

4 OFFICE OF GENERAL COUNSEL

5 [REDACTED] COUNSEL

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 [REDACTED] We will go on the record. Good morning. This is a transcribed
2 interview of Peter Sullivan. Chairman Jordan has requested this interview as part of the
3 committee's oversight of the Federal Bureau of Investigation. Would the witness please
4 state your name for the record.

5 Mr. Sullivan. Peter John Sullivan.

6 [REDACTED] And could agency counsel please state your name for the record.

7 [REDACTED] [REDACTED] counsel with the FBI.

8 [REDACTED] [REDACTED] FBI, Office of General Counsel.

9 [REDACTED] And, Mr. Sullivan, you understand that agency counsel has a primary
10 fiduciary duty to the Bureau and not to you individually?

11 Mr. Sullivan. Yes.

12 [REDACTED] And so you'd like to continue with agency counsel today?

13 Mr. Sullivan. Yes.

14 [REDACTED] On behalf of the committee, I want to thank you for appearing here
15 today to answer our questions. The chairman also appreciates your willingness to
16 appear voluntarily. My name is [REDACTED] I am with Chairman Jordan's staff. I
17 will now have everyone else from the committee who is here in the room introduce
18 themselves as well.

19 [REDACTED] [REDACTED] counsel with Chairman Jordan.

20 [REDACTED] [REDACTED] with Ranking Member Nadler.

21 [REDACTED] [REDACTED] with Ranking Member Nadler.

22 [REDACTED] [REDACTED] [REDACTED] with Ranking Member Nadler.

23 [REDACTED] [REDACTED] Ranking Member Nadler.

24 [REDACTED] [REDACTED] Ranking Member Nadler.

25 [REDACTED] [REDACTED] with Chairman Jordan.

1 ██████████ Thank you. I would like to now go over the grounds rules and
2 guidelines that we'll follow during today's interview. Our questioning will proceed in
3 rounds. The majority will ask questions first for one hour. Then the minority will have
4 an opportunity to ask questions for an equal period of time if they so choose. We will
5 alternate back and forth until there are no more questions and the interview is over.
6 Typically, we take a short break at the end of each hour, but if you would like to take a
7 break apart from that, please just let us know. As you can see, there's an official court
8 reporter taking down everything we say to make a written record. So we ask that you
9 give verbal responses to all questions. Do you understand this?

10 Mr. Sullivan. Yes.

11 ██████████ So the court reporter can take down a clear record, we'll do our best
12 to limit the number of people directing questions at you during any given hour to just
13 those people on the staff whose turn it is. Please try and speak clearly so the court
14 reporter can understand and so the folks down at the end of the table can hear you. It
15 is important that we don't talk over one another or interrupt each other if we can help it,
16 and that goes for everybody presence at today's interview. We want you to answer our
17 questions in the most complete and truthful manner as possible, so we will take our time.
18 If you have any questions or if you do not understand one of our questions, please let us
19 know. Our questions will cover a wide range of topics. So, if you need clarification at
20 any point, just say so. If you honestly don't know the answer to a question or do not
21 remember, it is best not to guess. Please give us your best recollection. And it is okay
22 to tell us if you learn information from someone else; just indicate how you came to know
23 that information. If there are things you don't know or can't remember, just say so, and
24 please inform us who, to the best of your knowledge, might be able to provide a more
25 complete answer to the question. You should also understand that by law you are

1 required to answer questions from Congress truthfully. Do you understand that?

2 Mr. Sullivan. Yes.

3 [REDACTED] This also applies to questions posed by congressional staff when
4 interviewed. Do you understand this?

5 Mr. Sullivan. Yes.

6 [REDACTED] Witnesses that knowingly provide false statements or false
7 testimony can be subject to criminal prosecution for making false statements under 18,
8 U.S.C., section 1001. Do you understand this?

9 Mr. Sullivan. Yes.

10 [REDACTED] Is there any reason you are unable to provide truthful answers to
11 today's questions?

12 Mr. Sullivan. No.

13 [REDACTED] Finally, I would like to make note that the content of what we
14 discuss here today is confidential. We ask that you not speak about what we discuss in
15 this interview to outside individuals to preserve the integrity of our investigation. For
16 the same reason, the marked exhibits that we will use today will remain with the court
17 reporters and go in the official transcript, and any copies of those exhibits will be
18 returned to us as we wrap up.

19 All right. That's the end of my preamble. Is there anything my colleagues from
20 the minority would like to add?

21 [REDACTED] No, we would just like to thank Mr. Sullivan for appearing here
22 today. We appreciate it. And we would also just like to note that we at this point have
23 done well over a hundred transcribed interviews, and only a fraction of the transcripts
24 have been released, and we would encourage our majority counterparts to release all of
25 them.

1 [REDACTED] I will just note for the record that our minority counterparts have
2 equal access to the transcripts, and I'll turn it over to agency counsel who would like to
3 make some remarks.

4 [REDACTED] Thank you. As you know, the FBI has determined to make Mr.
5 Sullivan, a non-SES employee, available to speak to the committee today, pursuant
6 to the accommodations process, related to the facts and circumstances of this matter,
7 including his personal knowledge and communications he has had with financial
8 institutions as part of his work at the FBI. As part of that, it's our understanding that we
9 are likely to talk about a specific suspicious activity report, or SAR, today. The existence
10 of any details within any SAR are confidential according to the Bank Secrecy Act. The
11 Department of Treasury, specifically FinCEN, maintains the SAR program. It's our
12 understanding that Treasury has confirmed the existence of the SAR at issue today and
13 has further provided access to the SAR to the committee and the scope of this inquiry.

14 Accordingly, Mr. Sullivan can talk about this specific SAR today. If falls within his
15 official duties as a current FBI employee to respond to questions within this transcribed
16 interview to the extent that it remains within the scope of the committee's stated inquiry
17 and as he is here today in his official capacity. He will not be able to detail specific
18 identifying information of individuals correlated with the SAR or any other SARs. Any
19 other dissemination of this information outside of the committee is subject to the Bank
20 Secrecy Act's obligations concerning confidentiality.

21 Finally, we would like to request that Mr. Sullivan's name is redacted from any
22 public releases about this interview, including those that have already been released and
23 are currently posted online. He is a non-SES employee, and we ask the committee
24 respect longstanding practice to not publicly post non-SES names to protect line-level
25 employees from threats and other security concerns, which are acutely present here.

1 Thank you.

2 [REDACTED] The clock now reads 10:06 a.m. We'll start our first round of
3 questioning. I'll turn it over to my colleague, [REDACTED]

4 EXAMINATION

5

BY [REDACTED]

6 Q Mr. Sullivan, when did you first join the Federal Bureau of Investigation?

7 A In 1999.

8 Q And what was your key motivation for joining the FBI?

9 A Mostly because I wasn't good enough at baseball, but I wanted to -- I had a
10 family that had a law enforcement and a government service background, and it was one
11 that I wanted to participate in and contribute in any way I could.

12 Q And what is your current position at FBI?

13 A Currently, I'm an intelligence analyst in a Financial Targeting Analysis Unit.

14 Q And can you describe your roles and responsibilities in this position?

15 A In my current position, I'm on a leadership team to advance some of the
16 mission items with respect to financial targeting, terrorist financing, and leveraging
17 financial sector data internally for FBI investigations.

18 Q And can you elaborate a little more on what financial targeting and
19 leveraging financial data means?

20 A It's a very basic concept of financial targeting being -- narrowing the focus of
21 data to understand whether or not a threat exist, and then reactively using existing
22 intelligence or investigative activities that reveal something to a terrorist nexus to which,
23 you know, we examine further and support operations.

24 Q And, in your current role, is it limited to terrorist financing?

25 A It's limited to terrorism.

1 Q To terrorism. And do you work with private sector companies in the
2 current role?

3 A I do not. I work with my former unit. I work directly with them. It's the
4 Strategic Engagement Unit where I was the finance sector liaison for the division.

5 Q And can you describe the organizational structure of your office?

6 A Of my office? We fall under the Targeting Development Section. There
7 are many units that are basically set up for terrorism targeting as well as on the
8 counterterrorism analysis side all-source analysts. Within my unit, we're on the
9 Targeting Development Section side. So we support current investigations and look at
10 proactive information, various sources, tips, and leads to try to enhance whether or not
11 we should further pursue those targeting leads.

12 Q And you stated as a part of the Strategic Engagement Unit?

13 A Strategic Engagement Unit is in a separate section. They are in the
14 Engagement Section.

15 Q And so what section are you in?

16 A I'm in the Targeting Development Section.

17 Q Okay. And is that a part of a larger division?

18 A They're all part of the Counterterrorism Division.

19 Q Okay. And how is the information you receive ordinarily provided?

20 A In my current role or in the role that I had for today's proceedings?

21 Q In your current role.

22 A Information either is received through upper management. It could be
23 intel. It could be existing investigations, leads from existing investigations to which, you
24 know -- within our mission of targeting, we'll provide that support to the investigation or
25 development of the lead.

1

BY [REDACTED]

2

Q If I could, when did you leave the Strategic Partner Engagement Section?

3

A In December on paper. In January.

4

Q December of 2023?

5

A Yeah.

6

Q And then you moved over to become an intelligence analyst in January 2024.

7

Is that correct?

8

A Yeah. I was an intelligence analyst when I was a finance sector liaison in a

9

supervisory capacity at the time of the Capitol riots.

10

Q And how long did you hold the position that you left in December 2023?

11

A I held it for 3 years.

12

Q Three years. And how many people did you supervise in that role?

13

A As part of the Strategic Engagement Unit?

14

Q Correct.

15

A Yeah, two, over that time period.

16

Q And what were their titles?

17

A Supervisory special agent.

18

Q And can you tell us how the Strategic Engagement Section is organized?

19

A The Strategic Engagement Section -- it's the Strategic Partner Engagement

20

Section. They are organized as a ops support branch. They fall under the National

21

Joint Terrorism Task Force. It falls under the Strategic Partner Engagement Section as

22

well as Strategic Engagement Unit. They have a couple of new units that they've

23

developed, the Guardian Enhancement Unit. I believe they have two; one that's

24

CT-focused, and one that has, I think, terrorist links that also connect to other operational

25

divisions.

1 Q And you focus on the financial sector. Is that correct?

2 A In my previous position in the Engagement Unit?

3 Q Correct.

4 A Yeah, so my job was to engage at the executive level with financial
5 institution.

6 Q And, when you say "executive level," what do you mean?

7 A It would be -- it would vary from in any supervisory capacity from senior vice
8 president to managing level director to BSA AML director.

9 Q And the two individuals that you supervised, did they work specifically with
10 the financial sector as well?

11 A They did.

12 Q And, within the Strategic Partner Engagement Section, were there
13 individuals who worked with other sectors?

14 A Yes, within our unit. So our unit, I was a finance sector liaison. I worked
15 with a number of financial institutions, banks and nonbank financial institutions. We
16 also within the unit covered the trucking and shipping sector, the tech sector, the
17 hospitality sector. We did also engaged with the retail sector.

18

BY [REDACTED]

19 Q And where is your duty station now?

20 A Headquarters.

21 Q And how often do you interact with the FBI Director?

22 A Very little. As my GS-15 position would -- is likely consistent with most
23 GS-15 positions. Very little.

24 Q How often do you interact with the FBI Deputy Director?

25 A I know the Deputy Director personally, but professionally, I interact with him

1 very little.

2 Q And do you interact with Main Justice often?

3 A Very little in my capacity of what we're talking about today within my
4 capacity as Strategic Engagement Unit. In prior capacity, I worked a little bit more with
5 Department of Justice reporting to White House National Security Council.

6 Q And, before we move on, can you walk us through the positions you've held
7 at the FBI?

8 A Sure. So, starting in 1999, 25 years, my first position was with the Special
9 Surveillance Group out of Washington Field Office. I worked counterterrorism and
10 foreign counter intelligence surveillance, all types of surveillance. I served on a special
11 recognizance team. We had -- WFO had number of high-profile investigations. I was
12 on the arrest team for the Russian spy Stanislav Gusev, who was listening in on State
13 Department meetings. I also served on the special recognizance team for evidence
14 recovery for the Robert Hanssen case as well as worked with a number of my colleagues
15 in WFO, because of my duties on the special recognizance team, recovering evidence at
16 the Pentagon after the 9/11.

17 Q And those were all in the surveillance roles that you mentioned?

18 A Yes. Correct.

19 BY [REDACTED]

20 Q Okay.

21 A Correct. You want me to keep going in my career, or you asked me about
22 my career?

23 Q Yeah, the positions you've held?

24 A Yeah, so, following that surveillance, I became an intel analyst for the
25 Terrorist Financing Operation Section in roughly 2003, where I served in about four

1 different units covering operations, targeting, all-source analysts. I was -- I served on a
2 number of capacities dealing with other government agencies and access to different
3 financial platforms. And then I served on the Syria-Iraq Task Force as a supervisory
4 intelligence analyst. I believe I became a supervisor in 2009. The Bureau, I applied for
5 and was granted a sabbatical opportunity to get my master's degree in 2010. I did that,
6 and a year later came back into my role as a supervisory intel analyst at the Syria-Iraq
7 Task force. From there, I applied for and was promoted to my GS-15 position as the
8 Bureau's first deputy intel officer for threat finance for the Bureau of Intelligence Council,
9 where I worked various matters representing FBI executives at the White House National
10 Security Council, Office of Director of National Intelligence, as well as working with
11 section chief DAD and AD level for the operational divisions on policy, intelligence, and
12 operations matters that were related to finance. From there is when I returned back to
13 the Counterterrorism Division as I the Finance Sector Liaison in the summer of 2020.

14 Q And what is your formal education, training, or prior work experience just
15 formal education really?

16 A Yeah, so I mentioned my master's degree in strategic intelligence. I have
17 an undergrad. As far as -- do you want to know about training about other job training
18 or just academic?

19 Q Any other certifications?

20 A Yeah, so I'm an AKM certified. So that's an anti-money laundering
21 specialist. There are -- it's a pretty wide-scoped certification. And then over more
22 than half of my career spending it on finance-related side, just a number of financial
23 intelligence operations and compliance training, and just basically more -- some formal
24 and a lot of on-the-job training and a number of those positions that I discussed.

25

BY [REDACTED]

1 Q And, during your time at the Strategic Partner Engagement Section from the
2 summer of 2020 to December 2023, can you describe for us the reporting structure that
3 you followed? Did it change at all? Was it the same?

4 A What was the dates, again, I'm sorry?

5 Q You said you went back to the Strategic Engagement Section the summer of
6 2020 and then you left --

7 A Back to the division, yeah. Right. I never been in the Strategic
8 Engagement Unit until I returned in 2020.

9 Q In 2020. Okay. So, between 2020 and 2023, did you have the same
10 reporting structure?

11 A Yes.

12 Q And can you describe that reporting structure?

13 A I did have the same reporting structure to the unit chief position.

14 Q To the unit chief?

15 A Which was also a GS-15.

16 Q And the unit chief, they were they -- were they overall the whole Strategic
17 Partner Engagement Section or just specific to a unit?

18 A The unit fell under the section.

19 Q Okay?

20 A So that would be a subset. Every unit is a subset of a section at
21 headquarters.

22 Q So you reported to the unit chief, and then there was someone above the
23 unit chief?

24 A Section chief.

25 Q Who was that -- the section chief. And then who did the section chief

1 report to?

2 A Up to the Deputy Assistant Director.

3 Q The Deputy Assistant Director of the Counterterrorism Division?

4 A Correct. Yes.

5 Q Okay. And who --

6 A One of three Deputy Assistant Directors.

7 Q And who was the Deputy Assistant Director at the time?

8 A I believe it was Kevin Vorndran.

9 Q Kevin Vorndran. And then --

10 A And you say at the time of when I was hired?

11 Q At the time, did it change at all between 2020 and 2023?

12 A Yeah, I mean headquarters management changed. It was all the time.

13 Q But would you say you mainly the Deputy Assistant Director at the time was
14 Kevin Vorndran?

15 A At this the of the Capitol riots, yeah, absolutely.

16 Q And the Assistant Director at the time was who?

17 A Was at the Tim Langan. Tim Langan.

18 If my memory serves, I believe it was Tim Langan. I served three ADs, so -- in the
19 Counterterrorism Division, and many others in other divisions.

20 BY [REDACTED]

21 Q In that role, what was the mission of that, if you remember that?

22 A To engage with the private sector on all things law enforcement-related.

23 The banks and nonbank financial institutions all had BSA obligations to report suspicious

24 activity as well as understand how to do better due diligence when it comes to various

25 threats, but certainly within our role in Counterterrorism Division concentrate focusing on

1 terrorism.

2 Q And, as the financial sector liaison, can you talk through some of your
3 general duties and responsibilities?

4 A Yeah, on a daily and weekly basis, to engage with executives at various
5 institutions. Most of the engagement went primarily by volume of the financial
6 institution and what they took on in terms of the volume of threats that they were trying
7 to cover down on. But it could go all the way down to, you know, a nonbank financial
8 institution as a fintech company that had proprietary data, and they also had BSA
9 reporting obligations. And they would be looking to participate in information exchange
10 on threats, on typologies, on indicators, on that type of thing. And that's what our team
11 would take in -- was responsible for taking in tips and leads. Oftentimes, because of SAR
12 reporting thresholds, oftentimes they came in the form of a SAR. Other times, that
13 engagement was reactive, meaning the Bureau, my unit, myself or someone on my team
14 had, you know, a legal process, such as a grand jury subpoena, that they wanted
15 expedited on a priority investigation.

16 Q And why does your division reach out to the private sector?

17 A Actually, out of all the operational divisions, they all have an element that
18 has an engagement responsibility with the private sector and partnerships in general.
19 It's one of Director Wray's pillars, his partnerships. In the Counterterrorism Division,
20 under the national security lens, we've actually done a very good job at formalizing that
21 engagement based off of the threat-based threats that we cover on the national security
22 side. So that engagement -- you know, our authorities to engage spreads across all the
23 operational divisions. But, in the Counterterrorism Division, it's definitely more
24 formalized. And we've codified that, I believe, in 2019 before I came to the section.

25 Q And are there other industries besides financial institutions that --

1 A Yeah, the different sectors that I mentioned previously.

2 Q Okay. And how do you manage your outreach and your relationships with
3 the private sector?

4 A It's really about, you know, engagement at the supervisory and executive
5 level. You're dealing with information and brainstorming that obviously your
6 counterpart has many other people under them that have BSA reporting thresholds.
7 They have due diligence reporting requirements. They have their own internal audits,
8 right, that they deal with. That engagement is daily on interacting of what the threat is
9 as well as brainstorming with the institutions. I also set up briefings for the institutions
10 to bring in subject-matter experts when I as a generalist wouldn't be able to brief them
11 on a specific type of terrorist threat. I wasn't an all-source analyst. So my job was to
12 bring in the right folks and facilitate that engagement.

13 Q And how do you decide who to reach out to or who to partner with?

14 A So, when I came into the division, you know, my previous experience as a
15 line analyst in the Terrorist Financing Operation Section, there were a number of legacy
16 partnerships. Most of those were very -- are anchored in those legacy partnerships with
17 the large financial institutions. So that engagement had been codified before I came
18 back into the unit. And I was actually recruited to come into that position because the
19 GS-15 that had that position that was appointed by Director Mueller specifically had
20 passed away of a heart attack. And I was recruited to come back from my position as an
21 intel officer to take on that role.

22 Q When you say that these relationships were codified or formalized, what do
23 you mean by that?

24 A Just internally as far as, you know, even though all of the operational
25 divisions don't -- aren't required to have a codified relationship, I think because of the

1 legacy partnerships that were anchored in that engagement since 9/11. There were
2 various programs and initiatives that supported operations and that also supported
3 compliance reporting obligations by the institution that the Bureau supported. And so
4 there was so much engagement that we felt like, at the division level, that we wanted to
5 formalize that.

6 Q And do you have to receive approval before reaching out to an entity in the
7 private sector or an individual in the private sector?

8 A No.

9 Q Are there any formal procedures or guidelines that you all followed in
10 dealing with the private sector?

11 A Like what?

12 Q Manuals, guidance, training?

13 A No, I mean, I think that, in terms of engagement and what my role was
14 engaging with executives, there was certainly compliance assumptions in terms of legal
15 process and lawful regulatory allowances, whether it was SARs or grand jury subpoenas,
16 on either side of the fence. There was a management level that had that understanding.
17 So, in terms of a manual, there was no manual -- we didn't need a manual because of the
18 experience on both sides of that engagement.

19 [REDACTED] But general policies --

20 Mr. Sullivan. Yeah, FBI policies applied broadly, right, with that engagement.

21 But, in terms of, you know, FBI and DOJ authorities, that's what permitted me to engage
22 on a regular basis.

23 BY [REDACTED]

24 Q And how is your relationship with financial institutions important?

25 A Partnerships in general. But certainly my role as the finance sector liaison,

1 finance and financial information plays a huge role in understanding whether or not we
2 need to assess a specific threat or finding out more information to support an
3 investigation. It's one of many different information areas of need, right, when you're
4 supporting operations or any investigation. But finance is a very deliberate piece of
5 information. Communications intelligence and other things that are gathered within the
6 investigation are all critical. Finance is just one piece of that critical evidence or
7 information.

8 Q And how would you describe your relationship with the private sector in
9 general, the FBI?

10 A I mean, in short term, great. The relationship was very professional.
11 There was never any misunderstandings about -- day-to-day or weekly things were
12 quickly taken care of, I think due to the experience on both sides of the coin, that
13 engagement either from me to an executive or to a supervisor that was supervising, you
14 know, supervising specific analysts within the bank that we're looking at, say, ISIS or
15 al-Qaida or another threat.

16 BY [REDACTED]

17 Q And, in your role as financial sector liaison, did you share information with
18 members of the private sector?

19 A Oh, absolutely, yeah. Anything at the unclassified level, we shared on a
20 regular basis. If -- we also shared information in briefings to include case successes,
21 cases that were adjudicated, fully adjudicated in unclassified briefings to investigators as
22 almost a training and also a morale booster for investigators that do a lot of hard work
23 pushing out SARs or setting up alerts and doing a lot of analysis. There is plenty of other
24 information that, you know, we share on a regular basis that is unclassified. However,
25 we also invite financial institution senior executives to an annual counterterrorism

1 conference where they're read in to a briefing to receive classified information so that
2 they can get a context of how to better tackle a threat. So that relationship is very, very
3 unique and critical to the various assistant directors I've fallen under. And, of course,
4 Director Wray holds the Counterterrorism Division as one of the positive partnership
5 engagement.

6 Q And so what sorts of materials are you sharing with the private sector?

7 A It could be information that's approved by the case agent and the program
8 manager at headquarters at the unclassified level. It could be PII. It could be grand
9 jury subpoena, soft copies in order to expedite subpoena on a priority investigation. It
10 could be information about a threat, right. Again, going back to giving briefings or just
11 brainstorming on information that I've seen either through our all-source analyst section
12 that's been downgraded to unclassified or discussions with our targeters that are seeing
13 trends in specific data that we might be able to share. So it's a lot of different
14 information. But mostly at the unclassified level.

15 Q Yeah, and are they liaison information reports? What is the name of the
16 documents, and what medium are they sharing?

17 A If it's downgraded to unclass and shareable, if it's an actual production,
18 that's something that our unit will receive from the analytic section or the Office of
19 Private Sector. Usually, it's only finished production that we would share in that case.
20 But I am addressing your LIR issue. But there are plenty of other unclassified, you know,
21 pieces of information that we would also share.

22 Q Is that ordinarily shared via email or another medium?

23 A Typically email. Typically email.

24 Q Directly to an executive at a financial institution?

25 A Or it could be briefed orally over, you know, like a Teams briefing or

1 something like that.

2 Q Do you have to get approval prior to sharing those materials?

3 A Only approval in a sense of typically our upper management would say,
4 this is -- if it's a finished production, finished intelligence production, we typically would
5 get it from either our unit chief or our section chief and say, "Feel free to share it with
6 your partners."

7 Q Okay. And does the private sector regularly share information with you?

8 A Yes.

9 Q Outside of the Bank Secrecy Act space, do they share other kinds of
10 materials?

11 A I don't really understand the question.

12 Q Do they share PowerPoints? Do they share documents?

13 A Yeah, I don't know that that would be outside their BSA requirements.

14 Q So they only would share things that are pursuant to the Bank Secrecy Act?

15 A Well, BSA data, in general, is, you know, it requires the financial institutions
16 to obligate to share suspicious activity and other information. So, within those kind of
17 broad -- that broad scope, I would say it's all generally within BSA.

18 Q Okay. And what medium is that information normally shared?

19 A BSA data, it would be due the FinCEN portal -- or once SAR is published, it
20 may be through an email -- a secure email portal.

21 Q And, once it's received, how is it stored within the Bureau?

22 A Once it's received, typically the unit, depending on what we review -- first of
23 all, we review the information that we receive from them every time as we're receiving it
24 from an executive level. You have to understand that there are like 5 million SARs that
25 are published a year. So, if I am receiving, say, give or take, a hundred SARs in a given

1 year, I'm receiving a handpicked SAR from an executive at a financial institution that
2 thinks that it might be worthy of taking a look at. There is no understanding by the
3 institution that that would require us to open an investigation. But the fact that the
4 executive is highlighting that is enough for me to say, "Yeah, I'm going to review what you
5 send me," and then further assess does this need to be looked at further.

6 Q So, within that universe of 5 million SARs, you said you get a hundred or so,
7 we'll say. So there are SARs that are filed in the FinCEN portal, and then there are SARs
8 that are sent directly to you from an executive?

9 A All of the SARs that are sent to me are already published in the FinCEN
10 portal.

11 Q So, in addition to sending them in the portal, it may be sent to you?

12 A Might be. A number of times within my role at the time, there would be
13 occasions where they would just give me the BSA ID, and then one of our analysts on our
14 time would retrieve that with from the FinCEN portal. Or we have a SIPRNet access to
15 SARs that the Bureau intakes that will take a look at it that way.

16 Q And why would they ordinarily send it in addition to filing it in the portal to
17 you or someone on your team?

18 A If they thought that it was worthy of taking -- for me or someone on my
19 team to take a review, they may send it once it's published by the institution into the
20 FinCEN portal.

21 Chairman Jordan. And who makes the determination whether it gets to you?
22 Is it the executive at the bank or is it someone in the FBI who is screening them all and
23 then -- or could it be both?

24 Mr. Sullivan. No, it's generally the executive at the bank or the supervisor.

25 Chairman Jordan. So they have to -- according to the Bank Secrecy Act, they

1 have to time some -- they file these SARs, and it goes into this portal. And then they
2 said, "These 5 million we filed, I think this is important enough" -- that they are going to
3 alert you to it.

4 Mr. Sullivan. Yeah, I mean, when I say 5 million, that's across all financial
5 institutions.

6 Chairman Jordan. I understand.

7 Mr. Sullivan. So that would be kind of the strategic picture of the volume of it.
8 But, within the line-item SARs that are sent to my attention, it's because they think that it
9 either could have a potential terrorist nexus or, a number of the executives that I've dealt
10 with, because we had a very robust program and engaging with the private sector.
11 Oftentimes, they may -- the information that they would share may be involved in
12 nonterrorist issues, and they knew that we had good cross-divisional communication with
13 our other operational divisions, whether it be the Criminal Investigative Division, Cyber
14 Division, or WMDD, or, in rare cases, counterintelligence. So, if we felt after reviewing
15 the information that would be relevant to one of the other operational divisions, that
16 trust with the executives and the executives that I was engaging with at the time knew
17 that I would find the right home for it to put it in front of whatever investigator or
18 supervisor should take a look and determine at that point if it warranted further
19 investigative review.

20 Chairman Jordan. Okay.

21

BY [REDACTED]

22 Q And so, once you receive one and you start that review process, what does
23 that review look like?

24 A Just reviewing -- I mean, primarily reviewing the SAR narrative, which is at
25 the conclusion of the end of the SAR; making sure that I understand the suspicious

1 activity; the information that's being communicated, if I have any questions in my mind
2 about that, I may request the supporting documentation. If, in fact, it came with the
3 SAR, or it was listed in the narrative that there's supporting documentation for it, I would
4 request that. If I still had questions, then I may ask the question again. That was kind
5 of a critical first review piece before I determined whether or not we were going to take a
6 further look at it and either assign it to the SSA that was working for me at the time or an
7 analyst on our team.

8 Q What is supporting documentation?

9 A Supporting documentation may or may not be included referenced in a SAR.
10 Typically it's referenced within the narrative that supporting documentation exists. It
11 could be, you know, every -- you know, the scope of supporting documentation could be
12 very informal research or screen shots of data that they were looking at that helped them
13 formulate the SAR narrative and actually published the SAR. So it could be a Word doc.
14 It could be an Excel spreadsheet. It could be just various, you know, very open-sourced
15 intelligence type of things that the bank would have access to. Oftentimes, you know,
16 screen shots of, you know, commercial software that they used in order to do better due
17 diligence on the thing that they were investigating.

18 Q Does it often include customer names or just the customer transactions?

19 A Sometimes. Not all the time.

20 Q Okay. Do you interact often with the Office of Private Sector?

21 A Often, I interact with them. What would you consider often?

22 Q Well, why don't you tell me? How often do you interact with them?

23 A In my role at the time?

24 Q Yeah.

25 A Probably once a quarter, roughly. So four times a year -- I'm

1 generalizing -- maybe more. Maybe eight. It might be four.

2 Q As the financial sector liaison, how are the responsibilities that you had
3 similar or different to the role of the Office of Private Sector?

4 A Yeah, so the Office of Private Sector, they have more of an overarching
5 engagement role to the private sector. There -- think of them -- I generalize here, but
6 Office of Private Sector would be more of the C-suite engagement at kind of the
7 wide-scoped C-suite engagement kind of level. We do a lot of information sharing that
8 reaches unclass levels. You mentioned LIR, and you mentioned LIR. There are a
9 number of things that they would share from OPS whereas, at the Counterterrorism
10 Division level and other operational divisions, that engagement is to support operations.
11 So that engagement is direct to support operations and to share information on the
12 threat.

13 Q So you would say your work is more granular?

14 A Yeah, I mean, in a general sense, you could say that, but the Office of Private
15 Sector's work is no less important than ours. It just serves a different function.

16 Q Okay.

17

BY [REDACTED]

18 Q And when did your engagement with the FBI's investigation into the events
19 that occurred at the Capitol on January 6th, 2021, begin?

20 A I couldn't tell you the exact time, but it was immediately after the Capitol
21 riots.

22 Q And how did that engagement start?

23 A It just -- after the Capitol riots happened, there were -- obviously, there was
24 a large number of individuals that took part in violent, criminal behavior, and that, within
25 the first 24 hours -- and I'm generalizing here -- I believe that the Counterterrorism

1 Division had taken the lead knowing that there was some suspicion of domestic violent
2 extremist activity -- obviously not limited to that because there was other criminal
3 behavior. In that whole Capitol riots investigation, there were a lot of people there that
4 day. So the Counterterrorism Division started to get leads in on, you know, perpetrators
5 of the criminal behavior of the violent criminal behavior.

6 Q And which division did you have an understanding was leading the FBI's
7 investigation into the January 6th matter?

8 A I mean, there was a general sense -- at my level, there was a general sense
9 that the Counterterrorism Division would play at least a lead role at the time of the outset
10 of it. But, again, you know, oftentimes, you can see that there are, you know, violent
11 attacks that weren't maybe as large as the Capitol riots that turn into, say, like a Criminal
12 Division investigation. And it would remain with a Criminal Division, you know, squad in
13 the field depending on where the threat emanated from. So, in this particular case, we
14 knew Counterterrorism Division was at least one of, if not the lead, in the Capitol riots
15 investigation.

16 Q During your engagement on the January 6th investigation, did you interact
17 with the Washington Field Office at all?

18 A I did, not at the onset. I believe probably within the first 2 weeks. I don't
19 think we -- I don't think I interacted with the Washington Field Office in the first 2 or
20 3 days. But, again, it's possible I did, but you have to remember that, hours after and
21 then a day after and 2 days after, Counterterrorism Division is being flooded with leads,
22 tips and leads, calls with financial institutions. They want to know what's going on. So
23 there was a lot of triaging, as you might imagine, that happens on large events like that.
24 So it's possible I could have spoken to them within the first few days, but I believe that I
25 spoke to them probably like more like 2 weeks after.

1 Q And what was your specific role in the investigation? Were you tasked with
2 doing anything?

3 A No, just to receive information, triage information, review information that
4 internally that we were receiving on investigations, determining what deserved priority,
5 what we should be sharing with the institutions versus, you know, some of the internal
6 communication that our unit would be doing with the other operational units.

7 Q And when did you start sharing information with financial institutions?

8 A Well, I believe the -- I believe the first -- I believe this is the case that the
9 Financial Crimes Enforcement Network the Friday after the Capitol riots asked
10 Counterterrorism Division to jump on a call with them on Friday afternoon. It was an ad
11 hoc meeting. And I was told by my upper management to represent Counterterrorism
12 Division on the call.

13 Q And your upper management being which title or which role was that
14 individual?

15 A Unit chief and section chief.

16 Q And you were to represent the whole Counterterrorism Division on that call.
17 Is that correct?

18 A Yeah. That was my understanding, yes.

19 Q Okay.

20 [REDACTED] Following the events at the Capitol on January 6th, are you aware
21 of communications between FBI and Bank of America?

22 Mr. Sullivan. Yes.

23 [REDACTED] I would now like to enter in two emails from Peter Sullivan to
24 Bank of America, both dated January 15th, 2021, with the subject line, "Upcoming SAR
25 product idea/brainstorming and check-in with you both" into the record as exhibit 1.

1 [Sullivan Exhibit No. 1.

2 Was marked for identification.]

3 [REDACTED] Can you confirm that you sent these emails?

4 Mr. Sullivan. Yes.

5 [REDACTED] I will just note for the record that these documents were produced
6 to the committee from Bank of America. And you will see at the bottom the Bates
7 stamp indicate that it came from Bank of America. I just wanted to make sure you knew
8 where there was coming from, but please take a moment to review.

9 Mr. Sullivan. Yeah. I'm familiar.

10 BY [REDACTED]

11 Q Is this the first email correspondence you had with Bank of America directly
12 following January 6th?

13 A I don't know if it was the first, but it's certainly -- on the 15th. I don't know
14 if it was the first. I would be surprised if it was the first, but I also wouldn't be surprised
15 if it was the first. Because I spoke with a lot of financial institutions this week, the week
16 following, and the weeks following that. But this is my email to them for sure. Both.

17 Q The second email states that you and Bank of America had a phone call
18 before you sent the email. Do you remember that phone call?

19 A Yes.

20 Q And?

21 A I had two phone calls actually. So there was a phone call that occurred
22 before, before the email on the 15th and then a phone call that occurred before the email
23 on the 15th that went out at 12:40, the second one that you showed me.

24 Q And what did you discuss on those calls?

25 A The Bank of America representative who I knew who I knew was on the

1 FinCEN call that was invited by FinCEN to participate in a Friday call were not the two
2 people that that individual wanted me to speak with. It was my understanding, through
3 the phone call, before this email that that individual from Bank of America who has also
4 held a supervisory role wanted me to get with the two individuals on the email that I sent
5 at 9:56 on the 15th.

6 Q And so, on the second phone call, what was discussed?

7 A A lot of what you see in the email was discussed. A lot of what you see in
8 the email, I can't say exclusively, is what I discussed on the FinCEN call, the Friday before.
9 But a lot of the fact-based pattern indicators where FinCEN asked us to discuss different
10 fact-based patterns that would help institutions look at their data, review their data for
11 anything worth things that would help the institutions understand if they had any threats
12 that may help cover down on the threat to Inauguration Day.

13 Q So you reached out to these two individuals from Bank of America as a result
14 of a Bank of America individual on the FinCEN call reaching out to you?

15 A Say that again, I'm sorry?

16 Q Well, I'm trying to follow, when you reached out to Bank of America on the
17 first email, why did you reach out to them?

18 A Because of the phone call that I had with one of the two individuals on the
19 attention line, the one I sent on 9:56 a.m., she was privy to getting a heads up from the
20 individual that was on the FinCEN call the Friday before that FinCEN asked me to jump on.
21 And that discussion was, "Yeah, let's touch base." So this was me following up that
22 phone call and touching base.

23 Q And that --

24 A And, adding other executive onto the email, which was also discussed on the
25 phone call.

1 Q And she was privy to what?

2 A The fact that one of her colleagues at --

3 Q Bank of America?

4 A Yes. One of her colleagues at Bank of America had sat in on the financial
5 crimes enforcement call to discuss the threat to Inauguration Day.

6

BY [REDACTED]

7 Q When you say do you have time this morning to discuss SARs and a couple of
8 ideas, what did you mean by a couple ideas?

9 A That would just be me informally just saying, you know, brainstorming,
10 which I often did with all financial institutions.

11 Q You said brainstorming. Is that correct?

12 A Yes.

13 Q And, when you were brainstorming, was that information you could share
14 with Bank of America, or was that information that Bank of America can share with the
15 FBI?

16 A Yeah, and any time that we would be brainstorming over the phone or on a
17 Teams call or any other medium, it would be unclassified information that I could share
18 with them.

19 Q Okay. So, when you said you have couple of ideas, that was information
20 going to Bank of America, in your mind?

21 A Yeah, just to talk about the threat.

22 Chairman Jordan. Do you know what the subject line means? You say,
23 "Upcoming SAR product idea/brainstorming and check-in with you both." Were you
24 suggesting to them information that you wanted from them?

25 Mr. Sullivan. No, I mean, if anything, oftentimes, you know, unlike the other

1 set -- there were a lot of other sectors that don't have SAR provisions as part of their
2 regulatory regime. So, oftentimes, I may say SAR product idea because I know that's
3 primarily what medium they would have if they found something that met a SAR
4 threshold, it would be a SAR. It wouldn't be something else. In other words, for this
5 particular email, the discussion wasn't going to discuss -- which I sent various other emails
6 that actually discussed this, would be expediting subpoenas or something that was on the
7 proactive side from the Bureau trying to get information that was also through a lawful
8 purpose. In this particular case, because I work with all banks and all nonbank financial
9 institutions that have SAR reporting obligations, this is just me generalizing in terms of
10 what may come if, in fact, they met SAR thresholds for those brainstorming. If they
11 didn't, then I wouldn't get a SAR.

12 Chairman Jordan. Maybe I don't fully appreciate -- understand how SAR works
13 then. The banks are required to give certain information, SARs, is the, you know, how
14 it's done is my understanding. So you said earlier there are millions sent to whatever
15 number you use, some number, sent to the government.

16 Mr. Sullivan. FinCEN.

17 Chairman Jordan. FinCEN. But I guess when I read this subject line, it's almost
18 like you're saying, "Hey, this is information, or this is the kind of SAR." -- I am just not
19 fully understanding this subject line. Because it looks like you are the one trying to
20 initiate what should go in this and when this report should come.

21 Mr. Sullivan. No.

22 Chairman Jordan. Okay.

23 Mr. Sullivan. No. I mean, if a SAR came from it, again, I would go back to -- you
24 know, my engagement was not just with Bank of America. My engagement was with all
25 finance sector. And so that covered banks, fintech, it covered neo banks,

1 cryptocurrency, I mean, you name it.

2 Chairman Jordan. So what does that mean, "Upcoming SAR product idea"?
3 What was the idea that you shared with.

4 Mr. Sullivan. No, I think, in general, institutions on the call, FinCEN relayed, you
5 know, the Bureau could potentially assist in helping the financial institutions understand
6 how to look at that threat. Obviously, with the Capitol riots, when you look at it from an
7 event and from a crime scene, obviously, there are a lot of lawful citizens there to
8 participate, and there are a lot of people that participated in criminal violent activity.
9 So, from a kind of a larger investigation standpoint, knowing on the FinCEN call what was
10 specifically discussed was FinCEN wanted the institutions to hear how might they go
11 about understanding what the potential threat to Inauguration Day was.

12

BY [REDACTED]

13 Q And, if you flip to next page of exhibit 1, there is that followup email that
14 we've discussed that looks like you sent this first email, you had a call, and then you sent
15 this followup email that identified threshold. Were these thresholds discussed on the
16 call?

17 A On the call, and many of these were discussed on the FinCEN call.

18 Q And who came up with these thresholds?

19 A I mean, I certainly came up with some of the thresholds in terms of
20 fact-based patterns that would help them narrow their focus. Meaning, in and of
21 themselves, none of these indicators were discussed either on the FinCEN call or my
22 followup calls with Bank of America or any other institution, that, in and of themselves,
23 they could put, you know, they could narrow their focus by just one of those indicators.
24 It was specifically discussed that these fact-based patterns would be looked at collectively
25 in order for the institutions to actually find out whether or not they can narrow their

1 focus enough.

2 Q And so did all of the thresholds that were mentioned here in the bullet
3 points, did those all have to be met, or was it just one?

4 A That was the assumption. How the bank, however, whether or not they
5 felt they met threshold for SARs, that would be exclusively up to them.

6 Q So do you know how Bank of America interpreted these thresholds? Was it
7 all of these thresholds had to be met or just one?

8 A That was my understanding.

9 Q It was your understanding that Bank of America thought all of these
10 thresholds had to be met in order for someone to be included in the SAR?

11 A In order for them to narrow their focus or to understand whether or not that
12 focus with all factors present, along with any other activities they saw, right, because we
13 don't have access to their duty, if collectively those met SAR thresholds, then I knew that
14 potentially I would get that in the form of a SAR because financial institutions have BSA
15 SAR reporting thresholds that they can use.

16 Q So it's your understanding that Bank of America, in looking through their
17 customer data, would have to with look to see whether purchases were made in the
18 Washington, D.C., area between the 5th and the 6th and then, subsequent to that,
19 reservations were made at a hotel or Airbnb for the day before or during the
20 inauguration, just to name the first few.

21 [REDACTED] I'm sorry; are you asking his understanding or Bank of America's
22 understanding of it?

23 BY [REDACTED]

24 Q His understanding, and then we can take it both.

25 A Yes.

1 Q So that was your understanding. And do you know if Bank of America
2 understood it that way?

3 A I assume they did because I discussed -- I had frequent interaction with both
4 individuals that I was on the call with.

5 Q And then, looking at the SAR that Bank of America filed with FinCEN and
6 others -- there's other emails I am sure we'll get into in a later hour where they send the
7 filing to you, did you look at that filing?

8 A Once it was published to FinCEN, I believe I did receive it in the secure email
9 portal, yes.

10 Q And did Bank of America's production of the SAR and information that was in
11 the SAR, did it correlate with these thresholds?

12 A It did.

13 Q And it correlated with the understanding that all of the thresholds needed to
14 be met?

15 A That's the way that I read the SAR narrative.

16 Q Okay.

17 Chairman Jordan. Do you recall how many individuals then were identified in
18 that SAR?

19 Mr. Sullivan. My recollection is that there were 211 individuals that met the
20 three thresholds that you can see within the email.

21 Chairman Jordan. So, backing up, when you said, the subject line both in this
22 email and the prior email, "Upcoming SAR production idea," then the production idea was
23 you produce a SAR if these three elements are met. Is that fair?

24 Mr. Sullivan. When you say "production idea," I mean, again, this is me -- that
25 subject line is a generalization of what I brainstorm and share information and concepts

1 with financial institutions all the time.

2 Chairman Jordan. So it's a subject line you use all the time?

3 Mr. Sullivan. I mean, it would be similar to a subject line that I might use for --

4 Chairman Jordan. Fair enough, but I guess I'm asking --

5 Mr. Sullivan. -- it, but the Capitol riots is a very unique situation, so, but I can't --

6 Chairman Jordan. Fair enough. But I'm asking -- you said, you recommended
7 like produce a SAR that has these -- if anyone -- the individual with these three elements
8 would be in a suspicious activity report that you would send to the government?

1 [11:00 a.m.]

2 Mr. Sullivan. I didn't say it produced a SAR, if that's what you're inferring. I
3 didn't tell the bank to produce a SAR. And they know that I would never tell them to
4 produce a SAR either.

5 Chairman Jordan. Okay, fine. I just want to make sure I understand.
6 Upcoming SAR product --

7 Mr. Sullivan. Uh-huh.

8 Chairman Jordan. -- and then you outlined three criteria that should be met, and
9 if so, you received a SAR that identified 211 people. That's what happened, right?

10 Mr. Sullivan. I received a SAR that had 211 individuals that met the three
11 fact-based patterns that --

12 Chairman Jordan. That you outlined to the bank?

13 Mr. Sullivan. That I discussed with the bank.

14 Chairman Jordan. Okay.

15 [REDACTED] And with the 211 --

16 Mr. Sullivan. This wasn't a one-way conversation. Sorry. I want to make that
17 clear. It was never a one-way conversation in any capacity when I discussed these types
18 of brainstorming ideas after a threat occurred with not just Bank of America, but any
19 institution.

20 Chairman Jordan. Understand. But you sent this email to Bank of America with
21 the subject line we've now discussed at length, with these three criteria having to be met,
22 and then subsequent to that, you received a SAR with 211 Americans' names on it that
23 met those three criteria?

24 Mr. Sullivan. That met those three criteria, correct.

25 Chairman Jordan. Okay.

1

BY [REDACTED]

2

3

4

Q And once the FBI received the SAR after it was posted on the FinCEN portal and it identified the 211 individuals that met the thresholds, what did the FBI do with that information?

5

6

7

8

9

A So I reviewed the SAR first. I reviewed the narrative. I verified that the fact-based patterns were present, and I did -- either I requested or I was able to get the supporting documentation once the SAR was published, so that I could see how they pieced out. I don't know if you guys have read the -- if you've read the SAR. My understanding is that you have.

10

Q Uh-huh.

11

12

13

14

15

16

17

A To understand, within -- they had tabs within the supporting documentation. So I wanted to make sure that I understood the SAR narrative and the supporting documentation, because once I review the SAR narrative in its entirety, I knew at a minimum -- again, at a minimum -- there was a question that I needed to ask regarding one of the fact-based patterns that I wanted headquarters to be able to -- my office to then further review and determine if there was an assessment that we needed to push out to respective field offices.

18

Q And what was that question that you needed answered?

19

20

21

22

23

24

A I called Bank of America and I wanted to understand, within the fact-based patterns that they had down as weapons purchases since July, I wanted to know, of the fact-based patterns that were met, which of those weapons purchases were -- and, again, I can't stress this enough, weapons-related transactions -- which of those transactions, from a data standpoint, was made after the Capitol riots, after Jan. 6th and before what would be inauguration day and beyond.

25

So once I received the clarification on the supporting documentation within those

1 211 customers, I was -- I received the information that four individuals of the 211 met
2 that threshold that made weapons-related transactions after the 6th.

3 And so I remember going to my supervisor and saying, we should push out these
4 four, do baseline queries of these four, which are basic criminal background queries, and
5 push out via assessment -- it's called a Guardian. A Guardian is a no-stone-unturned
6 assessment. It's not an investigation. But we pushed those four guardians out to
7 three field offices, respectively.

8 Q And do you remember what field offices those were?

9 A Memphis, San Francisco, and Tampa.

10 Q And with the other, you know, 211 individuals as a whole, what action did
11 the FBI take on that information beyond just requesting information on firearm purchases
12 after the 6th?

13 A I can only speak generally --

14 Q Okay.

15 A -- to your question. I know that the information -- the four Guardians that
16 we did to three field offices, once the Guardians went out, we uploaded the four
17 Guardian references to what's called electronic communication, and that electronic
18 communication also included the case file for our internal unit, as well as the WFO case
19 file on the Capitol riots because Washington Field Office had the lead on the Capitol riots
20 investigation. And it's practice that if your Guardians that you're pushing out, either at
21 the headquarters level or at the field office level, that you would include a case file that's
22 related or linked to an open investigation. In this case, WFO had the case file, so we
23 uploaded the four Guardians in reference to the SAR for Washington Field Office.

24 From there, I know Washington Field Office had a number of leads that were sent.
25 I can't speak to the decisionmaking in those leads, and so you would have to ask

1 Washington Field Office about those.

2 There were a number of -- so ours, to be clear, ours was the four Guardians, and
3 there were a number of leads and a handful of Guardians that also went out that my unit
4 did not handle.

5 [REDACTED] Did you know that at the time?

6 Mr. Sullivan. No, I did not.

7 [REDACTED] We're at our hour, so we'll go off the record.

8 [Recess.]

9 [REDACTED] Okay. We can go back on the record.

10 EXAMINATION

11

BY [REDACTED]

12 Q Mr. Sullivan, thanks again for appearing here today. I'm going to step back
13 and ask some pretty general background questions.

14 You have been with the FBI for 25 years now?

15 A Yes.

16 Q And have you received any awards or recognition during your service?

17 A Yeah, many awards, time-off awards, of course, for priority foreign
18 counterintelligence investigations, including Robert Hanssen, the Stanislav Gusev case,
19 the Russian spy case, Anwar Awlaki. And I was nominated for the Director's Award. I
20 didn't receive it, but I was nominated in 2008 for a Southeast Asia case linked to a San
21 Jose material support sibling that was sending money over to his then famous
22 bomb-making brother over in the Philippines.

23 Q And when you say "material support," you mean material support for
24 terrorism?

25 A Correct.

1 Q That's the shorthand?

2 A Correct. And just, you know, other -- I did receive a Mission Integration
3 Award from the Office of Director of National Intelligence prior to returning back to
4 Counterterrorism Division and my role for the Strategic Engagement Unit.

5 Q And what was that award for?

6 A That was for mission integration. I took the lead, with other three-letter
7 agencies, to help enhance the policy and the intelligence footprint on a specific type of
8 national security threat.

9 Q I believe you stated in the earlier hour that you've worked about half of your
10 25-year career in the field of financial intelligence, correct?

11 A Yes.

12 Q Can you describe what that means exactly, what intelligence means,
13 generally and specifically, what financial intelligence means?

14 A Sure. I mean, intelligence drives operations. You know, the FBI receives
15 over half of its tips and leads from private sector and foreign partners. And intelligence
16 comes in various forms. It's not just one type. There are several intelligence
17 disciplines where we receive intelligence. There's also tactical and operational
18 intelligence that a tactical analyst or an investigator, FBI agent, would get through, you
19 know, various means, whether commercial databases.

20 In the intelligence realm that I worked in, you know, of course there's the
21 classified intelligence you're getting from other collection platforms within the intel
22 community and the law enforcement community, law enforcement sensitive level. And
23 integrating that intelligence is what continues to drive and support operations, certainly
24 within the threats.

25 Primarily, my career has been in the Counterterrorism Division, so it's been for

1 supporting terrorist threats and terrorist operations and covering down on those, but not
2 limited to that.

3 Q Can you explain how specifically financial intelligence helps in
4 counterterrorism efforts? How does it help keep Americans safe?

5 A Yeah. I mean, it's one of many different aspects of how a terrorist might
6 acquire, move, store money in order to carry out an attack. And in another tactical very
7 basic sense, financial intelligence can illuminate a lot of deliberate information where that
8 person pattern -- it could tell pattern of life. It could understand, you know,
9 transactions that could indicate potential violent activity. It could highlight how a
10 terrorist might, you know, move their money in order to, you know, to support their daily
11 expense.

12 If you're looking at a network, finances can tell a lot about who's connected to
13 that network. But it's one of many. It's just -- but I believe it remains a critical piece of
14 looking at terrorism.

15 Q And is it fair to say that one of the critical pieces of that is that financial
16 intelligence can help you identify who might be a terrorist, whether it's an international
17 or domestic terrorist --

18 A Yes.

19 Q -- based on the nature of their purchases --

20 A Absolutely.

21 Q -- or their activities?

22 So I want to step back a minute and just talk about the FBI's mission generally.

23 The primary mission of the FBI is to protect the American people and uphold the
24 Constitution of the United States. Is that correct?

25 A Correct.

1 Q And protecting the United States from terrorist attacks is the top priority of
2 the FBI?

3 A Yes.

4 Q And does that include attacks by domestic terrorists?

5 A Yes.

6 Q And so the counterterrorism work of the FBI is really fundamental to what
7 the FBI is here to do in the United States, to protect Americans and keep us safe?

8 A Absolutely.

9 Q Are you familiar with the term "domestic violent extremism"?

10 A Yes.

11 Q Okay. And that's often abbreviated as DVE?

12 A Uh-huh. Yes.

13 Q And I believe you mentioned that earlier. So any time I use that phrase,
14 that's what I'm referring to.

15 A Okay.

16 Q Are you familiar with how the FBI defines domestic violent extremism?
17 How do you define it?

18 A Yeah. Generally, it's a terrorist that, basically, that has to satisfy three
19 different caveats. It would be that there is the -- some sort of ideology -- terrorist
20 ideology involved, that there's a violent aspect that's involved or an intent to use
21 violence, and that there's some sort of criminal activity present, obviously terrorist or
22 otherwise.

23 Q And so when you say there's an ideological component, the ideology itself is
24 not what would have somebody labeled as a domestic violent extremist --

25 A Correct.

1 Q -- correct?

2 A Yeah. All three would be required in order for even an investigation to be
3 opened up.

4 Q So it's essentially someone -- it would be fair to say that it refers to
5 somebody who wants to use -- threatens violence or actually uses violence to further
6 their ideological goals?

7 A Yeah. Violence is the -- really the linchpin of that, of the three.

8 Q And so the mere advocacy of a particular political or social position using
9 strong rhetoric, even just sort of a philosophic embrace of violent tactics is not enough,
10 correct?

11 A Correct.

12 Q There has to be more, there has to be the actual official threat of violence or
13 actual violence?

14 A Uh-huh.

15 Q May I have a moment?

16 And in the domestic context we're talking about folks who are operating primarily
17 in the United States, if you're talking about a domestic violence extremist, correct?

18 A In most cases, yes.

19 Q Can you describe the current landscape in the United States with respect to
20 DVEs and what you're seeing, the nature of the threats they pose? Is it on the rise?
21 What are you seeing?

22 A Sure. Yeah, I can speak generally to it just because I'm not an all-source
23 analyst in the domestic terrorist -- you know, I'm not a domestic terrorist --

24 Q Fair enough.

25 A -- analyst. But in terms of my previous engagement looking at data related

1 to domestic violent extremists, I know that within the Counterterrorism Division, I know
2 during the social unrest leading up to the Capitol riots and since then, you're talking
3 about more than doubling of the cases within Counterterrorism Division that have been
4 opened at the time.

5 Q And I imagine you've seen a real spectrum of activity. For example, lone
6 actors committing acts of domestic extremism, correct?

7 A Yes.

8 Q And then also folks who mobilize in groups, correct?

9 A Yes. However, I would caveat that to say that State Department designates
10 foreign terrorist organizations so that opening investigations on international terrorism is
11 much easier.

12 The challenge is -- on the domestic terrorist side is, because there is no such thing
13 as a domestic terrorist group -- and you have to have those three factors that I mentioned
14 present -- the challenges to identifying networks are much greater than if you were
15 investigating it on the IT side.

16 Q So separate and apart from formal networks -- and by the way, "IT" you
17 mean international terrorism?

18 A International terrorism. Sorry about that.

19 Q That's okay.

20 Separate from the concept of a formal domestic terrorist organization, the FBI has
21 seen groups of people mobilize online through social media, for example, to act together
22 or at least talk about acting together to commit acts of violence to promote certain
23 ideologies.

24 A Yes.

25 Q Is that fair to say?

1 A Yes.

2 Q And would you agree that domestic violence extremists have a large
3 presence on the internet?

4 A Yes.

5 Q And that social media platforms and messaging platforms facilitate the
6 ability of these folks to radicalize and recruit individuals who might be receptive to their
7 message?

8 A Yes. Generally, yes.

9 Q And do you -- this might seem like a silly question, but it's something that I
10 have to ask because it seems there's some dispute about this. Do you believe that the
11 FBI should be devoting resources to identifying domestic terrorists and preventing
12 Americans from dying at their hands?

13 A Oh, I think that the FBI is dedicating resources to that.

14 Q And you believe that's an appropriate deployment of the FBI's resources?

15 A Well, you have to understand the Bureau. FBI's budget covers a myriad of
16 threats, all of which are priorities. National security threats aren't just within the
17 Counterterrorism Division, but they are in cyber, counterintelligence, and there are some
18 threats in the Criminal Investigative Division that are also national security threats.

19 So when you're talking about national security, I think that, in general, we don't
20 have enough resources to cover down on all threats, but I think that the response that
21 Counterterrorism Division has had on the domestic terrorist threat has been generally
22 appropriate.

23 Q You believe it's been proportional to the nature of the threat to the extent
24 possible with the resources you have?

25 A It has grown enough in the emphasis at the headquarters level that I've seen

1 has been dedicated to that growth.

2 Q Okay. Thank you.

3 Are you familiar with the Domestic Investigations and Operations Guide?

4 A Yes. Generally, yeah.

5 Q It's also referred to as the DIOG?

6 A Yes.

7 Q And the DIOG applies to all FBI employees and all other individuals operating
8 under the FBI's authority --

9 A Correct.

10 Q -- correct?

11 And it applies to all domestic intelligence activities conducted by the FBI?

12 A Correct.

13 Q And all of your work is covered by the DIOG?

14 A Yes.

15 Q And the DIOG is meant to ensure that the criminal and national security and
16 foreign intelligence investigative activities are consistent throughout the FBI?

17 A Correct.

18 Q Okay. I'd like to introduce an excerpt from section 3.1 of the public version
19 of the DIOG.

20 [REDACTED] And just to note for the record, the version we're introducing I think
21 is a year or two old. It's the non- -- I know part of the DIOG is currently
22 law-enforcement sensitive. We don't have access to that. This is the version that's
23 made to be publicly available that we're introducing.

24 [REDACTED] Okay.

25

[Sullivan Exhibit No. 2.]

1 was marked for identification.]

2 [REDACTED] And you can see it says "unclassified" on the bottom.

3

BY [REDACTED]

4 Q Okay. So section 3.1 starts by listing the core values of the FBI. And I'm
5 just going to read them into the record, and you can tell me if I read this correctly.

6 The first is rigorous obedience to the Constitution of the United States. The
7 second is respect for the dignity of all those we protect. The third is compassion. The
8 fourth is fairness. The fifth is uncompromising personal integrity and institutional
9 integrity. The sixth is accountability by accepting responsibility for our actions and
10 decisions and their consequences. The sixth (sic) is leadership, by example, both
11 personal and professional. And the seventh (sic) is diversity.

12 Did I read that correctly?

13 A Yes.

14 Q And are you familiar with these core values?

15 A Yes.

16 Q And through your 25 years at the FBI, have you worked to ensure that all of
17 your actions have adhered to those core values?

18 A Yes.

19 Q And have you witnessed a similar commitment from your colleagues at the
20 FBI?

21 A Yes.

22 Q And from FBI management as well?

23 A Yes.

24 [REDACTED] Mr. Sullivan, can I just ask you to speak up so the people at the end
25 of --

1 Mr. Sullivan. Yeah.

2 [REDACTED] -- the table can hear you.

3 Mr. Sullivan. Sure.

4 [REDACTED] Okay.

5 BY [REDACTED]

6 Q Now, the second sentence of the first paragraph underneath the core values
7 says, "Our individual and institutional rigorous obedience to constitutional principles and
8 guarantees is more important than the outcome of any single interview, search for
9 evidence, or investigation."

10 Do you agree with that sentence?

11 A Yes.

12 Q Okay. And is it fair to say that that means your goal in any one case or
13 situation cannot override your obedience to the Constitution and the other laws that
14 guide the FBI?

15 A Yes.

16 Q And that applies even if you're involving terrorism or domestic violence
17 extremism?

18 A Yes.

19 Q Now, you mentioned in the earlier hour, I believe you stated the mission of
20 the Strategic Engagement Unit, but I'd ask you to repeat it because I'm not quite sure I
21 caught it.

22 A Yeah. The mission of the engagement unit was to basically cultivate and
23 share information on core terrorist threats with the ability to help the private sector
24 understand the threats and help push out information that may be relevant to law
25 enforcement and support operations.

1 Q And operations with respect to terrorism -- counterterrorism?

2 A Correct.

3 Q Okay. So SEU is specifically about counterterrorism?

4 A It is. And we handled some leads that we would facilitate or push
5 information within other divisions.

6 Q And I believe you said that sometimes the people you knew at the banks
7 would send you leads on other issues because they knew that you would send them --

8 A Get it to the right person.

9 Q -- to the right people?

10 A Correct.

11 Q Are you familiar with the term "National Security Special Event"?

12 A Yes. Generally, yes.

13 Q Okay. What is your understanding of what a National Security
14 Special Event is?

15 A Yeah, a large event that is either -- oftentimes sees potential criminal activity
16 around it, so Super Bowl, other types of events. It could be something like the Capitol
17 riots or 9/11, that type of thing.

18 Q And would the Presidential inauguration fall under the category --

19 A Yes.

20 Q -- of a National Security Special Event?

21 A Yes.

22 Q I'd like to introduce a letter, January 31st of this year, and this is a letter
23 from Assistant Director Patrick Findlay to Chairman Jordan. And I'm not sure if you've
24 seen this, but you can take a few minutes to read it.

25 [REDACTED] Oh, of the FBI, correct?

1 [Sullivan Exhibit No. 3.

2 was marked for identification.]

3 [REDACTED] And Mr. Findlay is the assistant director -- FBI's assistant director for
4 congressional affairs.

5 [REDACTED] Oh, sorry. Thank you.

6 Mr. Sullivan. Yes, I've seen this.

7

BY [REDACTED]

8 Q Okay. So if you look at the second paragraph about midway through, it
9 says, "For NSSEs" -- which is the abbreviation for National Security Special Event -- "such
10 as an inauguration, the Super Bowl, or the Olympics, the FBI has designated responsibility
11 for domestic intelligence, counterterrorism, and the investigation of Federal crimes
12 leading into an event."

13 That's correct, I take it?

14 A Yes.

15 Q And that's your understanding?

16 A Yes, that's my understanding.

17 Q And, "Such events represent significant targets for a variety of criminal or
18 national security threats, and the FBI relies heavily on cooperation and coordination with
19 a variety of stakeholders to protect lives and security."

20 Do you agree with that statement as well?

21 A Yes.

22 Q The letter goes on to say, in the third paragraph, that, "The Strategic Partner
23 Engagement Section" -- which Chairman Jordan referenced in his letter to the FBI -- "can
24 play an important role in advance of NSSEs by developing proactive initiatives with key
25 interagency, public and private sector partners in furtherance of developing actionable

1 intelligence which can be leveraged to enhance threat mitigation and preventive
2 strategies."

3 Do you agree with that statement?

4 A Yes.

5 Q And does that statement characterize what your efforts were in the wake of
6 January 6th?

7 A Yeah. Generally, yes.

8 Q And then the letter goes on to say, "As part of this work, the Strategic
9 Partner Engagement Section partners with financial institutions in their effort to
10 safeguard the United States from the abuses of financial crime, including money
11 laundering, terrorist financing, and other illicit transactions."

12 Would you agree with that?

13 A Yes.

14 Q Okay. Now, banks are not required to work with SEU, correct?

15 A They're obligated to report suspicious activity. So knowing that suspicious
16 activity is almost exclusively in the hands of law enforcement agencies, to include the FBI,
17 not limited to the FBI but to include them, oftentimes paralleling that, they themselves
18 have programs where they feel that engagement is required or necessary -- they,
19 themselves.

20 Q So they're required to report the activity, but they could choose to not
21 engage with you in terms of brainstorming ideas for how to identify that activity.

22 A Absolutely.

23 Q Is that fair to say?

24 A Sure.

25 Q They could just take their own understanding of what they're required to

1 report, their own interpretation, and send it through the portal and not have the --

2 A Correct.

3 Q -- the type of partnership that you describe?

4 A Correct.

5 Q And it's their choice to have those partnerships with you?

6 A Yes.

7 Q Okay. So I want to talk a little bit about the Bank Secrecy Act, and I assume
8 that any time you said "BSA," you're referring to the Bank Secrecy Act?

9 A Correct.

10 Q So if you take a look back at Assistant Director Findlay's letter on the second
11 page --

12 A Yeah.

13 Q -- in the first paragraph, it says, "The Bank Secrecy Act and its implementing
14 regulations provide for financial institutions to report information for use, quote, in
15 criminal, tax, or regulatory investigations, risk assessments and proceedings, end quote,
16 including reports on, again quotation marks, suspicious transactions relevant to a possible
17 violation of law or regulation."

18 Is that your understanding of the Bank Secrecy Act.

19 A Yes.

20 Q And if you look at the footnote in that letter, it actually cites the U.S. Code
21 provisions that constitute the Bank Secrecy Act, correct -- or that are referenced there?

22 A Yes.

23 Q And I believe that you touched on this in the earlier hour, but the letter goes
24 on to state that, "Suspicious Activity Reports, or SARs, are filed with FinCEN and made
25 available, under strict statutory and regulatory protections, to the FBI and other

1 authorized law enforcement, national security, and regulatory agencies."

2 And that's consistent with your understanding of SARs --

3 A Correct.

4 Q -- and their availability -- excuse me -- availability to the FBI?

5 A Correct.

6 Q And the letter then goes on to say, "The FBI understands that the BSA and its
7 implementing regulations require financial institutions to determine what activities and
8 transactions are deemed persistent to -- deemed suspicious pursuant to the BSA."

9 And, again, that's consistent with your understanding of what the Bank
10 Secrecy Act requires?

11 A Correct.

12 Q So the banks are obligated to file a Suspicious Activity Report for anything
13 that meets the thresholds set by regulation, correct?

14 A Correct.

15 Q And it's up to them, the banks, not you, to determine whether they see
16 information that meets those thresholds --

17 A Correct.

18 Q -- and to compile the report?

19 [REDACTED] All right. And if I could just ask you to let her finish the question
20 before you answer so we --

21 Mr. Sullivan. Sure.

22 [REDACTED] -- have a clean record.

23 Mr. Sullivan. Sorry.

24 BY [REDACTED]

25 Q And you indicated this earlier, but just to be clear, BSA data, including SARs,

1 is used across many types of criminal investigations in the FBI: money laundering,
2 organized crime, fraud, terrorism, drug trafficking. I mean, pretty much anything that
3 the FBI is investigating --

4 A Yes.

5 Q -- a SAR could be relevant to, correct?

6 A Yes.

7 Q Okay. And the FBI considers, as reflected in this letter, the preliminary and
8 unverified leads that you receive in SARs to be raw intelligence, correct?

9 A Yes.

10 Q And can you explain what that means? What does that phrase "raw
11 intelligence" mean?

12 A It's, you know, in any investigation, or if you're an analyst or an investigator,
13 raw intelligence would be all of the information that in and of itself may not be anything
14 but that helps you understand what is and isn't connected to the thing that you're looking
15 at.

16 So it could be -- raw information could be an informal tip from a private sector,
17 not even under the guidelines of the regulatory environment with BSA. SARs just
18 happened to be more formally regulated raw information. So there's -- raw information
19 could come in various forms.

20 Q Okay. Thank you.

21 And are there -- well, can you give us an example -- I know you've already
22 described several of the higher profile cases that you've worked on, but a case where a
23 SAR helped identify or prevent -- identify a perpetrator of a violent crime or helped
24 prevent one, can you think of a case?

25 A Yeah. In my mind of what's adjudicated, yes.

1 Q Yes. Thank you.

2 A So the FBI provided information regarding chemical precursors that could be
3 used for bomb-making materials and provided that information to -- the engagement unit
4 provided that information to a finance sector partner, who used that to set alerts within
5 their system, to understand, when they saw those transactions, what combination of
6 those chemical precursors were being purchased.

7 They -- obviously from a proactive standpoint, because they're setting the alerts
8 themselves on general chemical precursors in combination, they produced several SARs.
9 One SAR in particular looked like other SARs that had chemical precursor purchases in it.
10 The engagement unit reviewed it and decided that they were going to do a Guardian
11 assessment.

12 There's a terrorist explosive device -- they call it TEDAC -- down at Quantico that
13 verified our assessment that this should go to the field office. In this case, it was the
14 Chicago Field Office. The transactions for the chemical precursors, when Chicago
15 Field Office received the Guardian, they decided to go visit the consumer whose bank
16 account had made these transactions.

17 There was a husband and wife that lived there. When they asked them about
18 the transactions, they said, oh, that's our son, he's into science. And they asked if they
19 could see some of the things that, you know, he was into, and they agreed to a consented
20 search where FBI agents discovered elaborate plans for their son to carry out an attack at
21 his high school, using several pipe bombs, grenades, a backpack bomb that he, himself,
22 wrote down that it would kill between 12 and 20 people.

23 And they wound up arresting the person and -- the minor, and the case, you know,
24 obviously went from there, but that terrorist attack was prevented because of the SAR
25 that was published by the financial institution.

1 Q And if I understood what you just explained, the genesis for that SAR was the
2 Strategic Engagement Unit explaining to the banks what chemicals to look for because
3 the banks might not know that --

4 A Correct.

5 Q -- this combination of materials could be used to create a bomb?

6 A Correct.

7 Q And is that typical of the nature of the sort of advice and guidance that you
8 provide to your partners?

9 A Absolutely.

10 Q Okay. So even though the banks have their own -- they have their
11 reporting requirements, they might not know what transactions could be indicative of a
12 violent offense without the information provided to the FBI. I mean, sometimes I
13 imagine it's very obvious and other times --

14 A Yeah, correct.

15 Q -- it's --

16 A Yeah. I mean, I think the way that you characterize it is spot on. In some
17 cases they would know and they've already set up their alerts; in other cases, they would
18 use that law enforcement information to set their alerts.

19 Q And when the FBI receives any tip from a third party, including a SAR from a
20 financial institution, it has to take its own step to review that? It would conduct its own
21 review of that information, correct?

22 A Yes.

23 Q You don't open an investigation or send out a Guardian on every SAR that
24 comes in?

25 A Correct.

1 Q You have to go through a review process to determine if there is enough to
2 move forward with the initial steps of an investigation?

3 A Correct.

4 Q I want to step back a minute. We've talked a lot in the previous hour about
5 the events of January 6th. Can you describe, in your own words, what happened that
6 day?

7 A Yeah. You know, I would say, on that day there was a large gathering
8 outside the Capitol, and there were a number -- a large number of individuals that
9 decided to partake in violent, criminal activity, violence that was intended for not only
10 law enforcement but also threat of violence to a lot of the legislative branch members
11 that, you know, that I'm talking to today.

12 Q And you're aware that Director Wray has referred to the events of that day
13 as domestic terrorism -- acts of domestic terrorism?

14 A Yes.

15 Q And do you agree with that assessment?

16 A Yes.

17 Q And some of the participants in the riots that day displayed insignias that
18 have been used or adopted by DVEs, correct?

19 A Yes.

20 Q There were nooses and plastic restraints that were found at the Capitol or
21 stationed at or near the Capitol?

22 A Yes.

23 Q You're aware that people -- police officers were violently attacked, one was
24 killed that day?

25 A Yes.

1 Q People were chanting "Hang Mike Pence," correct, who was, of course, the
2 Vice President at the time?

3 A Yes. It's my understanding, yes.

4 Q So in the immediate aftermath of January 6th, you described the flood of
5 tips and the flood of activity. The FBI was concerned, I imagine, about preventing
6 further violence, whether on a smaller scale or a larger scale, that was fueled by the same
7 ideologies and motivations --

8 A Yes.

9 Q -- that appealed to the folks who overtook the Capitol on January 6th?

10 A Correct.

11 Q Okay. Now, the inauguration of then President-elect Biden was scheduled
12 for 2 weeks -- about 2 weeks after that day, correct?

13 A Correct.

14 Q And as you've stated earlier, inauguration is a National Security
15 Special Event. And so the FBI was tasked with preventing acts of terrorism and violence
16 at that event, correct?

17 A Correct.

18 Q And after January 6th, online rhetoric regarding violence during the
19 inauguration increased. Is that correct?

20 A Absolutely, yes, correct. That was my understanding.

21 Q And your understanding was the FBI was seeing people online talking about
22 mobilizing to participate in acts of violence at the inauguration?

23 A Correct.

24 Q Similar to what we saw on January 6th?

25 A Correct.

1 Q And would you agree that January 6th showed that there were many,
2 perhaps thousands, of people who were willing to break the law and use violence to
3 prevent the peaceful transfer of power --

4 A Yes.

5 Q -- at that time from one President to another?

6 A Yes.

7 Q And the inauguration is the moment where that actually happens, where
8 power is transferred from one President to another?

9 A Correct.

10 Q And the FBI had specific intelligence indicating that it was likely that people
11 intended -- who were present at January 6th -- intended to return to D.C. to commit acts
12 of violence at the inauguration, correct?

13 A At the time that was my understanding, yes.

14 Q Okay. If I could have the January 14th email. And this is exhibit 4, I
15 believe, we're at.

16 [Sullivan Exhibit No. 4.
17 was marked for identification.]

18 BY [REDACTED]

19 Q So this is an email sent on January 14th, 2021, from the DSAC portal. Can
20 you explain what that is?

21 A Yeah. The DSAC portal is open to all DSAC members. The Office of
22 Private Sector is the one that coordinates that portal, and DSAC members, a lot of it's
23 Fortune 500 and large companies are members of the portal. They have access, and
24 they would receive -- they would ostensibly receive production within that portal, this
25 being one of the products.

1 Q And "DSAC" stands for the Domestic Security Alliance Council?

2 A Correct.

3 Q And can you just describe briefly what that is and what the portal is?

4 A Again, it's Office of Private Sector's portal for communicating production
5 related to a gamut of threats. It wouldn't be limited to terrorism, but any threats that
6 are relevant to FBI and the FBI operational divisions.

7 Q Okay. And it's open to any private sector company that meets certain
8 thresholds, correct?

9 A Correct.

10 Q Based on their revenue and --

11 A Right.

12 Q -- that sort of thing?

13 And it has a public website, correct?

14 A Uh-huh, yes.

15 Q So I could go on, I can look and see who the members are and who the
16 leaders are, that sort of thing?

17 A Yeah. I haven't been on the site in a while, but I think generally, yes.

18 Q Now, according to this email, the subject line is, "Some Domestic Violent
19 Extremists Likely Will React With Violence to the Presidential Transition Process." That's
20 the subject line, correct?

21 A Yes. That's what I'm reading here, yes.

22 Q And the email indicates in the first paragraph that, "The FBI assesses some
23 domestic violence extremists, DVEs, including anti-government or anti-authority violent
24 extremists, specifically militia violent extremists, abbreviated as MVEs, are very likely to
25 attend alleged armed protests where they are likely to use violence in response to what

1 they perceive as the illegitimate transfer of power from the current President to a new
2 administration."

3 Did I read that correctly?

4 A Yes.

5 Q And the FBI made this assessment of the likelihood of violence at the
6 inauguration with high confidence based on FBI CHS reporting -- and that stands for
7 confidential human source, correct?

8 A Correct.

9 Q -- open source information and law enforcement information reporting calls
10 for violence, correct?

11 A Correct.

12 Q And then this email has some examples of some of those threats and some
13 of those sources. So if you look at the second example, there was a human source with
14 direct assets, and the last sentence says that that human source reported that DVEs
15 reportedly plan to storm government offices on 20th of January 2021, according to that
16 human source, correct?

17 A Correct.

18 Q And January 20th of 2021 was the day of the inauguration?

19 A Correct.

20 Q And if you look at a few lines down, it says, "As of 8th of January, multiple
21 social media postings promoted the 'Million Militia March' on 20th of January 2021, to
22 prevent the new President from entering the White House, according to law enforcement
23 information."

24 Is that correct?

25 A Correct.

1 Q So these are just some examples of the specific threats that the FBI had
2 identified to the inauguration?

3 A Correct.

4 Q And if someone were to bring, for example, a fully automatic firearm to the
5 inauguration, they could potentially kill thousands of people, correct?

6 A Ostensibly, correct.

7 Q Including the soon-to-be inaugurated or the immediately inaugurated
8 President and his family?

9 A Sure.

10 Q The Chief Justice of the Supreme Court who's administering the oath?

11 A Correct.

12 Q And as this document reflects, the FBI was concerned the violence could spill
13 over outside of Washington, D.C., to the rest of the country, correct?

14 A Correct.

15 Q And as the first paragraph of this email indicates, the FBI was concerned that
16 potential violence could result in a range of consequences, including the loss of life,
17 property damage, disruption of government operations, and the overwhelming of U.S.
18 local, State, and Federal law enforcement, correct?

19 A Correct.

20 Q And the FBI, including you and your colleagues at SEU, wanted to use all of
21 the tools at the FBI's disposal to prevent that from happening, correct?

22 A Correct.

23 Q And in fact, you had a duty, as part of a sworn officer of the FBI, to do
24 everything possible within the letter of the law to prevent that from happening, correct?

25 A Correct.

1 Q And would you agree that the events of January 6th demonstrated that the
2 threat posed by DVEs in this country was greater and more imminent than previously
3 understood?

4 A Yes.

5 Q And that the successful breach of the Capitol and the loss of life that ensued
6 brought home the urgency of the threat to our national security that DVEs posed?

7 A Correct.

8 Q Now, you mentioned FinCEN during the earlier hour. That's the Financial
9 Crimes Enforcement Network of the Treasury Department, correct?

10 A Correct.

11 Q And they were also tasked with trying to prevent an attack on the
12 inauguration?

13 A Correct. That was my understanding.

14 Q Okay. And you mentioned a call that you participated in on the Friday after
15 January 6th. Was that call about -- was it focused on threats to the inauguration?

16 A Yeah. I mean, summarize on the call. So when I was told by my upper
17 management to represent Counterterrorism Division on the call, as a FinCEN-sanctioned
18 call, the gist of the -- of what I discussed on it was, you had the Capitol riots, violent
19 criminal activity as an event, and you had the investigation of that, and then you had the
20 inauguration that was happening soon and the unknown threat to that. So there's
21 managing the threat, right, and also supporting investigation.

22 Q And the conversations that you had with the bank representatives that led
23 to the email that we talked about -- and we'll get to that in a minute -- those were
24 focused on the future threat to the inauguration?

25 A Correct.

1 Q And it was about the inauguration specifically?

2 A Correct.

3 Q Okay. And all of the methods that were discussed in those calls and in
4 those emails, in these post-January 6th communications that you had with the bank, all of
5 these were in compliance with the requirement for the Bank Secrecy Act, correct?

6 A Absolutely.

7 Q Now, going back to your email, which was exhibit 1, there was a lot of talk
8 during the previous hour about the subject line. But just to be clear, the -- well, let me
9 ask you, the nature of the conversations that you were having with these Bank of America
10 employees, were they in the same vein as the conversations that you described in that
11 chemical precursor investigation where you were helping to identify what they should be
12 look -- you know, what to keep an eye out for, what might indicate --

13 A Yes.

14 Q -- suspicious activity?

15 A Similar in the sense of discussing the threat, talking about the threat, yes.

16 Q It was --

17 [REDACTED] Sorry. Could we go off the record for 1 minute?

18 [REDACTED] Absolutely.

19 [Discussion off the record.]

20 [REDACTED] And so I just wanted to be clear --

21 [REDACTED] Back on the record.

22 [REDACTED] Oh, sorry. Back on the record. Thank you.

23

BY [REDACTED]

24 Q The full subject line of this email says, "Re, colon, upcoming SAR product
25 idea, slash, brainstorming and check-in with you both," correct?

1 A Correct.

2 Q It doesn't just say "upcoming SAR product." It's an idea?

3 A Correct.

4 Q You were talking about -- I mean, "brainstorming" is self-explanatory, but
5 essentially you were discussing with the bank employees things they might look for. But
6 you at no point directed them to file a SAR for anything that met these thresholds,
7 correct?

8 A Correct.

9 Q It was up to the banks to consider the information you gave them, review
10 their own data, and make their own determination about whether a SAR was appropriate
11 or required under the Bank Secrecy Act?

12 A Correct.

13 Q Now, just to be clear -- you stated this during the prior hour, but I want to
14 make sure that it is very clear -- in your mind -- and your understanding was that Bank of
15 America understood this -- all of the thresholds had to be met that were specified in this
16 email, correct?

17 A In order to help the bank narrow their focus, correct.

18 Q So you didn't tell the bank, anyone who made a purchase in Washington,
19 D.C. on January 5th or January 6th, that alone is enough, we're interested in that?

20 A Right, correct.

21 Q And a purchase of an Airbnb or a hotel reservation in the D.C. area for the
22 time of the inauguration, that wouldn't be enough --

23 A Correct.

24 Q -- correct?

25 And historical weapons or weapons-related purchase going back 6 months, that

1 would not be enough, correct?

2 A Correct.

3 Q It had to be all three?

4 A It had to be, correct.

5 Q And that was what you indicated to the banks?

6 A That's what we discussed.

7 Q That's what you discussed, correct?

8 A Yes.

9 Q And your understanding was that's what the banks understood?

10 A That's what the banks understood of capabilities, how to narrow their focus,
11 correct.

12 Q And to be clear, your email doesn't mention firearms specifically at all,
13 correct?

14 A Right.

15 Q Okay. It just talks about weapons generally?

16 A Correct. Because the financial institution would not necessarily, in most
17 cases, not only have information tied to the type of transaction.

18 Q And just at a higher level, you were hoping to identify people who were
19 present at the Capitol, participated in those violent acts, and intended to return and
20 commit more violent acts at the inauguration? That was the goal of these
21 conversations, correct?

22 A The end goal, correct.

23 [REDACTED] Can you explain -- the criteria that we just walked through, can you
24 explain your understanding of why these criteria would identify individuals who had
25 committed acts of violence -- or had been present at the Capitol intended to return to the

1 inauguration to commit acts of violence?

2 Mr. Sullivan. Well, first, just to clarify, not to commit acts of violence, but
3 potentially committed acts of violence. I mean, which do you want me to address? Do
4 you want me to just read it or --

5 [REDACTED] I'm thinking, you know, we've walked through what each one of the
6 criteria says on its face, but you've said over and over it was the combination of these
7 three together that were designed to help identify relevant individuals. Can you explain
8 your understanding of why that was?

9 Mr. Sullivan. Yeah. I would simply say that these are all just fact-based
10 patterns that would narrow the focus of anybody that was doing data exploitation,
11 whether you were in a bank or another institution that would have data relevant to being
12 able to look at those factors together at the same time.

13 [REDACTED] Thank you.

14 BY [REDACTED]

15 Q And according to your understanding of the Bank Secrecy Act, the
16 information that you provided to the banks and any information they would've presented
17 to you in response to that conversation, you do not need legal process for that, correct?

18 A If I was receiving something in a SAR, I knew that the institution made -- met
19 SAR thresholds. So once it's published into FinCEN, I am a law enforcement recipient
20 just like any other law enforcement agency that has access to the same data.

21 Q And so once they filed that SAR, you knew they had made their own
22 determination that it met that threshold?

23 A Correct.

24 Q Okay. So I want to talk a little bit about the SAR. We discussed it briefly,
25 and I know we don't have it here, but I think you'll be able to answer these questions.

1 First, I just want to make clear, the SAR indicated that there were 211 total
2 customer relationships that were identified that met the three thresholds that we
3 discussed, correct?

4 A Correct.

5 Q Now, I believe Chairman Jordan said that there was a list of 211 Americans,
6 but we don't know that they were all Americans, correct?

7 A No.

8 Q It could've been any --

9 A Correct.

10 Q -- foreign nationals who were doing business with the bank?

11 Yeah, it could've been business entities as well, correct.

12 A Correct.

13 Q Okay. And the SAR itself did not have a list of those names, correct?

14 A The SAR itself did not have a list of those names, correct.

15 Q Right. That was part of the supporting documentation that was referenced
16 in the SAR?

17 A That's correct.

18 Q And the SAR -- the supporting documentation was divided into three tabs,
19 correct?

20 A I think it was more than that. I think there were more tabs.

21 Q Okay. But the initial tab was everybody who met those first three criteria,
22 correct?

23 A Yes, I believe so. I think the last tab -- the last tab, from what I recall, had
24 all 211 on it.

25 Q Okay. Thank you.

1 And the way the bank -- and tell me if this comports with your
2 memory -- described those three criteria were, customers confirmed with transacting,
3 either through bank account debit card or credit card purchases in Washington, D.C.,
4 between January 5th and January 6th, 2021.

5 That's the first part of the threshold, correct?

6 A Correct.

7 Q And then purchases made for hotel, Airbnb, RSVPs in D.C., Virginia, and
8 Maryland since January 6th, 2021, correct?

9 A Correct.

10 Q And any historical purchase of weapons or at a weapons-related merchant
11 since July 15th, 2020, correct?

12 A Correct.

13 Q It wasn't ever in the history of time --

14 A Correct.

15 Q -- if you made a weapons purchase. It was limited by time?

16 A That was never discussed --

17 Q Okay.

18 A -- past that date.

19 Q And as you testified in the previous hour, you had follow-up conversations
20 where you wanted to identify individuals whose weapons-related purchases postdated
21 January 6th?

22 A Correct.

23 Q Okay. Can you explain why that was important to you?

24 A After reviewing the SAR and seeing that -- you know, knowing that 211
25 customers met the criteria, I knew that was still a very small amount when you look at

1 the -- when you compare it to the Bank of America's customer base. But my intent,
2 again, going back to the call from FinCEN, including my call with Bank of America and the
3 email that we discussed, was covering down on potential threats to inauguration day.

4 So I felt, just as the transactions that you detailed that were post-January 6th, I
5 wanted to know, because the weapons-related transactions were since July, I wanted to
6 know, of the 211, how many we were talking about that also made transactions just after
7 January 6th, not since July of 2020.

8 Q And why would it be significant to you that somebody made a weapons
9 transaction post-January 6th? What was the nature of your interest in that?

10 A Because while it wouldn't necessarily mean that there was criminal activity
11 involved, it certainly, from a very -- narrowing the focus even further on the law
12 enforcement side, knew that we knew at the engagement unit, at the headquarters unit,
13 those four that wound up being those four identified, we didn't want to sit on potential
14 risk. And in order to offload that risk, in essence, we want to ensure that those
15 Guardian assessments were pushed out, those four, to the three field offices.

16 Q And when you say "sit on potential risk," you mean -- well, what do you
17 mean? I'm not going to put words in your mouth.

18 A If in the assessment, when the field office reads the assessment, it's up to
19 them to take further investigative activity. Those investigative activities would vary, but
20 it's at a very low level because there's no open investigation. It's a -- it's a
21 no-stone-urned, low-level look at whether or not the field office thinks that there's a
22 threat there.

23 Q And just going back, so anyone on that list had made a purchase for a hotel
24 or some sort of accommodation in the D.C. area after January 6th, correct?

25 A I'm sorry. Repeat that.

1 Q Anybody who was on the list that was in the supporting documentation for
2 the SAR had made a purchase for a hotel or Airbnb or some sort of accommodation in the
3 D.C. area post-January 6th?

4 A Correct. That was my understanding of the SAR.

5 Q And the reason for that is that indicates an intent to return to this area or to
6 travel to this area?

7 A In terms of the reservations, correct, yes.

8 Q Correct. And the four individuals who made -- well, you asked for
9 weapons-related purchases post-January 6th because the combination of a
10 weapons-related purchase and a hotel reservation to come to D.C. might raise alarm that
11 the person is coming to D.C. to use that weapon, correct?

12 A Ostensibly, but at the headquarters level, we wouldn't know that. That
13 would be up to the field office to further investigate.

1 [12:12 p.m.]

2

BY [REDACTED]

3

Q And that's what you mean by sitting on risk -- is you just pushed

4

out -- "maybe take a look at this person," and it's up to the field office to determine

5

whether or not to take look at the person?

6

A Correct.

7

Q The guardians that you sent out, they were, well actually -- the guardians

8

you sent out were information-only leads. Is that correct?

9

A Correct.

10

Q So what does that mean in the FBI parlance?

11

A It means, while there wasn't any definite -- there wasn't any criminal activity

12

identified, that the assessment itself that headquarters wanted to ensure that the field

13

office knew that those fact-based patterns were met in this case, and that any further

14

activity that they chose to do may help them identify potential criminal activity.

15

Q And they don't have to take any further action at all?

16

A Correct.

17

Q Correct? They could --

18

A Correct.

19

Q They could do absolutely nothing with that information?

20

A Correct.

21

Q And the SAR itself made clear, it actually stated that the individuals who

22

were part of the supporting documentation were not considered suspect at that time and

23

that it was filed for informational purposes only, correct?

24

A That's my recollection of the SAR narrative, yes.

25

Q Okay. Now, we've heard -- you stated earlier that the guardians that you

1 pushed out were sent to San Francisco, Memphis, and Tampa, correct?

2 A Correct.

3 Q You did not send any --

4 A No.

5 Q We have heard testimony from agents who said that the Boston Field Office
6 did receive some guardians related to these Bank of America inquiries. You don't know
7 how they got them or when. Is that fair to say?

8 A I only know generally that Boston received a lead, but that's only based on
9 my cursory review in trying to prepare for today, looking back 3 years to understand.

10 Q Fair enough.

11 A But, at the time, that would have been after the guardian assessments that
12 we did went out.

13 Q Okay. And so you don't know what assessment was made or why those
14 leads went out?

15 A No.

16 Q And, of the four leads that you sent out, they were all closed in
17 January 2020, shortly after you sent them out. Is that correct?

18 A Yes, between January 20th and January 28th, I think, is the scope of all four
19 guardians closed.

20 Q And I imagine that's typical with information-only leads?

21 A Yes.

22 Q Is it fair to say that those are the types of leads that you sent out in an
23 abundance of caution because you just said you don't want to sit on risk?

24 A Yeah, I would say the majority -- at least only speaking for myself, being in
25 the Engagement Unit for 3 years, we had several information-only guardians that went

1 out to the field.

2 Q And the agents in the field who are reviewing those guardians and making a
3 determination about whether or not to take any action, they will have a different set of
4 skills and training and experience than you do because they're field agents, correct?

5 A Correct.

6 Q And the purpose of sending them this information is to allow them to apply
7 their particular set of skills to the intelligence that you've developed --

8 A Correct.

9 Q -- and make their own independent assessment, correct?

10 A Correct.

11 Q Sorry. And, again, all of the actions that you took with respect to this
12 information was compliant with the Bank Secrecy Act --

13 A All of the actions I took were compliant with my authorities as an FBI and
14 DOJ authority, correct.

15 Q Thank you. And at any point did you or, to your knowledge, anyone else at
16 the FBI make representations to Bank of America or any other financial institution that
17 information contained in SARs alone could or would be used to predicate an investigation
18 against a suspect?

19 A No.

20 BY [REDACTED]

21 Q Yeah, I just want to be abundantly clear, the Bank of America's supporting
22 documentation included a list of 211 names. You said earlier that the supporting
23 documentation wasn't part of the SAR, it was a separate set of documents, correct?

24 A Correct.

25 Q And you knew there were -- presumably knew there were 211 names, but

1 you didn't investigate 211 customers, correct?

2 A Correct.

3 Q In fact, you went back to Bank of America and said, "I will need to narrow
4 this down, I'm looking for these more specific parameters"?

5 A Correct.

6 Q So, you know, I just want to be clear that the earlier -- there's a reference
7 earlier to 211 Americans on the list. First of all, we've established that there weren't
8 necessarily 211 Americans; it was 211 customers, correct?

9 A Correct.

10 Q And there might have been -- a customer might be an entity, it might be a
11 business entity?

12 A Correct.

13 Q It might be a foreign person?

14 A Correct.

15 Q Okay. Ultimately, if somebody were to leave here and say that the FBI
16 investigated 211 Americans based on those lists, that's not accurate, correct?

17 A Correct.

18 Q Thank you.

19 [REDACTED] Thank you. We can go off the record.

20 [Recess.]

21

BY [REDACTED]

22 Q We can go back on the record. It's 1:25. We'll start with the second
23 round of questioning for the majority.

24 Mr. Sullivan, at the end of the last round, my colleagues were talking about the
25 leads that were sent out. And you had said that other sections or divisions had sent

1 leads out that you were unaware of. When did you become aware that other leads
2 were sent out based upon Bank of America information?

3 A I did not become aware that leads were being sent out specifically, only that
4 the Washington Field Office was looking at the data.

5 Q And what did you understand that the Washington Field Office's look at the
6 data included? Do you know what steps they were taking? Were you involved in that
7 process at all?

8 A No, I had very preliminary discussions on different SARs that we had already
9 reviewed. This was one of them.

10 Q And, when you were liaising with the Washington Field Office, who were you
11 liaising with? And, if they're not an SES position, you can just give their title?

12 A An ASAC.

13 Q An ASAC. I think you can probably give their name.

14 A I don't want to give their name --

15 Q You don't want to give their name?

16 A -- in this proceeding, yeah.

17 Q Okay. Can we have the ASAC's name?

18 [REDACTED] We will email --

19 [REDACTED] Okay. So are you instructing the witness not to answer, or he is
20 just choosing on his own volition not to answer?

21 [REDACTED] Can we go off the record for a second.

22 [REDACTED] Yeah, we can go off the record.

23 [Discussion off the record.]

24 BY [REDACTED]

25 Q We can go back on the record.

1 A Yeah, so, apparently, the ADIC at the time, Steve D'Antuono, who has been
2 interviewed.

3 Q Okay. That was who you were liaising with, was Mr. D'Antuono?

4 A I wouldn't call it liaising, but communicating as another FBI employee who
5 came across private sector production and interaction with the private sector.

6 Q And how often during your engagement on the January 6th matter did you
7 speak with Mr. D'Antuono?

8 A Probably twice.

9 Q Okay.

10 A Give or take.

11 Q And did Mr. D'Antuono kind of fill you in on what steps they were taking on
12 the Bank of America information?

13 A No, only that they were in -- they had -- were also engaging with the private
14 sector but also reviewing financial information that we had discussed, not necessarily the
15 BOA SAR but just SARs in general.

16 Q And did you receive SARs from any other financial institution other than
17 Bank of America in the scope of the January 6th investigation?

18 A Yes.

19 Q What other financial institutions did you receive SARs from?

20 A Can I have a second?

21 [REDACTED] We can go off the record.

22 [Discussion off the record.]

23 BY [REDACTED]

24 Q We'll go back on the record.

25 A Yeah, so, during the FinCEN call, the first FinCEN call we already discussed

1 that Friday, they created a tag for all SARs related to the Capitol riots. So, if you are to
2 follow that tag from FinCEN, they -- you would be able to know the scope of the financial
3 institutions for that.

4 Q And did you receive any other SARs; how Bank of America, that executive
5 after they filed it with FinCEN, the executive then sent the SAR to you, did you receive any
6 other similar SARs in that manner?

7 A Yes.

8 Q And from what financial institutions?

9 A I would refer you to FinCEN for that. They would be able to provide you all
10 the scope of that tag.

11 Q I'm asking specifically did you receive any SARs in a similar manner as Bank
12 of America sent you their SAR after they filed it with FinCEN; did you -- you said you
13 received other SARs from other executives that forwarded you the SAR. Is that correct?

14 A From a handful. Correct.

15 Q From a handful.

16 Chairman Jordan. And was this the same three criteria?

17 Mr. Sullivan. I don't recall.

18 Chairman Jordan. Did you have similar conversations with those other
19 institutions saying, "Here is what I would -- here's how we would" -- what was term you
20 used? "Here's the product idea or how we would like it done, these three criteria, then
21 we get that information"?

22 Mr. Sullivan. No, there was never a discussion of how we the FBI would like it
23 done. It was always interaction with the institution.

24 Chairman Jordan. Okay. But, back to [REDACTED] question, then you did receive
25 that similar type of information from other financial institutions?

1 Mr. Sullivan. Correct.

2 Chairman Jordan. All right. Which one of those institutions?

3 [REDACTED] He is not able today to talk about any other specific SARs. He can
4 generally answer what was discussed and that he got other SARs during that time.

5 [REDACTED] And what's the privilege that the FBI is asserting?

6 [REDACTED] The Bank Secrecy Act.

7 [REDACTED] Which privilege is that?

8 [REDACTED] He is only allowed to speak about a SAR if it falls within his official
9 duties within the scope of answering the questions of the SAR already produced by the
10 Treasury in the scope of this inquiry.

11 [REDACTED] I think the committee would like to know the financial institutions
12 that interacted with Mr. Sullivan and sent their SARs to Mr. Sullivan like Bank of America
13 did. So I think the committee would like to know that information.

14 Mr. Sullivan. So my understanding for today's questions, which we were
15 supposed to have a week ago, was that the ODAG expressed concerns that the
16 committee would have access to the SAR, the Bank of America SAR. Because the
17 committee didn't have access to any other SARs, I don't want to speak to any other SARs.

18 [REDACTED] Okay. But, if you can take that back, we'd like --

19 Chairman Jordan. We're not asking you to speak not specificity of the SAR; we're
20 just asking you to tell us which bank sent it to you.

21 [REDACTED] We'll take that. I certainly appreciate the committee's question.
22 Given the Bank Secrecy Act's implication, we want to make sure not to put the witness in
23 any jeopardy of disclosing information before he has the clearance to disclose that. We
24 certainly understood the Bank of America SAR to be the committee's priority interest to
25 talk about it today, but we will certainly take it back and see if there is additional

1 information we can share.

2 [REDACTED] Is there a specific provision under the Bank Secrecy Act that you
3 can note for the record.

4 [REDACTED] I don't have it in front of me.

5 [REDACTED] I do. 31 U.S.C., 5318(g)(2), and the official duties exception is
6 (g)(2)(a)(2).

7 [REDACTED] Thank you.

8 Chairman Jordan. Do you know, approximately, how many other banks -- the
9 Bank of America --

10 Mr. Sullivan. I don't recall. There's a handful. I couldn't tell you exactly.

11 Chairman Jordan. But you know that other banks did, in fact, send you
12 information complying with those three criteria like Bank of America did.

13 Mr. Sullivan. Yeah, there were between 40 and 60 representatives on the first
14 FinCEN, which probably spanned 30 to 50 financial institutions. So I received a lot of
15 SARs related to the Capitol riots and the unknown threat to Inauguration Day.

16 Chairman Jordan. And did those SARs, like the documents that accompanied the
17 Bank of America SAR, did they name specific individuals?

18 Mr. Sullivan. Within the SAR? Yeah, potentially.

19 Chairman Jordan. Just to be clear, you told us, I think, in the first hour that there
20 were 211 names associated with the SAR coming to the government from Bank of
21 America on those three criteria. I'm just asking; that was similar with the other
22 institutions that sent information as well?

23 Mr. Sullivan. That the same fact-based patterns were in several of the SARs with
24 respect to the unknown threat to Inauguration Day, correct.

25 Chairman Jordan. Names were in the other SARs as well?

1 ██████████ He is not authorized to speak to the content of those -- only if
2 SARs -- if they existed.

3 ██████████ Were leads sent out to field offices based upon the other SARs?
4 You had identified four leads that were sent out based upon individuals who purchased
5 firearms after January 6th that your unit sent out. Were similar leads sent out based on
6 upon the other financial institution SARs?

7 ██████████ Can we go off the record.

8 ██████████ We can government off the record.

9 [Discussion off the record.]

10 BY ██████████

11 Q We can go back on the record.

12 A So, generally speaking, I can't speak to that each SAR that I received -- and
13 remember, I have -- at this same time, I am receiving SARs from multiple financial
14 institutions. I have never read a SAR that was exactly the same. And so, with respect
15 to this, I can't recall exactly how the SAR narrative was in these other SARs. But I
16 handled various SARs that we either determined did not or did meet the threshold of
17 guardian, for example, where we did assessments.

18 Q Okay. And, after you received the Bank of America SAR, you said you went
19 back to the executives and requested additional information based upon firearms
20 purchased. Do I have that right?

21 A I requested information based off of the supporting documentation that was
22 specifically talked about as attached to that SAR.

23 Q And, in order to -- how did you obtain the supporting documentation? Did
24 that come with the SAR, or did you have to request that from Bank of America?

25 A Typically, that's always a request. In that particular instance, once it was

1 published, there are some instances where we may receive the supporting
2 documentation. If, say, we would request it over the phone, as long as the SAR was
3 published, we could then get access to the supporting documentation.

4 Q And, for the other financial institutions that you received January 6th related
5 SARs from, did you request the supporting documentation for those SARs?

6 [REDACTED] All right. He is not authorized to talk about what came with the
7 other SARs.

8 BY [REDACTED]

9 Q So you can't even say if you received supporting documentation?

10 A My understanding is, yes, that I can't speak to that.

11 Q And, with regards to the other financial institutions, did you go back with
12 requests for additional information like you did with Bank of America to the other
13 financial institutions?

14 [REDACTED] Again, he is not authorized to talk about these other SARs.

15 [REDACTED] So he can't even answer if he went back and made another request?
16 Just generally overview.

17 Mr. Sullivan. So my understanding --

18 [REDACTED] Do you recall specifically any other --

19 Mr. Sullivan. My understanding is that the only reason we're speaking about this
20 today is that the SAR was leaked. And the SAR itself is a product that only law
21 enforcement under BSA and under FinCEN regulations is supposed to have access to. So
22 you're putting me in a compromising situation to speak to other SARs that I'm not
23 authorized to speak to. But, in my capacity, yes, I reviewed hundreds of SARs.

24 BY [REDACTED]

25 Q And so --

1 A Over my 3-year period in the unit.

2 Q Okay. So you do not -- was the answer that you don't recall if you reached
3 out to the other financial institutions, or is it that you're relying upon the instruction of
4 agency counsel not to answer the question?

5 [REDACTED] He's not authorized to talk about specific SARs and if he had a
6 communications afterwards about specific data within the SARs.

7 BY [REDACTED]

8 Q Okay. And --

9 A And I'm not trying to be difficult. I want to address all of your questions.
10 So, if it's about the BOA SAR, I am pleased by all means.

11 Q And do you remember -- going back to a previous question, do you
12 remember if any other leads were sent out based upon other SARs?

13 A Generally, but I can't speak to what specific SAR it was or what it was in
14 relation to. I can just say generally that we've reviewed SARs, and assessments have
15 gone out.

16 Chairman Jordan. Okay. So, in a general sense, were the SARs you got back
17 from other financial institutions similar to what you received from Bank of America in all
18 aspects? The number of people who were talked about, I mean, was that a general,
19 were they generally the same?

20 Mr. Sullivan. Again, a SAR, I have never read a SAR that was the same.

21 Chairman Jordan. I'm saying that -- okay.

22 Mr. Sullivan. Sorry.

23 [REDACTED] I'll enter as exhibit No. 5.

24 [Sullivan Exhibit No. 5.

25 Was marked for identification.]

1 BY [REDACTED]

2 Q This is an excerpt of testimony from Special Agent in Charge Bonavolonta
3 from the Boston Field Office. He came and testified before the committee. And, you
4 know, there's several pages of excerpts. I'll point you in the general direction of where
5 I'm going to read from. But please feel free to take as much time as you would like to
6 review.

7 A Thanks. This is portions of it. I'm sorry.

8 Q This is just portions of it. The front of it you'll see is the cover page of the
9 transcribed -- and then just relevant portions that I may refer to.

10 A Okay.

11 Q Okay. And I want to kind of refocus on the leads that were sent out by
12 other units or divisions that you were unaware of. Is that an accurate statement?

13 A Yes.

14 Q Okay. So, on page -- I'm referring to page 12. There is an answer section
15 from Mr. Bonavolonta. And I will just read that into the record. It says, "So they
16 brought the information to my attention, first and foremost, to make me aware that a
17 lead had been sent to our office from a unit within FBI headquarters that fell under the
18 Office of Private Sector. And the lead, the lead itself was for informational purposes
19 only. There was no directive in the lead to do anything, you know, from an investigation
20 standpoint. However, in the body of the lead, there was an information that was
21 provided by Bank of America following a certain number of criteria that in essence
22 aggregated a list of individuals that were supposedly living up in the New England area,
23 you know, either had potentially made certain credit card purchases for hotel
24 reservations or plane tickets or potential purchases at certain gun stores in and around
25 January 6th or plan for inauguration date like around January 20th, in that timeframe."

1 So is it your understanding that the lead was -- any other leads would have been
2 sent out by the Washington Field Office because SEC Bonavolonta seemed to think that it
3 came out of the Office of Private Sector? Are you aware of any other leads that were
4 sent from the Office of the Private Sector?

5 A So, no, and my general -- again, this is only part of, you know, his testimony,
6 so I can't speak to collectively how I might interpret this. But only from what you're
7 presenting to me, the Office of Private Sector wouldn't be the one to send out any kind of
8 operational or investigative lead. It would be the Strategic Engagement Unit or some
9 unit at headquarters. It could also be from a field office, such as, including but not
10 limited to WFO, the Washington Field Office. So it wouldn't have come from the Office
11 of Private Sector, number one. And, in terms of the leads, I'm sorry, your specific
12 question? I just want to make sure I'm answering it fully.

13 Q Yeah, so my question was, were you aware of any other leads that were sent
14 from the Office of Private Sector?

15 A My understanding there were no leads sent from the Office of Private
16 Sector, which is a headquarters, overarching the Office of Private Sector.

17 Q Okay. And then, further down on page 12 that I already read into the
18 record about, in essence, aggregated list of individuals that were supposedly living up in
19 the New England area. When you received the information, was it aggregated in that
20 type of way where the individuals or entities were sorted into geographic areas?

21 ██████████ What information are you asking about?

22 BY ██████████

23 Q The supporting documentation for the 211 individuals or entities.

24 A It was not aggregated by region.

25 Q And how would -- do you know if other field offices or other units at

1 headquarters aggregated that information based upon region?

2 A I mean, I don't know how either Washington Field Office -- again, going back
3 to Office of Private Sector, they would not put -- they would not send leads out period. I
4 think -- I think -- what then SEC Bonavolonta meant was a headquarters entity that
5 handles private sector leads. Office of Private Sector is an actual thing at headquarters
6 that's not in the Counterterrorism Division. So there is that. I'm sorry. Specifically?

7 Q I was just asking, were you aware of any steps that were taken to aggregate
8 the list based upon region?

9 [REDACTED] Do you know from reading this where this information specifically
10 came from?

11 Mr. Sullivan. No.

12 [REDACTED] Just --

13 Mr. Sullivan. I mean, in terms of what?

14 BY [REDACTED]

15 Q Okay. Back to the question that I asked.

16 A Yeah. I want to answer your specific question. That's why I asked.

17 Q So are you aware of any steps that were taken to aggregate the list based
18 upon region?

19 A By Bank of America?

20 Q By the FBI?

21 A No, I'm not aware.

22 Q Okay. So you're not aware SEC Bonavolonta received some sort of list that
23 was aggregated specifically to his region and area of responsibility. You wouldn't know
24 how that information got put together by the FBI?

25 A No, no.

1 Q And then, if you turn to page 17, at the very bottom, the last question that
2 was posed on that page is, "How many individuals were included on that list that were in
3 the jurisdiction of the Boston Division?" Answer, "Approximately six or seven, or around
4 that number."

5 And I know you testified previously that you were not aware of these leads being
6 sent out. But, just to make it clear for the record, you were not aware that another
7 headquarters unit or field office was sending, you know, lists of individuals specific to
8 field office area of responsibility to that field office for information purposes?

9 A At that time?

10 Q Correct.

11 A Correct.

12 Q And when did you come to know that that had happened?

13 A Not until much later that Washington Field Office was using the information.

14 Q Okay.

15 [REDACTED] I'll just mark as exhibit No. 6 testimony from Mr. Steve Jensen, who
16 was the section chief of the Domestic Terrorism Operations Section at this time.

17 [Sullivan Exhibit No. 6.

18 Was marked for identification.]

19 Mr. Sullivan. This is also not the whole thing, correct?

20 BY [REDACTED]

21 Q Correct. It's just relevant excerpts that we may refer to. Have you had
22 sufficient time to review it?

23 A I mean, it's partial, so we might as well just jump to it.

24 Q Okay. So, on page 147, Representative Gaetz asked Mr. Jensen, "What was
25 the Bank of America information that was provided?" Mr. Jensen said, "My

1 understanding -- and, again, I didn't see the information directly. I was made aware of
2 certain leads that were sent out of field offices. I don't recall how many. My
3 understanding of that information was it was certain purchaser transaction
4 individuals -- of individuals that Bank of America provided over to the FBI that wasn't
5 requested by the FBI. It was of their own volition."

6 I just wanted to provide some context. If we go to page 149, I'll ask -- read some
7 more, and then ask a specific question, but I wanted to make sure you had all the context.

8 A Well, I don't have all the context, but, with what you're giving me, yes.

9 Q Correct. So, as he had said previously, he was made aware that leads were
10 being sent out to other field offices. And, down towards the bottom of page 149 in a
11 response, he says, "But, as I noted, one of my employees made me aware that and we
12 took -- I didn't get to this part, but we took immediate action to pull those leads out of
13 our system." Mr. Gaetz said, "When was that?" Mr. Jensen said, "It was immediate
14 upon finding out that those leads existed. I don't know the date. It was a verbal
15 briefing that I received."

16 Were you ever made aware that Mr. Jensen or anyone at the Washington Field
17 Office or headquarters was pulling leads back based upon the Bank of America
18 information?

19 A Pulling leads, no.

20 Q Okay. Were you -- did you ever find out that it was like taken out of the FBI
21 system -- any leads were taken out of the FBI system based upon the Bank of America
22 information?

23 A Not at the time.

24 Q Not at the time.

25

BY [REDACTED]

1 Q I would like to go back to your thresholds that were sent to Bank of America.
2 Who put together these thresholds?

3 A Who put together the thresholds? The brainstorming discussion that I had
4 with Bank of America.

5 Q So that would be you and representatives from Bank of America?

6 A Executives at Bank of America, correct.

7 Q Was FinCEN involved?

8 A FinCEN was the one that sanctioned the first call that discussed fact-based
9 patterns that may help banks identify potential threats to Inauguration Day.

10 Q Did they include these fact-based patterns or thresholds?

11 A Yeah, I think -- I mean, I think I have spoken to that today already that the
12 fact-based patterns were discussed on the first FinCEN call and thereafter.

13 Q Okay. So which one of these thresholds were prepared by you and Bank of
14 America, and which ones were prepared by FinCEN?

15 A I couldn't tell you specifically. I can just tell you that that was a collective
16 brainstorming that we came up with fact-based patterns that could help them identify
17 potential threats to inauguration.

18 Q And so, when you're putting together fact-based patterns, what are you
19 relying on to do that?

20 A Just my own understanding of the threat itself. And then, if you're a data
21 analyst, understanding data and data capabilities both of the financial institution as well
22 as what might be useful to law enforcement and further looking at that data.

23 Q So what are you looking for when you're looking at that financial data? I
24 mean, you're on a call with Bank of America, and you guys are trying to determine
25 thresholds, what's that discussion like?

1 A Most of it is about, you know, when you're talking about narrowing focus,
2 you're talking about narrowing focus by relying on data that collectively may help narrow
3 that focus significantly.

4 Q And were these thresholds sent to other financial institutions?

5 A Those exact I couldn't tell you. I don't think those exact, but similar in
6 terms of the inauguration threat.

7 Q And, when you sent these thresholds, what was the expectation?

8 A You mean, when I emailed those thresholds that you're talking about?

9 Q Correct.

10 A The expectation was, if those helped them narrow their focus, that we
11 would -- we would be happy to review any information that met their thresholds for
12 sharing the information back to law enforcement.

13 Q So you stated before that this was sent by Bank of America of their own
14 volition. But you sent these thresholds and discussed a SAR product idea. Is that
15 right?

16 A I'm sorry; what's the question?

17 Q Well, the question is, is it voluntary for Bank of America to file a SAR after
18 discussing the very thresholds that were subsequently filed by Bank of America with you?

19 A Under BSA, it would be up to the bank exclusively whether or not they met
20 SAR thresholds?

21 Chairman Jordan. Anyone not respond?

22 Mr. Sullivan. You're going to have to clarify.

23 Chairman Jordan. Any financial institutions you sent similar requests to, like you
24 did the Bank of America, and Bank of America sent you back information, including
25 documentation that included 211 American customer names, any other financial

1 institutions you sent similar stuff to, did they not respond?

2 Mr. Sullivan. Of the folks that were on the FinCEN call? Of the banks or
3 financial institutions on the FinCEN call?

4 Chairman Jordan. You can limit it how you want. The question I'm specifically
5 asking is, financial institutions who received a similar request to what was in this email
6 that went to Bank of America, did any of them not respond?

7 Mr. Sullivan. I mean, my issue with your question is did they all not -- did any not
8 respond to the same request? I can't say that every institution had the same request.
9 There were a number of institutions on the FinCEN call that I did not have a followup
10 one-on-one phone conversation with or otherwise that produced SARs that related to the
11 unknown threat to Inauguration Day.

12 Chairman Jordan. Okay. Fair enough. Any of them that you did send
13 something out to today and not respond?

14 [REDACTED] Do you want to take a minute?

15 Mr. Sullivan. Sure.

16 [REDACTED] Off the record.

17 [Discussion off the record.]

18

BY [REDACTED]

19 Q Back on the record.

20 A So it's a hard question to ask because it was 3 years ago. But I want to
21 answer your question. So it's hard for me to answer whether there was any financial
22 institution that I had either a phone discussion with or who was on the FinCEN -- original
23 FinCEN call that didn't produce SARs. I can't recall any financial institution that didn't
24 produce SARs during that time.

25 Chairman Jordan. Okay.

1 Mr. Sullivan. I can't speak to 3 years ago if you're asking me that very specific
2 question.

3 Chairman Jordan. So I just want to make sure we understand, there's a phone
4 call before the 1/15/2021, 9:56 a.m. email that you sent to -- to folks at Bank of America.
5 There's a phone call prior to that. In that phone call, there is a call between you guys, or
6 is that the FinCEN call?

7 Mr. Sullivan. No, the -- before the 1/15 and 9:56 a.m. email, there was a phone
8 call to -- between myself and one of the people in the attention line on this email.

9 Chairman Jordan. Tell me when the FinCEN call happened because I don't have
10 that document.

11 Mr. Sullivan. Two days after the Capitol riots.

12 Chairman Jordan. So prior to all of this?

13 Mr. Sullivan. Correct.

14 Chairman Jordan. Okay. And you're saying, based on the FinCEN call, there
15 were a number of SARs that were sent to you guys?

16 Mr. Sullivan. That were highlighted to us. They were published to the FinCEN
17 portal.

18 Chairman Jordan. Highlighted to you guys?

19 Mr. Sullivan. There were a number of financial institutions that may have
20 published that didn't alert me, and FinCEN wound up also passing out to other law
21 enforcement agencies, us being included in that, that FinCEN tag that they decided all
22 Capitol riot SARs would be tagged with that FinCEN tag.

23 Chairman Jordan. Okay.

24 Mr. Sullivan. So I just want to make it clear, I'm receiving SARs from FinCEN at
25 the time, but I'm also receiving, "Hey, you might want to take a look at this. We've

1 already published it to the FinCEN portal."

2 Chairman Jordan. From the institutions themselves. From the financial
3 institutions. Okay. Got it. Then you have this email, and then there's another phone
4 call before the email where you lay out the thresholds?

5 Mr. Sullivan. Correct.

6 Chairman Jordan. Okay. And we've established, I think, throughout the day
7 that you had similar types of correspondence with other financial institutions you are not
8 allowed to get into. But my question is, of those other financial institutions that you've
9 talked to, did any of them not send you -- did any of them not send you a SAR?

10 Mr. Sullivan. Again, my answer is nuanced because, number one, it was 3 years
11 ago. Number two, the FinCEN call would have allowed institutions to be able to
12 determine whether or not they met SAR thresholds just from the FinCEN call. That
13 didn't require any followup conversation with me. Some did; some didn't. So me
14 speaking directly about that, to what you're saying specifically, I couldn't say.

15 Chairman Jordan. Okay.

16

BY [REDACTED]

17 Q And, on the FinCEN call, the thresholds that you're speaking about that some
18 financial institutions may have just taken and run with it, those thresholds were identified
19 by FinCEN and FBI. Is that accurate?

20 A I believe that they were brainstorming thresholds that we discussed on the
21 call. The call wasn't exclusively the FBI participation. I couldn't speak to other law
22 enforcement agencies that would log in. I can tell you that we were receiving tips and
23 leads and covering down on open investigations at the same time that this call is going
24 on. I do remember also being at home and handling other unclassified leads that were
25 tied to the Capitol riots investigations. So, once I was done talking about my

1 brainstorming of fact-based patterns that had -- might collectively help narrow their
2 focus, I was on to what I was working on. And I couldn't tell you who at FinCEN was
3 saying, "Yes, we don't like these fact-based patterns, or we like these fact-based
4 patterns." What I do remember FinCEN saying is, "Hey, any SARs that results, anything
5 that you the banks collectively are able to publish on SAR thresholds, we would request
6 that you use this specific FinCEN tag to group these in." So that's -- I mean, that's the --

7 Chairman Jordan. Did the FinCEN make -- maybe a couple -- did FinCEN make
8 similar suggestions on what the threshold should be, like what you did in the Bank of
9 America communication?

10 Mr. Sullivan. Like what? Like, sorry, I know -- I think I know what you're asking,
11 but if you could fine tune it.

12 Chairman Jordan. In your notification, you have timeframe purchased, location
13 purchased overlaid with any firearm purchase at any particular time. So you had these
14 sort of three things there. Did FinCEN do the similar stuff in that notification?

15 Mr. Sullivan. I think it was weapons-related and not firearms purchases.

16 Chairman Jordan. Fair enough. Did FinCEN do something similar?

17 Mr. Sullivan. I don't recall if FinCEN did something similar. I do recall the
18 FinCEN tag being on just about every SAR linked to the Capitol riots after that. So, based
19 on their directive, I do remember -- even if I were to get a SAR that was published in the
20 FinCEN portal, in this case, Bank of America, they sent it to me in a secure portal, as well
21 saying "this has been published. FinCEN, that tag was on that SAR and other SARs that
22 followed that.

23 Chairman Jordan. Okay.

24

BY [REDACTED]

25 Q We talked a little earlier about these thresholds. I think you said that you

1 assumed that these three thresholds needed to be met. Is that right?

2 A I didn't say that they needed to be met. This, again, going back to -- this is
3 a -- you have to understand my job role as the finance sector liaison is to engage with
4 these executives and brainstorm and talk about the threat. So this wasn't what we
5 needed but, rather, what we discussed.

6 Q So, when you said, "We are prepared to action immediately the following
7 thresholds," what did you mean by action?

8 A First of all, with every institution that I work with directly, especially at the
9 executive level, because I had weekly, daily, weekly, monthly engagement with these
10 executives, they would know what that meant. That would mean we would review it.
11 And, if anything met additional assessment level, low-level investigative activities, that it
12 wouldn't necessarily be based on the SAR, but that they knew we would review what they
13 had immediately.

14 Q And so, when these thresholds that follow, it could have been one that Bank
15 of America could have understood this to mean one individual threshold being sufficient?

16 A No. What was discussed on the call was that the thresholds in and of
17 themselves -- and I want to make this clear: There was an assumption on the phone call
18 as well as the email that these thresholds had to collectively be met. There was never
19 an indication of Bank of America -- especially at the executive level -- that would be highly
20 unusual. And I've never experienced this in the 3 years that I was finance sector liaison
21 where they take one of those fact-based patterns and say, "We've got a great SAR from
22 just this one fact-based pattern," because that would be -- from a data standpoint, would
23 be an unruly number of volume and irrelevant for us to even take a look at it. So it was
24 understood that these were collective thresholds.

25 Q Okay. The last asterisk -- I'll read it into the record. It states, "SEU intends

1 to capture with its FI partner concurrence all customers who might be more strategic in
2 carrying out the tags related to CTD interest, travel with weapons by vehicle, and not by
3 air given the current threat and aftermath of the 6 Jan Capitol Building incidents. The
4 intention by SEU is to identify all potential networks or threats, those individual threats to
5 Inauguration Day and beyond." What did you mean by FI partner concurrence?

6 A Financial institution.

7 Q Specifically, FI partner concurrence?

8 A Financial institution partner concurrence.

9 Q Meaning with their agreement, with their?

10 A No, the assumption there was, again, if they met information-sharing
11 thresholds under BSA, that, you know, again we would review it.

12 Q And the language to identify --

13 A If I can add, if anything, that's -- I wouldn't even necessarily, you know,
14 discuss this in an email. But the assumption there is that the institution is always under
15 BSA reporting thresholds. So I wouldn't see the data unless it was in an open
16 investigation where I was sharing like specific information of an investigation or a soft
17 copy of the grand jury subpoena to be expedited so that we can get records faster.
18 Does that make sense?

19 Q Yeah.

20 A Does that answer your question fully?

21 Q Yeah, I think so. When you say "to identify all potential networks or threats
22 versus individual threats to Inauguration Day and beyond," what did you mean by and
23 beyond?

24 A So the beyond was discussed -- I remember having a conversation with an
25 analyst in the domestic terrorist section that discussed, along with the earlier memo of

1 "unclassified for official use only" memo that went out by Office of Private Sector that
2 detailed potential unknown threat to Inauguration Day. That beyond -- the original
3 Inauguration Day was March the 4th, the 3rd or 4th. And, after whatever amendment
4 that was made, to change the date from March 4th to January 20th, that was discussed
5 on the phone call with Bank of America. And I can say that, you know, that was a
6 general date range. It wasn't -- we were requesting specific date range from Bank of
7 America that again was up to the bank's threshold.

8 Q So were all individuals that met the criteria of these thresholds viewed as
9 potential network threats?

10 A I'm sorry; were all?

11 Q All 211 individuals, were they considered, in your words, a part of networks
12 of threats?

13 A No.

14 Q Did anyone from Bank of America question the legality of the thresholds?

15 A No.

16 Q Did anyone from Bank of America express concern about the scope of the
17 thresholds?

18 A No.

19 Q Did you have to receive approval from supervisor or anyone at the FBI
20 before sharing these thresholds?

21 A No, but I did discuss them as I would normally discuss them with upper
22 management. My -- typically my direct writing official, which is also a GS-15 and a chief.

23 Q And how did those discussions go?

24 A Great. Like specifically what?

25 Q Did he or she express any concern?

1 A No.

2 Q So, going into these thresholds, how did you expect Bank of America to sort
3 its customers' financial data according to these thresholds?

4 A I couldn't tell you. You'd have to ask Bank of America.

5 Q You don't have any idea of what methods Bank of America might use?

6 A I don't have access. Law enforcement doesn't have access to bank records
7 and proprietary data.

8 Q Sure, but you're a financial sector liaison expert, and your testimony is that
9 you don't have any idea how Bank of America might return customers based on the
10 thresholds you provided?

11 A Yeah, again, I don't want to speak for the bank. I can tell you what I did.
12 Once I reviewed the SAR, I understood that -- and the bank knew this too -- that I would
13 need to review the SAR fully and its content to determine next steps for law enforcement.

14 Q Did the SAR reveal the methods that Bank of America used?

15 A No.

16 Q Did the supporting documentation?

17 A Outside of the fact-based patterns that were notated in the SAR narrative,
18 no.

19 Q The supporting documentation didn't either?

20 A The supporting documentation highlighted additional information on the
21 211.

22 Q And what was that additional information?

23 A It was just names. It was basic information. Name, address.

24 Q Do you think Bank of America could have used merchant category codes?

25 A You'd have to ask them. It would be under their capabilities.

1 Q So that wouldn't be unusual?

2 A For them to use merchant codes in reviewing criminal activity or suspicious
3 activity, no. Anything the bank had access to would be my understanding from my
4 interactions with the banks. It would be -- the capabilities are vast. The critical point
5 is, do they meet SAR thresholds under BSA? Yes or no? So my receiving end of that
6 would be law enforcement access to that.

7 Q Did you have any concern with the thresholds that were shared?

8 A No.

9 Q And, when these thresholds were shared, were there specific identifiable
10 individuals you were interested in, or was this created -- did those fact-based patterns
11 include specific identifiable individuals, or was it just based off looking at raw data?

12 A I mean, my review of the SAR was more about the data and understanding
13 the data to determine whether, you know, what next steps to take, whether, in this case,
14 the guardians that we pushed out, the four that we pushed out.

15 Q One of the thresholds states -- the fourth threshold, it states, quote, "any
16 historical purchase" -- and then, in brackets, you write, "going back 6 months generally
17 for weapons or weapons-related vendor purchases."

18 What did you mean what you said any historical purchase.

19 A Well, the financial institutions generally, generally do not know specific
20 purchases, so, to your point of merchant category codes, they may be looking for those
21 merchant category codes that typically have weapons-related transactions. But there
22 would be no way to determine without a doubt that there were a weapon per se. So,
23 when this was -- this again was a discussion that met a fact-based pattern that was
24 discussed on the call.

25 Q And, when you said any historical purchase, you meant any historical

1 purchase?

2 A Well, it says going back to 6 months generally. That's what Bank of
3 America felt would narrow their focus enough, at least initially in reviewing the data.

4 Q So Bank of America pushed back against any historical purchases?

5 A No, that's not what I said. My understanding is that there -- of the phone
6 call and this email, that this was the brainstorming discussion result.

7 Q Another one of the thresholds mentions purchases made for hotel, Airbnbs,
8 RSVPs in the DMV area, in brackets, the day before and during Inauguration Day since
9 1/6/21. Is purchasing lodging ordinarily evidence of criminal activity?

10 A No, none of -- any one fact-based pattern by itself is not an indicator -- all
11 three together are not an indicator. But, again, this was about the collective fact-based
12 patterns. I can also tell you I have never reviewed a SAR that would ever have one of
13 those fact-based patterns as the SAR. If it had, it wouldn't have been pushed to me by
14 an executive at a financial institution, and my initial review of it would be dismissive.

15 Q Is it normal for SARs to contain the names of 211 individuals or entities?

16 A Define normal.

17 Q Have you received a SAR with that number of persons before?

18 A It's up to the financial institution and the suspicious activity that they're
19 meeting thresholds for of whether or not they're including other individuals in that. So,
20 to answer your question, yes, I have seen many SARs that have more than one individual
21 on the SAR.

22 Q Is it how you have seen --

23 A I have seen thousands.

24 Q Thousands?

25 A Yeah.

1 Q Okay.

2 A And, again, I want to clarify, too, my original comment earlier this morning
3 was there are 5 million SARs that are produced that FinCEN can discuss with you at length
4 the various -- the scope of what's included in the SAR narrative. But, at the end of the
5 day, the FinCEN regulator is still the regulator for all those SARs, and the institutions are
6 responsible for what goes into the SAR and what's published.

7

BY [REDACTED]

8 Q Of the 211 names in there, how many of those persons did you investigate
9 or did you send to have investigated?

10 A Again, it wasn't an investigation. At the headquarters level, in order to
11 mitigate potential risk, we agreed that we satisfied the threshold of a guardian, which is
12 like a no-stone-untuned assessment. We determined, based off of my interaction with
13 Bank of America, my followup conversation on specifically the weapons-related
14 transactions that I wanted to understand which ones were made after January 6th that
15 we were able to drill down to only the four of the 211.

16 Q And the names that didn't reach the level of guardian, were those names
17 stripped from the FBI databases or anything?

18 A No.

19 Q They remain --

20 A No. The SAR, as published in FinCEN, all of law enforcement had access to
21 that SAR, not just the FBI. So any law enforcement agency, once this was released to
22 FinCEN, had access to that Suspicious Activity Report.

23 Q Do they continue to have access to that Suspicious Activity Report?

24 A Any SAR. And I can't speak to FinCEN. I have no idea if they have
25 redaction procedures or not. But I am sure FinCEN could answer that.

1 Q Do you know if there are retention limits on how long the SAR can remain in
2 the system?

3 A No, I think, for bank information generally on the bank side, it's 5 to
4 10 years.

5 [REDACTED] Do you know from personal knowledge?

6 Mr. Sullivan. No. FinCEN would have that information because they're the
7 steward of the data. They also house the data.

8 [REDACTED] Can we go off the record.

9 [Discussion off the record.]

10 BY [REDACTED]

11 Q We can go back on. So is it a normal process for SARs to be sent directly to
12 your email as it was in this case?

13 A What do you mean by normal?

14 Q How do you typically access a SAR?

15 A Either someone on my team accesses it through the FinCEN portal, or based
16 off of a bilat agreement that the Bureau has with FinCEN because of FBI is -- are power
17 users of SAR data, they can also access the data on our SIPRNet, FBI net system.

18 Q Do you know how many people access this filing?

19 A For which? For FBI net or for FinCEN portal?

20 Q Let's start within the FBI, the FBI net?

21 A I don't have those numbers. I can tell you that because of that bilat
22 agreement, because SARs are so critical to law enforcement, the fact that we have that
23 on FBI net accessible to our agents and analysts is huge. So FinCEN does an annual
24 report on users of their data. They wouldn't know what that number was unless they
25 spoke with the FBI, but they would have a number of FBI analysts and agents that log in

1 through the FinCEN portal.

2 Q Okay.

3 A I don't have the numbers. That's an information technology question for
4 us, and that's above my pay grade.

5 Q I apologize since I've been out of the room, but does FinCEN notify you when
6 they have a SAR?

7 A No, it would be impossible to notify when they have a SAR. However, in
8 some cases, like with the Capitol riots, because on that FinCEN call, they came up with
9 that FinCEN code to use in SARs related to Capitol riots, anything related to Capitol riots,
10 they were pushing SARs to me and other law enforcement entities. I think WFO, but I
11 can only tell you they pushed SARs to me during that timeframe. In a normal non-NSSE
12 event, right, I would never -- I may receive one of their products, which is kind of a
13 preliminary analysis of SARs collectively, you know, a potential threat. But, quite
14 frankly, I mean, it's not -- it wouldn't be typical, but during the Capitol riots, I did receive
15 SARs from FinCEN.

16 Q So all the SARs were tagged with a certain code that meant to get sent --

17 A Yes, that FinCEN wanted its financial institutions on that first Friday call after
18 the Capitol riots, they wanted the institutions to use.

19 Q Okay. And then, non-January 6th-type situations, what triggers FinCEN
20 reaching out to you with a SAR?

1 [1:21 p.m.]

2 Mr. Sullivan. Again, they have -- FinCEN, they -- over the years, they've taken on
3 different products where they're -- they review SARs and other BSA activity, like CTRs,
4 cash transactions above 10,000, and they'll put that in, almost like a summary product.

5 I can only speak to a few of them. They used to publish, I don't even know if
6 they still publish, flash reports, which is almost like a summary of multiple SARs on related
7 activities. So most law enforcement would have access to that just like they have access
8 to FinCEN portal for line item SARs that are going in there, thousands, you know, on a
9 daily basis.

10 [REDACTED] So were there, to the extent you know, individuals at FinCEN
11 who were reviewing every SAR that comes in?

12 Mr. Sullivan. On the Capitol -- for what?

13 [REDACTED] Beyond Capitol riots actually.

14 Mr. Sullivan. I can't speak to what FinCEN, you know, did or didn't do on that. I
15 just know that that tag prompted them to be able to, I guess in their own way, review
16 Capitol riots-related SARs.

17

BY [REDACTED]

18 Q So just to clarify, with respect to the Bank of America SAR, there was no legal
19 process provided to Bank of America?

20 A So, I mean, the question is odd because we only -- the partner engagement,
21 the Strategic Engagement Unit, in dealing with any private sector entity, will only deal in a
22 lawful avenue for sharing information.

23 Q Sure. Was process, in terms of a subpoena or national security
24 lever -- letter, sent to Bank of America in this specific instance?

25 A No.

1 Q And in the Bank of America filing --

2 A And if I could clarify, we wouldn't send process for information that was
3 provided to us based off of the financial institutions' meeting of SAR thresholds and they
4 produced in a SAR.

5 Q Thresholds in response to your email and the FinCEN call?

6 A No, not in response to anything. If we received a SAR or had access to a
7 SAR, there would be no subpoena provided for that, unless down the road after an
8 assessment or an investigation may be opened up on on an individual or business entity,
9 only then would we even want to provide grand jury subpoena for fuller records on that
10 individual.

11 [REDACTED] Can we go off the record for a minute?

12 [REDACTED] Sure.

13 [Discussion off the record.]

14 [REDACTED] We can go back on the record.

15 BY [REDACTED]

16 Q So just to continue to clarify, so when you asked for the supporting
17 documentation -- so the SAR is filed, it just has the general information -- when you
18 request the supporting documentation, you don't have to subpoena that?

19 A No.

20 Q You can just request that from the banks?

21 A No. No law enforcement needs to -- that has access to SARs needs to
22 subpoena for records that come -- supporting documents that come with the SAR,
23 provided it's attached to that SAR.

24 Q Okay. And are there any efforts to protect the privacy of the individuals
25 that are on there? How much -- well, are there -- step back.

1 Are there efforts to protect the privacy of individuals that are listed in that
2 supporting documentation?

3 A Well, in terms of there's no public access to that, correct.

4

BY [REDACTED]

5 Q On the filing provided by Bank of America, did it include historical purchases
6 of weapons?

7 A Yes.

8 Q Did it include historical purchases of lodging?

9 A You're talking about the supporting documents or the SAR?

10 Q Either.

11 A The SAR narrative discussed that as a threshold that was met.

12 Q Yeah.

13 A Correct.

14 Q So in the supporting documentation, did it include historical purchases of
15 lodging?

16 A The information captured in the supporting documents was related to that,
17 correct.

18 Q And did it include historical purchases of travel?

19 A Yeah. Any of the -- any of the thresh -- all thresholds that were discussed in
20 the SAR were directly related to the supporting documentation.

21 Q And once you received the filing, what was your expectation for how you
22 would use it at the FBI?

23 A Again, I mean, we receive thousands of tips and leads. SARs is one form of
24 raw intelligence we would receive. The financial institution filing the SAR knows that
25 law enforcement may or may not be, you know, the reviewer of their SAR.

1 Once we review it, we understand, does this warrant further assessment, and
2 then deal accordingly. In this particular case, we determined that there were four
3 Guardian assessments that were met.

4 Q And we may have touched on this already, but did you share the SAR
5 information with other FBI offices, apart from the four Guardian assessments?

6 A So when the four Guardian assessments were finished, and I spoke to this
7 earlier, we highlighted the four Guardian assessments -- there's a tag to each assessment
8 in what's called -- summarized them in what's called an electronic communication, or EC.
9 That EC that was done by our unit included the four Guardian assessments and the SAR
10 itself, and we uploaded it to our case file within the unit, and also the case file, which was
11 normal practice to -- if there is a case, if there is an investigation case file related to the
12 data you're looking at, you should upload it to that case file as well.

13 In this case, we uploaded it to the WFO case file on the Capitol riots, so that they
14 had access to the data and so that there wouldn't be any redundancy on any action or
15 nonaction that they felt was necessary reviewing the data.

16 Q And so when you uploaded the SAR, did that also include the supporting
17 documentation?

18 A I believe it did.

19 Q Would the Office of the Private Sector have access to that portal that you
20 uploaded it to?

21 A Yeah. Anybody with Sentinel case data access, FBI employee, would have
22 access to that.

23 ██████████ We can go off the record.

24 [Recess.]

1 [2:10 p.m.]

2 [REDACTED] Okay. We are back on the record.

3

BY [REDACTED]

4 Q And I want to start by talking a little bit about the Bank Secrecy Act, because
5 based on some of the questions earlier, it appears that there might be some
6 misunderstanding about it and about when legal process is and is not required. And I
7 would hate for any confusion about that to lead to legislation regarding the Bank
8 Secrecy Act based on a fundamental misunderstanding, so I just want to talk about it a
9 little bit.

10 The Bank Secrecy Act, among other things, one of its primary provisions is that it
11 requires financial institutions to report suspicious transactions relevant to possible
12 violations of law and regulation, correct?

13 A Correct.

14 Q So long as those transactions meet certain thresholds?

15 A Correct.

16 Q And it's up to the bank to determine whether or not they meet those
17 thresholds?

18 A Yes.

19 Q And that reporting requirement is something that the bank does pursuant to
20 the Bank Secrecy Act. It does not require a subpoena or a search warrant or anything
21 from law enforcement other than the Bank Secrecy Act itself --

22 A Correct.

23 Q -- correct?

24 A Correct.

25 Q So the Bank Secrecy Act itself is the legal process, correct?

1 A For financial institutions, correct.

2 Q Correct.

3 And I know, based on your educational background, that you're not an attorney,
4 but are you aware that, nearly 50 years ago, the Supreme Court ruled that the Fourth
5 Amendment does not apply to bank records because bank records are considered to be
6 the property of the banks and not the property of the customers whose records they
7 relate to.

8 A Yes.

9 Q You're aware of that, correct?

10 So to the extent that there's any restriction on the ability of banks to provide
11 financial records, those restrictions come from the Bank Secrecy Act --

12 A Correct.

13 Q -- correct?

14 And as you just said, that act requires the provision of certain records relevant to
15 suspicious transactions, correct.

16 A Correct. It obligates the financial institutions to report that activity.

17 Q And no legal process is required for that?

18 A For SARs --

19 Q For SARs.

20 A -- correct.

21 [REDACTED] And to be clear, when we're saying "legal process" meaning a
22 subpoena --

23 [REDACTED] Correct, exactly. A subpoena or --

24 [REDACTED] -- but basically the Act itself is legal process, but an additional
25 subpoena on top of the --

1 Mr. Sullivan. Yes, thank you for clarifying.

2 The Reporter. Hold on, please. Just one at a time, please.

3 [REDACTED] The Bank Secrecy Act itself is the legal process. A subpoena would
4 be a separate form of legal process. The Bank Secrecy Act itself provides legal authority
5 for banks to produce that information, correct?

6 Mr. Sullivan. Correct. Correct.

7 Sorry.

8 [REDACTED] And you were also asked a question about what steps you took to
9 ensure the privacy of the individuals whose names were referenced or incorporated by
10 reference into the Bank of America SAR. And I wanted to talk about the secrecy
11 provisions that are inherent and built into the Bank Secrecy Act. I'm actually going to
12 introduce those into the record. And apologies for making you look at a long section of
13 the U.S. Code.

14 Mr. Sullivan. It's okay.

15 [Sullivan Exhibit No. 7.

16 was marked for identification.]

17 [REDACTED] But I'm going to direct you to subsection -- so this is 31 United
18 States Code, Section 5318, the statute that was mentioned earlier. And if you look on
19 the second page of this, subsection (g), section (2).

20 [REDACTED] And the section we're looking at begins on the bottom of the second
21 column on the second page, and it goes on to the third page.

22 [REDACTED] Okay.

23 Mr. Sullivan. All right. Got it.

24

BY [REDACTED]

25 Q So technically this is 5318 (g)(2)(A) little 2, and it says, "no current or former

1 officer or employee of or contractor for the Federal Government or of or for any State,
2 local, Tribal, or territorial government within the United States, who has any knowledge
3 that such report was made may disclose to any person involved in the transaction that
4 the transaction has been reported, or otherwise reveal any information that would reveal
5 that the transaction has been reported, other than as necessary to fulfill the official duties
6 of such officer or employee."

7 Is that what the statute says?

8 A Yes.

9 Q And is that what you were referring to when you said earlier that the SARs
10 are nonpublic and, therefore, the information contained in them is enough to maintain
11 the privacy of those individuals?

12 A Correct.

13 Q Thank you.

14 Now, I want to go back to -- sure. I'm also going to read into the record one of
15 the implementing regulations. This is from, I believe it's 31 CFR, Section 1020.410.
16 We're going to introduce this. And we are on, this is exhibit 8, correct?

17 [Sullivan Exhibit No. 8.

18 was marked for identification.]

19

BY [REDACTED]

20 Q Actually, it's 1020.320. And if you look at the page that's numbered 1123
21 at the bottom. And in the middle of that page, section (2), it says, "Prohibition on
22 disclosures by government authorities. A Federal, State, local, territorial, or Tribal
23 government authority, or any director, officer, employee, or agent of any of the
24 foregoing, shall not disclose a SAR, or any information that would reveal the existence of
25 a SAR, except as necessary to fulfill official duties consistent with Title II of the Bank

1 Secrecy Act. For purposes of this section, "official duties" shall not include the
2 disclosure of a SAR, or any information that would reveal the existence of a SAR, in
3 response to a request for disclosure of nonpublic information or a request for use in a
4 private legal proceeding, including a request pursuant to 31 CFR 1.11."

5 Did I read that correctly?

6 A Yes.

7 Q And that is, again, your understanding of the secrecy provisions, or the
8 privacy provisions, I should say, of the Bank Secrecy Act?

9 A Yes.

10 Q Thank you.

11 ██████████ So just to put a finer point on this, in the prior hour the question was
12 asked to you, were there any efforts made to protect the privacy of the individuals
13 mentioned in the Bank of America SAR?

14 The answer is that the regulation, the Bank Secrecy Act itself, both inherently
15 provide for those privacy protections, correct?

16 Mr. Sullivan. Correct.

17 ██████████ Thank you.

18 BY ██████████

19 Q Now, I want to talk -- go back, and even though this ground has been
20 trudged quite a bit today, I think it's necessary to go back and just make some
21 clarifications, because I believe we've been loosely using the word "request" to describe
22 your email to Bank of America.

23 And I just want to be clear, this email was a memorialization of criteria that you
24 and the banks had discussed and agreed upon that might be helpful for them in
25 identifying suspicious transactions that could be related to potential violence surrounding

1 the inauguration, correct?

2 A Correct.

3 Q And there was no request in that email for the banks to take any particular
4 action, correct?

5 A Correct.

6 Q And there was no order for the banks to take any particular action?

7 A Correct.

8 Q No compulsion, no pressure?

9 A Correct.

10 Q I believe you -- it was characterized as you saying, here's how we would like
11 it done, but the email didn't even suggest that, correct?

12 A Correct.

13 Q And the banks were free to disregard that criteria and use their own criteria
14 to determine what transactions needed to be reported under the Bank Secrecy Act as
15 relevant to possible violations of crimes that prevent terrorism or other forms of violent
16 activity, to include in their SARs, correct?

17 A Correct.

18 Q Now, you were asked several questions about SARs received from other
19 financial institutions regarding these same criteria or similar criteria. And putting aside
20 the fact, we understand it was 3 years ago, and it's very difficult to remember what you
21 did and didn't receive, but given that the banks have their own independent obligation to
22 review their records and report suspicious activity, and given that everybody was focused,
23 in the days and the weeks after January 6th, on preventing future violence in that vein, I
24 imagine it would be very difficult to distinguish between a SAR that was made in
25 response, say, to that FinCEN call, as opposed to one that the banks just came across on

1 their own accord, correct?

2 A Correct.

3 Q You were also -- you made a reference earlier, and I believe it was in
4 response to a question about your use of the phrase "January 20th and beyond." And
5 you mentioned March 4th and the original inauguration date or something to that effect.
6 Can you explain what you meant by that and what you were referring to?

7 A Yeah. We discussed on the call, there was a -- the domestic terrorist
8 analyst, I remember there were discussions that came within the division that the
9 inauguration day, in terms of a threat, could also possibly mean the original inauguration
10 day, which was back -- I think changed in 1933 -- don't quote me on that -- as part of an
11 amendment, and that was permanently changed to what we know today as January 20th.

12 Q And do you recall there was a theory by QAnon and other domestic
13 extremist groups that former President Trump would actually be inaugurated on March
14 4th, that, quote/unquote, original inauguration date?

15 A I can't remember that specific, but variations of things like that.

16 Q Are you aware that Capitol Police had intelligence that showed a possible
17 plot to breach the Capitol by an identified militia on March 4th of 2020?

18 A Am I aware of who?

19 Q Capitol Police.

20 A That specifically, no.

21 Q Okay. But to be clear, there was concern, not just for violence at the actual
22 planned inauguration date, but that that same type of violence might happen again on
23 March 4th?

24 A That was the fear, correct.

25 Q That was the fear.

1 And you wanted to do what you could, using the lawful tools at your disposal, to
2 prevent that?

3 A Absolutely, yes.

4 Q Now, I want to ask you about some claims that have been made by some of
5 the witnesses in this investigation and by the majority. Are you familiar with
6 George Hill?

7 A I am.

8 Q Okay. And so you're aware that he's a retired FBI supervisory intelligence
9 analyst in Boston, correct?

10 A Yes.

11 Q And you're aware that he previously testified before this committee?

12 A Yes.

13 Q And in his testimony, he stated that Bank of America data-mined its
14 customer base and created, what he described, a huge list of any customer who used a
15 Bank of America debit card or credit card between the dates of January 5th to
16 January 7th.

17 To your knowledge, was that testimony accurate?

18 A No.

19 Q And why not?

20 A Only from the limited amount of what I've read that's been quoted, that's in
21 open source on what Mr. Hill testified to, he obviously wasn't a part of that actual
22 determining whether those assessments were, you know, reviewable and what that field
23 office was going to do with them, with the information.

24 So that particular quote that you're giving is just obviously just one piece that he
25 decided, for whatever reason, because he didn't have access to the information, that he

1 was going to focus on.

2 Q And to the extent that his understanding was that the only criteria to make it
3 onto the list was a financial transaction between those dates, that would be incorrect?

4 A Correct.

5 Q Okay. And he also testified that on top of that list, they put anyone who
6 had purchased a firearm during any date. That's incorrect as well?

7 A False, that's correct.

8 Q Because as we saw, Bank of America reported only firearms purchases from
9 July 2020 through --

10 A That also met --

11 Q That also met -- correct.

12 A -- the additional thresholds --

13 Q Exactly.

14 A -- which was key.

15 [REDACTED] Can I have a quick minute?

16 [REDACTED] Of course.

17 [REDACTED] Thank you.

18 [Discussion off the record.]

19 [REDACTED] Thank you.

20 [REDACTED] Thank you.

21

BY [REDACTED]

22 Q Mr. Hill also testified that there was a list of customers who used a B of A
23 product and who also purchased a firearm at any time that was then, quote, racked and
24 stacked and sent out as leads to the field office in Sentinel, from the case that the
25 Washington Field Office opened, quote/unquote.

1 Was that testimony accurate?

2 A No.

3 Q The entire list was not sent out as leads, correct?

4 A I can't speak to what any other FBI office did. I know that Washington
5 Field Office obviously from previous -- from discussions previously, that we uploaded the
6 information to Washington Field Office. I do know that later -- I found out later that
7 they used the information for further assessment. But I -- from everything that you've
8 read, my understanding is that did not happen the way that he described it. But I also
9 don't know what was in George Hill's head when he was speaking to this. A lot of it
10 didn't make sense to me.

11 Q Fair enough. And your understanding is that he did not actually see the
12 SAR itself --

13 A That's my understanding.

14 Q Thank you.

15 And during his transcribed interview, minority counsel posed a hypothetical to
16 Mr. Hill, and that hypothetical was that if counsel's sister visited him -- I'm sorry.

17 [REDACTED] Majority counsel.

18 BY [REDACTED]

19 Q Majority counsel. I'm sorry. Strange mistake to make.

20 -- but if his sister visited the D.C. area on January 5th, 2021, and made a purchase
21 at a Safeway, would her name have been on the list, and Mr. Hill testified, yes.

22 That was incorrect, wasn't it?

23 A That alone, but I wouldn't want to speak to hypotheticals either. I mean,
24 he would. I know he spoke about a lot of things that he wasn't aware of, but I don't
25 want to speak to any hypotheticals either, on my side of it anyways.

1 Q So last month after Bank of America produced documents to the majority,
2 including your January 15th email that's exhibit 1 to this transcribed interview, the
3 majority released a report entitled, "Financial Surveillance in the United States: How
4 Federal Law Enforcement Commandeered Financial Institutions to Spy on Americans."

5 Do you believe that the FBI commandeered Bank of America to do anything?

6 A No.

7 Q Do you believe that the FBI commandeered Bank of America's databases?

8 A No.

9 Q And I believe I covered this earlier, but I want to ask it again. Did the FBI
10 order Bank of America to conduct any search of its database in connection with your
11 email?

12 A No.

13 Q The minority's report alleged that Federal --

14 [REDACTED] The majority.

15 [REDACTED] The majority. It's been a day.

16

BY [REDACTED]

17 Q The majority's report alleged that Federal law enforcement officials were
18 brainstorming informal methods outside of normal legal processes for obtaining private
19 customer information from financial institutions.

20 What is your response to that allegation?

21 A It's false.

22 Q Okay. And why is it false?

23 A Because we've never exchanged information that we took any kind of
24 investigative activity on and whether that -- that wasn't lawful.

25 Q And also as we discussed earlier, legal process is not required for the

1 information that's produced in a SAR, correct?

2 A Specifically for a SAR, correct.

3 Q The report also criticizes the email you sent by saying that it constitutes a
4 request made without any legal process to individualize criminal nexus. And, again, it's
5 your understanding that legal process, such as a subpoena or a search warrant, was not
6 required for Bank of America to submit the information in that SAR, correct?

7 A Correct.

8 Q The report also referred to -- we discussed earlier, and this was a couple
9 hours ago now, but the DSAC portal that private corporations use to communicate
10 information and to submit information to the FBI, and the majority's report referred to
11 that portal as an obscure government-run portal or a back-door channel.

12 Would you agree with that assessment?

13 A From what I've seen, no.

14 Q And in fact, as we discussed earlier, there's a DSAC website explaining to
15 anybody who has access to the internet exactly what that portal is, who may join, and
16 what it does, correct?

17 A Correct.

18 Q Now, you know, we've talked a lot over this afternoon about legal process
19 and why it is not necessary for SARs. But I want to spend some time talking about the
20 times -- the situations in which you do use legal process.

21 The committee has received document productions from other financial
22 institutions, including Citibank, and I want to show some of those to you just to highlight
23 the difference between communications sent pursuant to legal process and the
24 communications related to SARs.

25 [REDACTED] So if I could have the -- I believe this is 9? Thank you.

1 [Sullivan Exhibit No. 9.
2 was marked for identification.]

3 [REDACTED] Thank you.

4 BY [REDACTED]

5 Q So if you look at the bottom, there's an email that you sent to another
6 individual at the FBI on January 7th, 2021. I don't know if that individual is an SES-level
7 personnel or not, and if not, then we'll make sure to have his name redacted, but can you
8 tell me what that person's role is at the FBI?

9 A That was my rating official of my -- my supervisor.

10 Q Okay. And the subject of the email is "Yellow - Florea." That's F-l-o-r-e-a.
11 And the email States, "Folks, good morning. As you might expect, the current situation
12 has turned this week into a busy week."

13 And I assume by "current situation," you meant January 6th?

14 A Correct.

15 Q Okay. "I have another one for you.

16 "Please check your holdings on Eduard Florea and all associated selectors below in
17 response to a Code Yellow, Pete."

18 And then you provided some more information, and we'll get to that in a minute.
19 But the first question I have for you is, can you explain what a Code Yellow is?

20 A Code Yellow is one of several -- part of a nomenclature we would use to
21 only -- in this instance and others -- discuss priority investigations where there's a
22 subpoena already involved.

23 Q Okay. So Code Yellow itself indicates that a subpoena has been issued for
24 the records?

25 A No. All I can say is that, in terms of protecting sources and methods,

1 existing investigations, this would apply to an existing investigation and a means to
2 prioritize an investigation for a financial institution that we're proactively sharing
3 information on that's covered by a grand jury subpoena.

4 Q Okay. Thank you very much.

5 A Yeah.

6 Q And underneath where you signed it Pete, it says, "FYA, Edward Florea, a
7 New York City resident who has claimed to be armed and intending to travel to D.C. to,
8 quote, unleash some violence, unquote. He previously urged violence against those he
9 disagreed with politically and posted a guide for how to create cyanide as well as photos
10 of knives. Florea was arrested in 2014 on firearms charges in New York City after the
11 NYPD seized 30 guns from his residence."

12 Did I read that correctly?

13 A Yes.

14 Q And then you have some biographical and personal identifying data for
15 Mr. Florea.

16 A Uh-huh.

17 Q Was it your understanding that the recipient of this email would forward it
18 to folks at the bank, at Citibank or whatever bank this was sent to, to identify
19 transactions?

20 A My under- -- so, again, without limiting what I say here, this has to do with a
21 priority investigation that's covered by a grand jury subpoena. The recipients in our
22 financial institutions would naturally involve those lower level that can do the queries in
23 order to understand more about their exposure.

24 Q And you would not make those queries, generally speaking, those types of
25 queries, that level of specificity, without a subpoena, correct?

1 A Yeah. This would have to be an open investigation.

2 Q Okay. And are you aware of whether Mr. Florea was ever arrested and
3 convicted in relation to the activities you describe below?

4 A I am not. There are some that I am, but I can't speak to it, and I wouldn't
5 know -- I probably wouldn't speak to it either because I wouldn't know if it was fully
6 adjudicated.

7 Q Okay. Well, I'm going to introduce a press release from the adjudication of
8 that, just for the record.

9 [REDACTED] And are we on 10? Thank you.

10 [Sullivan Exhibit No. 10.

11 was marked for identification.]

12

BY [REDACTED]

13 Q So this is a press release from the United States Attorney's Office for the
14 Eastern District of New York, dated December 16th, 2021. Is that correct?

15 A Yes.

16 Q And the press release reflects that Mr. Florea pled guilty and was sentenced
17 to 33 months in prison for threatening to kill Senator Raphael Warnock, correct?

18 A Correct.

19 Q And he also pled guilty and was convicted of being a felon in possession of
20 ammunition, correct?

21 A You are reading it correctly.

22 Q And he was found in possession of more than 1,000 rounds of ammunition
23 when authorities searched his residence pursuant to a warrant, correct?

24 A Correct.

25 Q And the press release reflects that Mr. Florea had made several posts about

1 traveling to D.C. and engaging in additional violence during the very hours when the
2 Capitol was under siege, correct?

3 A Correct.

4 Q For example, he posted, quote, Mine are ready, I am ready, we need to
5 regroup outside D.C. and attack from all sides. Talking to some other guys. I will keep
6 watching for the signal, end quote.

7 Did I read that correctly?

8 A Yes.

9 Q He also wrote, quote, Guns cleaned and loaded, got a bunch of guys all
10 armed and ready to deploy, we are just waiting for the word, end quote.

11 Did I read that correctly?

12 A Yes.

13 Q And then he said -- and this is the phrase that I believe was quoted in your
14 email -- quote, It's time to unleash some violence, end quote.

15 Correct?

16 A Correct.

17 Q Okay. I'd like to discuss another individual whose Citibank records you
18 requested in January of 2021.

19 [Sullivan Exhibit No. 11.

20 was marked for identification.]

21

BY [REDACTED]

22 Q Okay. So this is an email from you to that same -- I believe you said it was
23 the supervisor --

24 A Correct.

25 Q Correct. -- at the FBI, dated January 14th, 2021. And the subject line is

1 "Yellow - Hunt." And the email says, "Folks, Please run the following name and
2 associated selectors below in response to a Code Yellow.

3 "Brendan Hunt posted a video on social media calling for people to take back their
4 government and shoot up the inauguration day ceremony.

5 "We are interested in all suspicious activity, associations, and recent purchases.

6 "Thanks, Pete."

7 Did I read that correctly?

8 A Yes.

9 Q And then below that, there's a similar listing, as with the previous email, of
10 personal identifying information, correct?

11 A Correct.

12 Q Okay. And as you testified earlier, Code Yellow means that it's a prioritized
13 investigation?

14 A Yes.

15 Q Okay. And that there's a grand jury subpoena?

16 A It would be an open investigation.

17 Q An open investigation?

18 A Correct.

19 Q Okay. And are you aware of whether Mr. Hunt was arrested and
20 convicted?

21 A You're really quizzing me today.

22 Q That's okay.

23 A You know, there were a number of individuals that were part of the
24 prioritization system that involved people that were arrested.

25 Q And there were enough that you don't remember the details of all of them?

1 A Correct, yeah.

2 Q And these were the types of individuals who, because they had made threats
3 to commit additional violence after January 6th, the email that we sent earlier, the more
4 generalized email to Bank of America, was an attempt to uncover more potential suspects
5 who might be in a similar position, correct?

6 A Yeah. To be clear, the latter was within BSA.

7 Q Exactly.

8 A This was proactive from FBI open investigation.

9 Q Okay.

10 [REDACTED] And the open investigation, the proactive outreach from the FBI only
11 occurred with a subpoena in place?

12 Mr. Sullivan. Correct.

13 [REDACTED] Thank you.

14 [REDACTED] Okay. I would like to introduce the press release from Mr.
15 Hunt's sentencing.

16 [Sullivan Exhibit No. 12.

17 was marked for identification.]

18

BY [REDACTED]

19 Q All right. So this is a press release, again, from the United States
20 Attorney's Office in the Eastern District of New York, and it was issued on November
21 22nd, 2021. And this press release reflects that Brendan Hunt was sentenced to 19
22 months in prison for threatening to assault and murder Members of U.S. Congress, to
23 impede, interfere with, and intimidate those Members, and to retaliate against them on
24 account of their performance of their official duties, correct?

25 A Correct.

1 Q And the press release reflects that on January 8th, 2021, just 2 days after the
2 Capitol riots, Hunt posted a video, titled, Kill Your Senators, that included the summary
3 "Slaughter Them All." Is that correct?

4 A Correct.

5 Q And he made additional threats in the video, exhorting his viewers to
6 violence and telling them, quote, We need to go back to the U.S. Capitol when all the
7 Senators and a lot of the Representatives are there. And this time, we have to show up
8 with our guns, and we need to slaughter these MFs, end of quote.

9 Is that what's reflected there?

10 A You read that correctly.

11 Q Thank you.

12 And he also claimed that, quote, Our government at this point is basically a
13 handful of traitors, so what you need to do is take up arms, get to D.C., probably the
14 inauguration, so-called inauguration of this MF'ing communist Joe Biden. That'll
15 probably be the best time to do this, get your guns, show up to D.C., and literally just
16 spray these MFs, put some bullets in their f'ing heads. Is that correct?

17 A You read it correctly.

18 Q Okay. Probably a safe assumption that he actually spelled out the curse
19 words in the video.

20 A I don't know.

21 Q Sorry, you're not going to assume. Okay.

22 And then he said, If anybody has a gun, give it to me, I'll go there myself and shoot
23 them and kill them. We have to take out these Senators and replace them with actual
24 patriots.

25 That's what's reflected in the press release, correct?

1 A Correct.

2 Q All right. We're going to look at one more individual. This will be our last
3 one.

4 [REDACTED] This is 14, correct? Thirteen.

5 [Sullivan Exhibit No. 13.

6 was marked for identification.]

7

BY [REDACTED]

8 Q Okay. So this exhibit is an email that you sent to your supervisor also on
9 January 14th, 2021, with the subject line "Yellow - Lemke," L-e-m-k-e. And it says,
10 "Folks, Good morning. Please run the following name and associated selectors below in
11 response to a Code Yellow.

12 "On January 6th, 2021, Robert Corey Lemke made interstate threats of violence
13 targeting the family of a U.S. Congressman, as well as others, in furtherance of
14 anti-government, slash, anti-authority extremism. We are interested in all suspicious
15 activity and all recent purchases.

16 "Thanks, Pete."

17 Did I read that correctly?

18 A Yes.

19 Q And then below that, again we have the individual's personal identifiers?

20 A Correct.

21 Q And, again, because this is a Code Yellow, that means it was an open
22 investigation for which there was a grand jury subpoena for the information that you
23 requested?

24 A Correct.

25 Q And are you aware of whether Mr. Lemke was convicted of any offenses?

1 A I'm going to take a guess, probably. This particular instance, I don't have
2 the extent of the details.

3 Q Okay. Well, we will provide them.

4 [REDACTED] Before we go to that, just to be clear on these emails, the "from" and
5 "to," was there anybody blind-copied --

6 Mr. Sullivan. Yes.

7 [REDACTED] -- on these probably --

8 Mr. Sullivan. Yeah.

9 [REDACTED] -- from your general practice?

10 Mr. Sullivan. There are a number of executives that are blind-copy counted,
11 which would -- which is why you would see the email that you saw from Citibank.

12 [REDACTED] Sorry. Executives at the financial institutions or executives at the
13 FBI?

14 Mr. Sullivan. At the financial institutions. Blind-copy counted.

15 [REDACTED] Thank you.

16 Mr. Sullivan. The FBI person is in the regular attention line.

17 [REDACTED] Thank you.

18 BY [REDACTED]

19 Q Okay. So they're blind-copied, and that's why they were produced to us
20 from the bank, that the bank had -- that's how the bank became in possession of them
21 because --

22 A Aware.

23 Q -- they were blind-copied?

24 A Correct.

25 Q Thank you. And I appreciate that clarification.

1 [Sullivan Exhibit No. 14.
2 was marked for identification.]

3 BY [REDACTED]

4 Q So this is a press release from the United States Attorney's Office for the
5 Southern District of New York, so moving a little bit west here, and it's dated December
6 20th, 2021. And this press release reflects that Mr. Lemke was convicted and sentenced
7 to 3 years in prison for making interstate threats, correct?

8 A Correct.

9 Q And obviously it's a crime to make an interstate threat to kill Members of
10 Congress or their families?

11 A Yes.

12 Q Or really anyone?

13 A Correct.

14 Q And you were investigating that for him?

15 A The Counterterrorism Division was, correct.

16 Q Yeah, fair enough. Thank you.

17 The press release reflects that Mr. Lemke refused to accept the result of the 2020
18 Presidential election and sent electronic audio and video messages threatening
19 approximately 50 victims, including journalists, politicians, Members of Congress, and
20 individuals who had made statements expressing that then-President Trump had lost the
21 election, correct?

22 A Correct.

23 Q He even sent the Congressman from the New York City area a picture of a
24 home in the same neighborhood as the home of the Congressman's brother and stated,
25 Your brother is putting your entire family at risk with his lies -- and other words. We are

1 armed and nearby your house. You had better have a word with him. We are not far
2 from his either.

3 Correct?

4 A I'm sorry. Where -- what part of the article are you reading that from?
5 Sorry. I just --

6 Q It's on the second page, and one, two, three, four -- fourth and fifth
7 paragraph down.

8 A Oh, okay.

9 Correct.

10 Q These types of threats were not uncommon, correct, in the weeks
11 after -- and I don't mean specifically threats against Congressmen's brothers, but just
12 threats of violence?

13 A It wasn't -- I mean, it wasn't the only threat to Congressmen or other
14 officials. There were -- but, yes, there were several other threats.

15 Q And that's what your work was focused on in those weeks after January 6th
16 and before the inauguration?

17 A Correct.

18 Q And I want to completely switch gears and talk about a different type of
19 threat, because at the beginning of this interview, I believe that -- and I don't recall, I
20 apologize if it was you or your counsel that mentioned that threats and other concerns
21 about privacy are acutely present here in this case.

22 Has your name been publicized in relation to the majority's investigation about
23 Bank of America's searches?

24 A Yes.

25 Q And have you received any threats or harassment as a result of that

1 publication?

2 A I have not received any direct threats. However, the time around January
3 17th, when my name was released to -- in a letter to Director Wray, my personal cell
4 phone has been ringing off the hook.

5 Q With what kinds of calls?

6 A I don't pick up.

7 Q And do you know how your personal cell phone number was obtained?

8 A I don't know.

9 Q Do you have concerns for your safety or that of your family if, for example,
10 your name were not redacted from the testimony today?

11 A Yes. And I did then when I found out.

12 Q Okay. And have you been concerned basically consistently since January
13 17th?

14 A I wouldn't say consistently. More frustrated, but still concerned, yes.

15 BY [REDACTED]

16 Q I just want to make one point for the record. Going back to what I believe
17 is exhibit -- what was introduced as exhibit 5, which is the testimony of Mr. Bonavolonta, I
18 want to make it clear, on page 13 of that testimony, you were asked a number of
19 questions about the leads that may have been involved in --

20 A Yeah.

21 Q -- and indicated you didn't have personal knowledge of that. But I do want
22 to note, Mr. Bonavolonta said in his testimony, quote, So I reviewed the lead, and it was
23 very clear in the lead that there was not a request to engage with anybody. Or we
24 weren't being directed to do anything.

25 Do you see where it says that?

1 A Yes.

2 Q So Mr. Bonavolonta said during his testimony there was no directive for his
3 field office to take any particular action with respect to that lead, correct?

4 A That's what he's saying.

5 Q Right.

6 A Correct.

7 Q He said that on the record, that there was no directive associated with that
8 lead?

9 A Correct. Without knowing what lead he's talking about, correct.

10 [REDACTED] Okay. Thank you.

11 [REDACTED] And the leads you sent out were the same, they did not contain
12 any directives?

13 Mr. Sullivan. Well, I can't speak exactly to any leads that Washington Field Office
14 or any other field office pushed out. I'm aware that they occurred after our four
15 assessments. So in this case, I'm just simply saying I don't know which lead he's
16 speaking of.

17 [REDACTED] Right. But he said he -- in his own words he said that there was no
18 directive, no order, no instruction, that they were to take any action with respect to that?

19 Mr. Sullivan. You're reading it correctly, yes.

20 [REDACTED] Thank you.

21 We can go off the record.

22 [Recess.]

23 [REDACTED] All right. We'll go back on the record.

24

BY [REDACTED]

25 Q Picking back up, at some point, the Bank of America information was

1 recalled from FBI systems. Is that correct?

2 A I'm sorry. Repeat the question.

3 Q At some point, the Bank of America information was recalled from FBI
4 systems. Is that correct?

5 A Not to my knowledge, not the information that we sent out.

6 Q Okay. I'd like to now enter an excerpt of the transcript from the Judiciary
7 Committee's July 12th, 2023 hearing with FBI Director Wray into the record as exhibit 15.

8 [Sullivan Exhibit No. 15.

9 was marked for identification.]

10

BY [REDACTED]

11 Q And, again, that's just relevant excerpts.

12 A What page?

13 Q Page 33 and 34, if you want to take a second.

14 A All right.

15 Q I'll just go ahead and read into the record the relevant portions.

16 "Mr. Massie. In my remaining 1 minute, I want to turn to another issue.

17 George Hill, former FBI supervisory intelligence analyst in the Boston Field Office, told us
18 that the Bank of America, with no legal process, was -- gave to the FBI gun purchase
19 records with no geographical boundaries for anybody that was a Bank of America
20 customer. Is that true?

21 "Mr. Wray. Well, what I do know is that the -- a number of business community
22 partners all the time, including financial institutions, share information with us about
23 possible criminal activity, and my understanding is that's fully lawful.

24 "Mr. Massie. Did you --

25 "Mr. Wray. In the specific -- in this specific instance --

1 "Mr. Massie. Did you ask for that information?

2 "Mr. Wray. In the specific instance that you're asking about, my understanding is
3 that that information was shared with field offices for information only but then recalled
4 to even -- to avoid even the appearance of any kind of overreach. But my
5 understanding is that that's a fully lawful process."

6 What does it mean when information is recalled?

7 A It can mean a number of things, discontinued or otherwise. I don't want to
8 speak to what the interpretation here is of "recalled." I know that information cannot
9 be further pursued. It could be discontinued, but, again, I'm generalizing.

10 Q Is information removed from FBI systems when it's recalled?

11 A It depends on the instance. I can't speak to all instances where things are
12 recalled. I can only speak to my involvement in the Bank of America SAR and the
13 information that we dealt with.

14 Q Were you aware of this statement before just now?

15 A Yes.

16 Q And what's your reaction to it?

17 A That Director Wray is correct. I mean, he's informed on what
18 Counterterrorism did and didn't do with that information, so --

19 Q How soon after the Bank of America SAR was filed was the information
20 recalled?

21 A For which? So just to clarify, there was the assessments that we wrote
22 from my office and the information that was available to other folks that had access to
23 that in our Sentinel case file. That would include the field office who was running the
24 Capitol riots investigation and their case file, Washington Field Office.

25 Q I'm talking about whichever information was recalled.

1 A I'm only generally aware that information that was used for leads to other
2 field offices after we did our assessments, the four assessments that I detailed, that there
3 was some information that was discontinued and some information that was not
4 discontinued.

5 Q Information that included the Bank of America filing and supporting
6 documentations?

7 A I can't speak to specific information that was recalled. I can only speak to
8 the assessments we pushed out, and my general understanding that there was
9 information that another -- at least one other field office used to determine there may be
10 other leads that were relevant to this.

11 Q Were you part of the decisionmaking process to recall the information?

12 A For specifically what he's -- I can't speak to that.

13 Q So you weren't involved?

14 A I'm not -- I don't have the knowledge of that because I wasn't -- I have been
15 involved in other conversations related to this and other SARs with Office of
16 General Counsel in and around that timeframe. I can speak to that, but I can't speak to,
17 as an enterprise, what was decided on. I wouldn't be in a position to make those
18 decisions or know all of the information related to that.

19 Q Well, and that was the question. So were you a part of the decisionmaking
20 process to recall the information?

21 A No, not to my knowledge.

22 Q Do you know who made the decision to recall the information?

23 A Again, I don't know specifically what information was, quote/unquote,
24 recalled and what that constituted.

25 Q Are you aware of whether it included information that stemmed from the

1 Bank of America filing?

2 A Yeah. I only know that it was generally related to that filing. I know that
3 there was other information that was recalled not related to this filing.

4 Q Are you able to speak to what other information that is?

5 A No. Because I don't know.

6 Q You just know generally that there was other information?

7 A Uh-huh. Yes.

8 [REDACTED] So when you say that information was discontinued -- do I have
9 that correct? You used the word "discontinued"?

10 Mr. Sullivan. I used the word "discontinued," yes.

1 [3:07 P.M.]

2

BY [REDACTED]

3

4

5

Q When that happens, is there any directive to the field offices that goes along with that saying, "This information has been discontinued, you can't continue to investigate these leads"?

6

7

8

A If there is, that's up to the operations section or entity or the program management for their operations at headquarters. That's generally the decision that's made is involving them as kind of a forefront of that decision.

9

10

11

12

13

Q They would make that decision and then direct the field offices?

A I mean, I can't speak just for again the operations section. I'm telling you generally how it works. There may be other Office of General Counsel and other discussions at an executive level to determine if there would be a message or not that would discontinue something. From where I stand. From what I know.

14

15

16

Q When the director says that the information was recalled to avoid giving the appearance of any kind of overreach, was there any discussion around that that, that it was improper to request and receive this information from Bank of America?

17

A No.

18

[REDACTED] Are you saying was he in that discussion?

19

BY [REDACTED]

20

21

22

Q Were you in a discussion, or are you aware of any discussions about that? When it was recalled to avoid this appearance of any kind of overreach, was there any discussion of maybe we shouldn't have done this in the first place?

23

A There was no discussion of maybe we shouldn't do this in the first place.

24

Q Were you surprised that the information was recalled?

25

A Again, I don't know what specific information was recalled. Because,

1 remember, we had already pushed out our assessments on the four of the 211. I am
2 only generally aware that Washington Field Office used the information, and I don't know
3 what other field offices or any other entity that used the information, but the information
4 was accessible.

5 Q Have you ever had any other information that you worked to procure be
6 subject to this kind of recall before?

7 A Not to my knowledge. Not to my recollection. And, again, I don't want
8 to -- I don't want to beat a dead horse, but recall and what that means, I don't know
9 because I can only tell you what I did with the assessments that were involved and then
10 how we uploaded the information and how it was accessible.

11 Q After you upload the information and notice it was accessible, is your role
12 done at that point?

13 A Not necessarily. We can always revisit information that we think may
14 warrant for whatever reason, additional information where we feel like it may meet
15 threshold for further assessment, but that's rare.

16 Q Okay. Would you ever advise field offices on how to use the information
17 and how to conduct their investigations?

18 A Field offices would, you know, routinely contact us if we did write a
19 guardian. Typically, on an information-only guardian, we don't get a lot of questions,
20 but it varies. It varies by field office. There's 56 field offices and legats that would
21 receive the information that responses vary.

22 Q What do you think Director Wray meant by the appearance of overreach?

23 A I'm not going to speak for Director Wray, especially in my position. But,
24 you know, I can only tell you, you know, that, as far as the information that was closed on
25 the four assessments, to your previous question too, that we could have revisited the

1 information, but we did not. And, when the leak of the SAR occurred to FOX News on
2 the fourth, I believe, I have a general awareness that a lot of leads outside of the four that
3 we detailed were discontinued once the SAR was leaked.

4 Q So those leads were discontinued. Is the information still accessible on the
5 FBI databases?

6 A Which specific information?

7 Q The leads that were discontinued, can those still be accessed by FBI agents?

8 A Yeah, and you can see that it was discontinued as well.

9 Q Okay.

10 A Or you may see something along the lines of closed for various reasons,
11 because each field office may get the lead and respond in a slightly different way.

12 Q Okay.

13 A From my exposure to our case system and reviewing guardians.

14 [REDACTED] The last time you saw it and checked, right?

15 Mr. Sullivan. Yeah, from the last time I reviewed and checked.

16 BY [REDACTED]

17 Q I want to move back to the legal standard under the Bank Secrecy Act, as you
18 were brainstorming the thresholds with Bank of America, are there other limits on what
19 thresholds you can share?

20 A I mean, those limits would be intuitive, right? Can you be more specific?
21 Like what?

22 Q Are there limits in terms of the kind of transactions that you can express an
23 interest in as being possibly suspicious?

24 A From my law enforcement standpoint, there is various things that we can
25 discuss and brainstorm. So, in that sense, you know, it varies. It's a pretty wide scope.

1 Q Okay. So that standard, in other words, allows the Bureau to decide what
2 thresholds are suspicious and share that information with financial institutions.

3 [REDACTED] I'm sorry; can you repeat that question?

4

BY [REDACTED]

5 Q Yeah. The legal standard under the Bank Secrecy Act permits the Bureau to
6 determine what threshold its interested in actioning for the financial institution to
7 subsequently act on?

8 A No, I think the BSA -- so the BSA is the bank's regulation side. On the
9 Bureau side of it, under my authorities and FBI and DOJ authorities, my discussion can be
10 on various topics and brainstorm on various, you know, fact-based patterns or typologies,
11 indicators. So that's what I'm saying; it varies widely on the FBI, the Department of
12 Justice side. Under the BSA, that's the financial institution and what they're allowed to
13 do or capable of doing or responsible for reporting.

14 Q Sure, but you liaise with the financial sector. You worked with them in
15 putting together the thresholds. Are there limits on what thresholds you could decide
16 to share with financial institutions?

17 A As a financial institution?

18 Q No, as the Bureau.

19 A Yeah, I mean, I would say the same answer. You know, under the FBI DOJ
20 authorities, I'm able to speak about the threat, and I am able to brainstorm about
21 narrowing the focus of data. I mean, it's a wide scope. I think BSA puts more of
22 the onus on the institution to determine how they're going to report it but that it's their
23 obligation to report suspicious activity.

24 Q Okay. I would like to turn back to the transcript of Joseph Bonavolonta.

25 Page 14. At the bottom of the page, we discussed how -- we discussed who the lead

1 came in from. So the question is posed, "Who did the lead come in from?" "The lead
2 came in from our -- I believe the Strategic Engagement Unit, but I can't say for sure if
3 that's the actual name of the unit, but it fell under or falls under the Office of the Private
4 Sector, which --" "Is that in Boston or out of headquarters?" Answer: "No, out of
5 headquarters." Question: "Do you know if they solicited the information from Bank of
6 America or whether Bank of America just offered it up?" Answer: "The way it reads in
7 the lead, it was -- it did not solicit the information, that the information was just
8 proactively provided to them."

9 Do you agree with that statement that the information was just proactively
10 provided?

11 A Yeah, in my limited access to then SAC Bonavolonta's transcribed interview,
12 yes.

13 Q Do you have an idea why Mr. Bonavolonta believed the information was
14 proactively provided and not requested by the FBI from the way the lead reads?

15 A I'm not going to assume what he thinks by making that statement. I can
16 only tell you my perspective is, if I were him, if I'm reading it this way is because the fact
17 that it's in a SAR.

18 Q Okay.

19 A Yeah.

20 Q And, turning to page 17, there's a question at the middle of the page that
21 states, "And it was also represented to us that individuals were prioritized on that list if
22 they had a firearms purchase. Did that match your recollection?" Answer: "So I
23 don't have any knowledge of anybody being prioritized over a firearm purchase, but in
24 one of the criteria that was in there in terms of Bank of America's data was related to
25 purchases that had been made at either gun shops or, you know, stores that would sell

1 firearms." Is that accurate?

2 A Is what accurate? What you read?

3 Q Yes.

4 A Yes, what you read was accurate.

5 Q And is Mr. Bonavolonta's testimony accurate in terms of how it described
6 the Bank of America information?

7 A Can I review it again?

8 Q Of course.

9 A Again, my answer is going to be based off of limited access to this
10 transcribed interview. I don't have everything in front of me, but if I can just take a
11 second and review this. Yes, I would say that it's correct in that it's weapons-related
12 transactions.

13 Q Okay.

14 A Is there anything specific, though, that -- the reason you're asking, like a
15 more specific question?

16 Q Yeah, were firearm purchases prioritized?

17 A Weapons-related transactions were one of many fact-based patterns that
18 were prioritized by Bank of America in this SAR.

19 Q Okay. And I would like to move to the testimony of Steven Jensen.

20 A What page?

21 Q I'm sorry; I'm going to redirect you.

22 A Okay.

23 [REDACTED] You can set aside that right quick. I now enter an email dated
24 January 18th, 2021, and then attach the liaison information report prepared by the FBI's
25 Office of the Private Sector, titled "Domestic Violent Extremists Likely Emboldened in the

1 Aftermath of the Capitol Breach," into the record as exhibit 16.

2 [Sullivan Exhibit No. 16.

3 was marked for identification.]

4

BY [REDACTED]

5 Q What are liaison information reports?

6 A They are reports that are put together by our analysis section, and they can
7 oftentimes be in concert with unclassified intelligence information that we're able to
8 push out. I say "we" as a division, Office of Private Sector often may have access -- may
9 have their member access to it. But the LIR, from my understanding, is -- it's an analytic
10 product.

11 Q And are you familiar with this liaison information report?

12 A Yeah. Around the 17th of January, yes, I remember reading this.

13 Q And when did you become first aware of the report?

14 A You know, I can only generalize. We're going back 3 years. I can't tell you
15 exactly when. I apologize.

16 Q I want to direct you to the date at the top left. Is that the correct date,
17 January 17th, 2020?

18 A I didn't produce this report, so I am not going to make any assumptions that
19 that date is correct. But it looks like a final product that's been disseminated, so likely.

20 Q And do you know who wrote this report?

21 A I do not. I can only tell you that an analytic element would be responsible
22 for putting this information together and producing it. This would not be within my
23 partner Engagement Section.

24 Q So, at the top, it says Office of the Private Sector.

25 A Yes.

1 Q Did the Office of the Private Sector author this?

2 A They were the ones to disseminate it. They likely coordinated on it. I
3 don't know that they did -- they wouldn't have done the analysis of it, but they would
4 have been one of the tools of kind of the chain of how it was produced.

5 Q And did you work with any of the individuals that prepared it?

6 A No, my unit was engaged with the private sector. This would not be
7 something that our unit authored or published.

8 BY [REDACTED]

9 Q Have you seen this document before?

10 A I have. Like to his question, I couldn't tell you exactly when I read it.

11 Q Do you know if you were still within the Strategic Engagement Section when
12 you saw the document?

13 A I believe so. Probably.

14 Q Do you know if it was during the course of your duties working on
15 January 6th-related investigations that you saw this document?

16 A I can't be sure of it. Likely, yes, probably.

17 Q Were you ever responsible for transmitting this document to any financial
18 institutions?

19 A I don't know that I sent this or if our front office had sent it to all sector
20 partners. Again, you have to remember this is during an NSSE. This is 17th January.
21 This is only 11 days after the Capitol riots, and we're supporting operations on an hourly
22 basis, and leads that are coming in. So that's the only reason I can't tell you for sure if I
23 sent it. I'm not saying that I didn't, but I don't know that I did. But LIRs, I have, we
24 have processed other -- in terms of disseminated LIRs that were published and granted
25 access. I think, earlier this morning, I was given a similar email where my supervisor had

1 said "Feel free to push this out to your partners" -- I'm paraphrasing -- I can't remember
2 the exact email. And, you know, our job is to engage and provide information. So
3 anything that was published officially we would be the steward of that.

4 Q And I know you said you were doing a lot during this time period. Were
5 there other LIRs that were sent out pursuant to the January 6th investigation?

6 A Probably. I couldn't tell you exactly how many or what topics they were
7 outside of, you know, general threat information at the unclassified level.

8 Q Do you remember pushing any LIRs out to your strategic partners in the
9 financial institutions?

10 A I could have. I don't remember specifically. I do remember sharing
11 information with them on a regular basis.

12

BY [REDACTED]

13 Q How is this report distributed?

14 A I'm not in charge of how it's distributed. I can just tell you that, when it's
15 published, oftentimes we're made aware of it and that it's okay to share, because at that
16 point, if it's at the unclassified level, we can share data like that.

17 Q And so what purpose did sharing this liaison information report with
18 financial institutions serve?

19 [REDACTED] Are you asking on a general level because he's already testified that he
20 doesn't recall specifically how this was disseminated?

21

BY [REDACTED]

22 Q What would a liaison information report like this being shared with financial
23 institutions, what purpose would that serve?

24 A Just covering a gambit of what it could serve just in my regular engagement,
25 it would be information only if there is information in the report that helps them set

1 better alerts. That may be the case. If that was the case or the private sector member
2 had specific questions about something that the division provided to them to read, I may
3 be the first person to take the question or maybe not.

4 Q Yeah, footnote 1 states, quote, "The information in this LIR is provided to
5 inform law enforcement of the referenced narratives and theories which may play in
6 mobilizing criminal actors and DVEs to violence." Why was this shared with financial
7 institutions if it was meant to inform law enforcement?

8 A I can't speak to the authors of this of why they decided to footnote. I
9 mean, you can see the footnotes are specific to the quotes and the different assessment.
10 I wouldn't have taken part in that assessment either in analyzing it or producing it.

11 Q And I would like to move back to the DSAC portal. Can you explain briefly
12 the DSAC portal? I know you've touched on that previously.

13 A Yeah, just generally, the DSAC portal -- DSAC members in the private sector
14 may have access to information sharing that occurs in the portal. I don't -- Office of
15 Private Sector runs the portal. Again, Office of Private Sector is enterprise C-suite level
16 engagement. On the engagement that I do, we don't use the DSAC portal to -- and nor
17 do the other operational divisions -- I don't want to speak for them, but I mean for the
18 CTD in terms of sharing information, operational information, and other information on
19 the threat. We don't use the DSAC portal.

20 Q Are the materials shared via the DSAC portal public?

21 A My understanding is that it can be, but I have a very -- I would direct you to
22 the Office of Private Sector to give you a very fine scope of what is and what isn't
23 accessed.

24 Q Because companies have to apply to be a member of the DSAC?

25 A That's my understanding.

1 Q And so, if you're not accepted, you might not have access to that
2 information?

3 A You may not. Again, but that's generally speaking. My understanding.

4 Q Is the liaison information report something that might be shared via the
5 DSAC portal?

6 A I can't be sure. I think that it could have been. The fact that it's coming
7 from the Office of Private Sector, my understanding from the specific types of LIRs that it
8 could be.

9 Q Are there any other organizations like DSAC that provide for public-private
10 portals?

11 A There are -- in terms of specifics, I couldn't speak to specifics. I know that
12 there are other public-private sector partnerships kind of across government, whether it
13 be FBI, other law enforcement agencies, you know, specific sectors that share
14 information with, you know, various field offices in the different law enforcement
15 agencies. I mean, there are different types of public-private partnerships that share
16 information.

17 Q Okay.

18 [REDACTED] We can go off the record for a second.

19 [Discussion off the record.]

20 BY [REDACTED]

21 Q We can going back on the record. Mr. Sullivan, just a couple more
22 questions, and I think, you know, we're done, while our minority counterparts have
23 another round. So I want to turn back to the testimony of Mr. Jensen. I believe that is
24 exhibit 6, looking at page 152. And I'll read the Q&A towards the end of the page here
25 and then ask you a couple of questions on it. The question was, "If an individual was

1 identified because they used their Bank of America debit card in Washington, D.C., on
2 January 6th, but that's all you have, you would agree that that's not enough information
3 to go speak with that person about their role in illegal activities on January 6th?"

4 Answer: "My concern is those instances where Bank of America data was used to
5 initiate leads is that the leads lacked allegations of Federal criminal conduct. Contact by
6 an FBI agent can be consensual at any time, right? But sending leads out based solely on
7 information of purchase history that have no attachment of potential crimes or criminal
8 conduct is what was concerning to me." Do you agree with Mr. Jensen's concerns here?

9 A In terms of how the question was posed, they're only talking about one
10 specific fact-based pattern, yes. But the answer would be no if you're talking about if
11 this question was posed, has Bank of America pushed out the SAR, which was -- had other
12 fact-based patterns present also.

13 Q And when he said -- says "that sending leads out based solely on information
14 of purchase history that has no attachment of potential crimes or criminal conduct is
15 what was concerning to me," were you concerned that the information that was
16 contained in the SAR lacked allegations of Federal criminal conduct?

17 A As far as the assessments that we took part in and pushed out to the four
18 offices that I mentioned, those assessments were specifically done as information-only
19 leads based off of those fact-based patterns that could allow the field offices to use the
20 information to determine if there was a potential threat, i.e., Federal criminal conduct.

21 Q So you don't agree with Mr. Jensen's concerns here that leads that he was
22 sent or he knew were sent lacked Federal criminal conduct?

23 A I'm not saying I disagree with him. I'm saying I agree with his statement in
24 and of itself. But the question that's posed before it only discusses one type of purchase
25 that my office and nobody I know in the Counterterrorism Division would think would be

1 useful in pushing out any type of assessment.

2 Q So was it concerning to you that the information that was obtained from
3 Bank of America through the SAR through the thresholds that were identified by the FBI
4 and FinCEN on a call were then used to push leads out to the field that lacked Federal
5 criminal conduct? Was that concerning to you?

6 A I don't understand the question. What specifically are you asking?

7 Q So was it concerning to you that the information that Bank of America sent
8 to the FBI was then used to push out leads to the field that lacked Federal criminal
9 conduct according to Mr. Jensen who pulled the leads out of the system, was that
10 concerning to you at all?

11 A It wasn't concerning to me in the role that I played in the assessments that
12 went out for my unit.

1 [3:37 p.m.]

2

BY [REDACTED]

3

Q So after it left your unit, you weren't concerned about how the data would

4

be used?

5

A No. In fact, you know, like I mentioned before, the data that we put in the

6

electronic communication involved the four assessments to prevent any potential

7

redundancy if, in fact, there was another entity -- it could be Washington Field Office, in

8

this case, who had the lead on the Capitol riots investigation -- determined that they

9

wanted to use the data for something else.

10

Q So the data -- besides just the four, you know, individuals that you identified,

11

that other data was still available in the FBI system. Is that correct?

12

A So I don't -- please clarify because there -- the data was the data. So there

13

aren't two different types of data. So what are you speaking about?

14

Q So the 200- -- the supporting documentation with the 211 individuals or

15

entities that were identified, you took out four of those to, you know, do Guardians that

16

you thought had more of a likelihood to have criminal conduct because they had bought a

17

firearm after January 6.

18

Was the other information still available in the FBI system just beyond those four

19

individuals?

20

A Well, first, you're -- and just to clarify, you're mischaracterizing. It wasn't a

21

likelihood that there was criminal conduct. It was the assessment to determine. The

22

field office would make that determination if there was reason to further investigate it.

23

Q Uh-huh.

24

A And I'm sorry, the second part of your question?

25

Q Was the information on the 211 individuals or entities, was that still in the

1 FBI system? The supporting documentation, was there still access to that?

2 A In the electronic communication that our unit authored, yes.

3 Q Okay. That was my question.

4 A Yeah.

5 Q Thanks.

6 A That was uploaded to the Washington Field Office's case file.

7 [REDACTED] Uh-huh. We can go off the record.

8 [Recess.]

9 [REDACTED] All right. We are back on the record.

10 At the top of the hour, I just want to note, during the minority's prior hour of
11 questioning, we introduced as exhibits 9, 11, and 13 a number of emails -- email chains
12 between the FBI and Citibank. The exhibits, as introduced, had PII included in them.
13 We're going to swap those exhibits for identical exhibits that have PII, email addresses,
14 phone numbers redacted.

15 Mr. Sullivan. Thank you.

16 [REDACTED] I just want to make that note on the record.

17 Mr. Sullivan. Thank you.

18 BY [REDACTED]

19 Q Mr. Sullivan, I want to turn back to the Jensen and Bonavolonta testimony.
20 And we actually don't need to go back into it, but I want to clarify the record on a couple
21 points.

22 A Sure.

23 Q To be clear, when you brainstormed information with Bank of America, your
24 goal was to develop information that could be used to prevent violence at the
25 inauguration and potentially on March 4th as well, correct?

1 A Right.

2 Q Okay. And so you weren't --

3 A Not on March 4th, but leading up to that and --

4 Q Correct.

5 A -- in that area. That timeframe.

6 Q Understood. But my point is that the reason that you were having that
7 brainstorming session, the goal was to prevent violent -- prevent violence that might
8 happen in the future?

9 A Potential. Correct.

10 Q Okay. There were references that we discussed kind of extensively in the
11 prior hour with the majority counsel to various leads and what might have been done
12 with various leads by different field offices. Do you recall that conversation?

13 A Yes.

14 Q And what Washington Field Office might have done with various leads,
15 correct?

16 A Correct.

17 Q You didn't send out leads -- whatever the Washington Field Office did, you
18 did not send those leads out, correct?

19 A Correct.

20 Q So there was a reference -- I think the assumption is that the Washington
21 Field Office took the 211 names and sent them out to field offices. You don't know what
22 happened?

23 A Correct.

24 Q You have -- you know, there has been representations made to you, but you
25 don't have any personal knowledge of that?

1 A No.

2 Q Okay. And you don't know when Jensen -- when Mr. Jensen -- you read Mr.
3 Jensen's testimony. He said that certain leads had been recalled. You don't know
4 what leads had been recalled?

5 A I only know generally that some were discontinued.

6 Q But you don't have personal knowledge of what or who or how?

7 A No.

8 Q Okay. And there was reference to the data that WFO had. You don't
9 know what data WFO had, correct?

10 A Correct. Generally speaking, yes.

11 Q So they -- so you said that the Bank of America saw or the information was in
12 the system, but you don't know if other information was in the system as well, for
13 example?

14 A Yeah. There was plenty of other information out of the Capitol riots case
15 file.

16 Q Okay.

17 A A ton of information.

18 Q And so -- and you didn't work in Washington Field Office?

19 A Correct.

20 Q So you don't know what WFO did?

21 A Correct.

22 Q Okay. In the prior hour, the majority introduced as exhibit 15 testimony
23 from Director Wray's testimony before this committee. And I'm going to ask you to
24 return to that --

25 A Okay.

1 Q -- and also to pull out exhibit 1, page 2. I guess it's Bates stamped 225, but
2 it's the second page of the exhibit. It's the actual email from you to the Bank of
3 America.

4 A Okay.

5 Q I want to turn to page 90 and look at the -- some comments that were made
6 on page 90 against your email side by side.

7 A Yeah.

8 [REDACTED] I'm sorry. Which email was that?

9 Mr. Sullivan. Oh, I'm on -- you said what page?

10 [REDACTED] Okay. Sorry. So we're going to pull out exhibit 1, which is your
11 email to Bank of America.

12 Mr. Sullivan. Oh, okay. Sorry. I've got a lot of papers. Sorry. Is it in there?
13 Oh, thank you.

14 Okay. I got it.

15 BY [REDACTED]

16 Q And then look at that side by side with page 90 from the hearing transcript.
17 And I want to look at some statements that Chairman Jordan made during the
18 hearing, and I'm going to ask you if they're actually an accurate representation of what
19 your email says.

20 A Okay.

21 Q So on line 2196 on page 90, Mr. Jordan asks, "Did the FBI ask financial
22 institutions to turn over their customers' debit and credit card purchase history in the
23 Washington, D.C. area for January 5th and 6th, 2021?"

24 Do you see where it says that?

25 A Uh-huh.

1 Q The answer to Mr. Jordan's question is no, correct?

2 A Yes.

3 Q The FBI did not ask financial institutions to turn over their customers' debit
4 and credit card purchase history in the Washington, D.C. area for January 5th and 6th,
5 2021, correct?

6 A Correct.

7 Q Okay. Mr. Jordan continues on. He says -- he reads from your email, and
8 he says, "I have the email in hand."

9 He says, "Let's read it. To recap" -- and he reads out loud, "To recap our morning
10 call, we are prepared to action the following threshold, customers transacting debit card,
11 credit card, Washington, D.C. purchases between 1/5/21 and 1/6/21."

12 Do you see where it says that?

13 A Yes.

14 Q In fact, your email -- that bullet point says, "with the additional identifying
15 targeting thresholds," doesn't it?

16 A Correct.

17 Q So Mr. Jordan's representation of what you said was not accurate, correct?

18 A Correct. It was not accurate.

19 Q Because it left out the part where you said "with additional thresholds"?

20 A Correct.

21 Q Okay. And he says, "That is scary enough."

22 Do you think it's scary for the FBI to have these conversations with the Bank of
23 America?

24 A No, not at all.

25 Q Okay. Then he says, "But the next bullet point is even more scary."

1 He says, "Any, any historical capital letters, all caps, any historical purchase of a
2 firearm."

3 Do you see where Mr. Jordan said that?

4 A Yes.

5 Q And, in fact, your email says "any historical purchase going back 6 months
6 generally for weapons or weapons-related vendor purchases."

7 Do you see where your email says that?

8 A Correct.

9 Q So, in fact, Mr. Jordan's statement did not fully represent what your email
10 said, correct?

11 A I agree. That's correct.

12 Q Okay. And then he says again on line 2205, "Did you guys" -- meaning the
13 FBI -- "ask them?"

14 And, again, the FBI did not ask the Bank of America for anything, correct?

15 A Correct.

16 Q On the following page. At lines 2208 to 2213, I'm just going to read this
17 out.

18 Mr. Jordan said, "Well, does this email trouble you as much as it does members of
19 the Judiciary Committee, that the FBI is asking for every single -- I mean, we had
20 Members of Congress here that week, first time they are getting sworn in as a new
21 Member of Congress, their family in town. And you are sweeping. And they may
22 happen to be a customer of Bank of America. And you are sweeping up every debit and
23 credit card purchase of their family who are in town that week because their husband or
24 their dad or their mom is getting sworn in as a new Member of Congress? And then you
25 are also overlaying that information with, did you, did this person buy a firearm?"

1 Do you see where Mr. Jordan said that?

2 A Yes.

3 Q Mr. Sullivan, were you sweeping up the credit card purchase history of new
4 Members of Congress and their families?

5 A No.

6 Q Okay. And, in fact, Mr. Jordan's representations here do not accurately
7 reflect the many -- the one, two, three, four, five -- the six bullet points included in your
8 email, correct?

9 A They do not. Correct.

10 Q And, in fact, your email was much more targeted than that, correct?

11 A More specific.

12 Q And so to the extent that somebody purchased a firearm, that alone
13 wouldn't be sufficient?

14 A Correct.

15 Q And even if the person purchased a firearm and was a customer of Bank of
16 America and purchased something in Washington, D.C., January 5th or 6th, that would
17 not be sufficient, correct?

18 A Correct, with the linked weapons-related transaction.

19 Q Right.

20 A Not firearm, per se.

21 Q Right. Weapons-related transactions --

22 A Uh-huh. Correct.

23 Q -- dating back 6 months generally.

24 And in addition, there was a requirement that there was a purchase made -- or
25 the threshold included bullet point two, which was purchases made for hotel, Airbnb, or

1 RSVPs in the DMV area, correct?

2 A Correct.

3 Q So, in other words, the actual conversation between FBI and Bank of
4 America, the brainstorming session, the thresholds were much more specific?

5 A Correct. Collectively.

6 Q Correct. And it wasn't -- none of these thresholds were to be taken on
7 their own?

8 A Correct.

9 Q Okay. Line 2227, that, "This is lawful, that you can ask this is scary."
10 Again, you didn't ask for anything, correct?

11 A Correct.

12 Q And he said, "This is something else we are going to have to change."

13 I think I can represent that Chairman -- that Ranking Member Nadler is very
14 concerned that this is a suggestion that the Bank Secrecy Act should be taken down. I
15 think that act has been in place since 1970, so it's 54 years.

16 I just want to reiterate. You, in your prior capacities, regularly relied on
17 information provided through Bank Secrecy Act provisions, correct?

18 A Correct.

19 Q And we talked through earlier that the Bank Secrecy Act, for example,
20 helped to stop -- the information provided through the Bank Secrecy Act helped to stop
21 the bombing of a school, correct?

22 A Correct.

23 Q It's frequently used to help target fentanyl trafficking operations, correct?

24 A To my knowledge and speaking to Criminal Investigative Division people that
25 use SARs, generally, I can say correct.

1 Q So you would agree that the Bank Secrecy Act is a pretty valuable tool for
2 the FBI?

3 A Absolutely.

4 Q Okay. Thank you.

5 [REDACTED] Thank you. We can go off the record.

6 [Whereupon, at 3:53 p.m., the interview was adjourned.]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Certificate of Deponent/Interviewee

I have read the foregoing ____ pages, which contain the correct transcript of the answers made by me to the questions therein recorded.

Witness Name

Date

#External Sender# Additional names/selectors for SAR purposes only at your FI's discretion

From: "Sullivan, Peter (CTD) (FBI)" [REDACTED]@fbi.gov>
To: [REDACTED] (CTD) (FBI)" [REDACTED]@fbi.gov>
Bcc: [REDACTED] <[REDACTED]@santander.us>
Date: Fri, 15 Jan 2021 15:25:25 +0000
Attachments: List of names and selectors for SAR purposes only.docx (25.37 kB)

Folks,

SEU has been working hard over the last week to get you additional names/selectors linked to the 6 January Capitol incident and the current threat environment leading up to Inauguration Day.

Please see the attached list of names/selectors linked to the 6 Jan Capitol building incidents and review at the discretion of your own investigation/compliance teams---**for SARs purposes only**.

If you chose to publish a SAR, SEU will be interested to review and disseminate to the appropriate FBI operations personnel immediately.

To be clear, none of the names on this list are part of our SEU's code Yellow/Red/Equity Check outreach tool. But this list is being provided as a collective effort by SEU to help your investigations/compliance teams in your normal course of value-added SAR production.

SEU requests that nothing in the attached be considered a higher priority than SEU's current [pending and future] outreach code YELLOWS/REDS/Equity Checks.

-Pete

Peter Sullivan
Senior Private Sector Partner Outreach
Strategic Partner Engagement Section
[REDACTED]

Message

From: [REDACTED]@sc.com]
Sent: 21/01/2021 18:54:23
To: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED]@sc.com]; [REDACTED]@sc.com]; [REDACTED]
Subject: RE: Additional names/selectors [REDACTED]
Attachments: List of names and selectors [REDACTED]

Sensitivity: Company Confidential

CONFIDENTIAL

Pete,

A search of our systems did not yield results for any of the individuals on the attached list. Please let me know if you need anything else.

[REDACTED]

[REDACTED]

Standard Chartered Bank
 Phone: [REDACTED]
 Email: [REDACTED]
 Address: [REDACTED]
 Website: [REDACTED]

From: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov>
Sent: Friday, January 15, 2021 10:25 AM
To: [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov>
Subject: [External] Additional names/selectors [REDACTED]

ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails.

Folks,

SEU has been working hard over the last week to get you additional names/selectors linked to the 6 January Capitol incident and the current threat environment leading up to Inauguration Day.

Please see the attached list of names/selectors linked to the 6 Jan Capitol building incidents and review at the discretion of your own investigation/compliance teams [REDACTED]

[REDACTED]

To be clear, none of the names on this list are part of our SEU's code Yellow/Red/Equity Check outreach tool. But this list is being provided as a collective effort by SEU to help your investigations/compliance teams in your normal course [REDACTED]

SEU requests that nothing in the attached be considered a higher priority than SEU's current [pending and future] outreach code YELLOWs/REDS/Equity Checks.

-Pete

Peter Sullivan
Senior Private Sector Partner Outreach
Strategic Partner Engagement Section





DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

February 9, 2024

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Jordan:

Thank you for your January 30, 2024, letter concerning the Financial Crimes Enforcement Network (FinCEN) and the ways in which FinCEN supported law enforcement in the aftermath of the violent attack on the U.S. Capitol on January 6, 2021, to help identify those responsible and bring them to justice. To date more than 1,200 people have been charged with crimes in connection with the Capitol attack and nearly 900 have been convicted.

FinCEN and the Department of the Treasury (Treasury) take the matters described in your letter extremely seriously. FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence. FinCEN is deeply committed to fulfilling this important national security and criminal justice mission in accordance with the law.

As you may know, new leadership took over at FinCEN within the past six months. While we have provided some additional background here, we are still working to ensure that we fully understand FinCEN's activities in supporting the Department of Justice (DOJ) and other law enforcement agencies in the aftermath of the January 6 Capitol attack and in advance of the 2021 Inauguration.

FinCEN and the Bank Secrecy Act

FinCEN's mandate encompasses several roles and responsibilities. First, pursuant to the Bank Secrecy Act (BSA), FinCEN is authorized to collect, analyze, and disseminate financial intelligence to law enforcement, national security, and regulatory agencies for use in connection with criminal investigations and related matters.¹ In this capacity, FinCEN promulgates regulations regarding the filing of certain information by financial institutions and individuals, and FinCEN is also responsible for "maintain[ing] a government-wide access service" to provide authorized users with access to this important data that is extremely valuable to law enforcement.² Second, FinCEN regulates financial institutions for compliance with the BSA and its implementing regulations. In this capacity, FinCEN brings enforcement actions against

¹ 31 U.S.C. 310(c).

² *Id.*

financial institutions and other regulated entities for failure to comply with the BSA and its regulations. Finally, FinCEN serves as the Financial Intelligence Unit (FIU) of the U.S. government, and as such is responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to competent authorities financial information related to certain criminal activity.

BSA Reporting

One of the key sources of information that FinCEN uses to carry out its mission are suspicious activity reports (SARs), which are filed by banks and other financial institutions that possess customer transaction information. The BSA requires that a bank or other financial institution file a SAR whenever it identifies “a suspicious transaction relevant to a possible violation of law or regulation.”³ SARs constitute critical tip-and-lead information that helps law enforcement identify, stop, and apprehend criminal actors. SARs contain personally identifiable information about individuals and entities, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation, and as such they are subject to strong confidentiality protections under the law, and FinCEN takes its responsibility to safeguard SAR information extremely seriously.

Law enforcement agencies use BSA reporting in investigations and prosecutions of criminal activities to detect, target, and disrupt illicit financial networks that threaten our national security. BSA data is used across many types of criminal investigations—from fentanyl and other drug trafficking matters, human trafficking, organized and other violent crime, fraud, public corruption, and other financial crime, as well as national security matters such as sanctions. DOJ and other law enforcement agencies also use information generated from SARs and other BSA reporting on both a proactive and reactive basis in investigations of individuals and entities to identify leads, “connect the dots,” and otherwise expand ongoing investigations. This information is also critical to the ability of law enforcement to identify broader trends and risks in illicit finance.

Banks and other financial institutions subject to the BSA are responsible for maintaining their own anti-money laundering (AML) programs, which must be designed, among other things, to ensure their compliance with the BSA and to assist them in detecting and reporting suspicious activity.⁴ While FinCEN and the prudential regulators provide general guidance to and oversight of banks concerning what constitutes an effective AML program, it is ultimately the banks’ responsibility to ensure that their AML programs are effective; that they file SARs in accordance with the law; and that their AML programs effectively detect and report suspicious activity on their networks. It is also the banks’ responsibility to ensure that they comply with all applicable financial privacy laws.

FinCEN Exchange Program

AML programs benefit from banks engaging with the government, so that banks are aware of law enforcement’s highest priorities and can benefit from current information about

³ 31 U.S.C. § 5318(g)(1).

⁴ 31 U.S.C. § 5318(h).

trends and patterns in money laundering and other crimes. As criminal enterprises expand and adapt, these public-private partnerships between banks and law enforcement are all the more important. By understanding how criminal actors operate financially, banks can design better and more effective AML programs. Similarly, these partnerships allow law enforcement to provide guidance to financial institutions, through FinCEN, on the most useful information to include in SARs—which leads to better, more effective SAR reporting by banks and, in turn, helps law enforcement detect and deter criminal activity.

Congress recognized the value of this public-private information exchange when it enacted—with bipartisan support—the Anti-Money Laundering Act of 2020 (AML Act). The AML Act codified a voluntary program, called FinCEN Exchange, to facilitate the sharing of information between law enforcement, FinCEN, and financial institutions for the purpose of disrupting money laundering, terrorism financing, and other crimes.

FinCEN Exchange is a valuable tool not just for our law enforcement partners, but for the financial institutions themselves. FinCEN and Treasury greatly appreciate the bipartisan support for this program, which FinCEN has used to advance law enforcement efforts on a variety of topics of critical importance to national security, criminal justice, and that of our allies. For example, recent FinCEN Exchange events have addressed: Russian sanctions evasion; the terrorist financing networks that support Hamas; fentanyl trafficking; human smuggling; and the abuse of the digital financial ecosystem by North Korea.⁵ In these Exchange events, law enforcement or FinCEN have shared critical information on financial methods used by bad actors and ways in which they try to evade detection, which in turn enhances the ability of participating banks to improve their AML programs and better identify and report illicit activity.

Participation in FinCEN Exchange is voluntary, and no bank is required to implement changes to their AML programs based on the information shared. Further, banks continue to use their judgment in assessing transaction information holistically, as reflected in their overarching AML program, to determine whether it is required to be reported under the BSA.

FinCEN Exchange Events Relating to the January 6 Attack on the Capitol

In the wake of the violent assault on the U.S. Capitol on January 6, 2021, FinCEN convened a series of FinCEN Exchange events. While we are still looking into the details of these events, we understand that these FinCEN Exchange events included government and private sector representatives who voluntarily participated in discussions and information exchanges focused on identifying the perpetrators of this attack and providing support to ongoing law enforcement investigations. The purpose of these FinCEN Exchange events was for law enforcement, FinCEN, and banks to share trends, analysis, and information that banks could consider incorporating into their existing AML/CFT programs to more effectively identify perpetrators of crimes during the January 6 attack or individuals who may have been plotting or conspiring to disrupt the 2021 Inauguration.

As part of these Exchange events, which began shortly after January 6 under the prior Administration, FinCEN and banks shared information about methodologies that banks could

⁵ See <https://www.fincen.gov/resources/fincen-exchange/fincen-exchange-press>.

consider using as part of their AML/CFT programs to identify indicia of suspicious activity relevant to the January 6 attack on the Capitol or threats of violence in connection with the then-upcoming presidential Inauguration.⁶ Many of these typologies were based on previous efforts to develop robust AML/CFT programs that could identify specific types of illegal activity, including activity related to violent extremists or active shooters. For example, one typology suggested methodologies for identifying active shooters based on, for example, series of large weapons-related purchases from multiple stores over a short period of time, in a pattern that was out of the ordinary for the customer, which was to be considered together with other indicators that the customer had already or was about to engage in imminent, mass violence—not to identify normal, lawful gun purchases.

FinCEN provided these typologies so that the participating banks could integrate this information into their AML/CFT programs to the extent they found it helpful. Banks consider a variety of factors and inputs as part of their AML/CFT efforts, including a bank's existing knowledge of its customers and their histories and information about the nature and purpose of specific transactions. No one specific word or transaction code included in these typologies was designed to be used in isolation to “flag” or “target” any individuals. Rather, to the extent key words or phrases were suggested, it was expected they would be used alongside other factors and data that banks regularly analyze as part of their AML programs to detect and report suspicious activity. For example, a document distributed on January 15, 2021 suggested that banks could review payment messages for indications that an individual participated in the assault on the Capitol and included terms such as “antifa,” “MAGA,” “Trump,” “Biden,” “Kamala,” “Schumer,” and “Pelosi,” along with terms indicating an intent to do violence, such as “shoot,” “kill,” “murder” and “storm the Capitol.”

We understand that FinCEN convened these Exchange events starting under the prior Administration and continuing until approximately mid-February 2021. During this time period, law enforcement was actively investigating the January 6 Capitol attack and was also concerned about efforts to disrupt or threaten the upcoming presidential Inauguration. FinCEN's primary role through these Exchange events was to support law enforcement efforts.

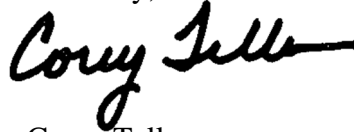
* * * * *

AML programs and the resulting suspicious activity reporting are a vital part of the government-wide effort to prevent the financial system from being used to finance terrorism, drug trafficking, money laundering, and other crimes, and ensure that those who use the financial system for illicit ends are brought to justice. While FinCEN provides guidance, it is ultimately a bank's responsibility to determine when—consistent with the BSA and its implementing regulations—a bank must file a SAR. Once filed, FinCEN takes its obligations to safeguard BSA data, including SARs, extremely seriously for many reasons, including to protect the privacy and civil liberties of citizens who use the financial system.

⁶ In mid-January 2021, law enforcement publicly warned of violence in connection with the upcoming inauguration. See <https://www.foxnews.com/us/fbi-warns-substantial-danger-explosives-protests-domestic-hot-spots-outside-capitol>.

Thank you again for your continued support for the people and mission of FinCEN.
Please reach out to the Office of Legislative Affairs if you have further questions.

Sincerely,

A handwritten signature in black ink that reads "Corey Tellez". The signature is written in a cursive, slightly slanted style.

Corey Tellez
Acting Assistant Secretary
Office of Legislative Affairs

cc: The Honorable Patrick McHenry, Chairman, Committee on Financial Services
The Honorable Bill Huizenga, Chairman, Subcommittee on Oversight and Investigations
The Honorable Blaine Luetkemeyer, Chairman, Subcommittee on National Security,
Illicit Finance, and International Financial Institutions
The Honorable Jerrold Nadler, Ranking Member, Committee on the Judiciary

Message

From: [REDACTED]@sc.com]
Sent: 20/04/2021 23:39:52
To: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov]; [REDACTED]@sc.com]; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED]@sc.com]; MajorCase, FCCInvestigations [REDACTED]@sc.com]
Subject: RE: YELLOW [REDACTED]

Sensitivity: Company Confidential

CONFIDENTIAL

Hi Pete

Thanks for the response. If you have some time may be we can discuss tomorrow so we can get you what you need.

Below is my cell

[REDACTED]

From: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov>
Sent: Tuesday, April 20, 2021 4:46 PM
To: [REDACTED]@sc.com>; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov>
Cc: [REDACTED]@sc.com>; [REDACTED]@sc.com>; MajorCase, FCCInvestigations <[REDACTED]@sc.com>
Subject: [External] Re: YELLOW [REDACTED]
Sensitivity: Confidential

ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails.

[REDACTED]

Thanks!

At your earliest convenience, could you please give me a call at my desk line at your earliest convenience?

FYA, typically for Code Reds and Yellows, we get more on the front end than 'positive', only.

However, the third bucket of priority--'Equity Checks', fall more in-line with your response of 'positive' only with no other info offered because Equity Checks are priority investigations but have no current threat to life or other emergency-related nexus. But because this outreach name on [REDACTED] was a code yellow, we'd like to get something additional. Hope this makes sense.

Pete

Peter Sullivan
 Senior Private Sector Partner Outreach
 Strategic Partner Engagement Section

Message

From: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov]
Sent: 1/14/2021 4:23:40 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7-[REDACTED]]
Subject: [External] RE: Bouncing an Idea off You

External email: Please be careful when opening attachments or clicking links.

Terrific - I'll call you at 1. Thanks!

-----Original Message-----

From: [REDACTED]@us.mufg.jp>
Sent: Thursday, January 14, 2021 11:10 AM
To: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov>
Subject: [EXTERNAL] RE: Bouncing an Idea off You

Terrific. If you're able to give me a time, just shoot me an email and I'll re-arrange meetings to be available. I'm free right now from 1-2 but as I said, can shift stuff around if need be.

-----Original Message-----

From: Tirol, AnnaLou [SES] [mailto:[REDACTED]@fincen.gov]
Sent: Thursday, January 14, 2021 8:34 AM
To: [REDACTED]
Subject: [External] Re: Bouncing an Idea off You

External email: Please be careful when opening attachments or clicking links.

Hi [REDACTED]
It's great to hear from you, and thank you for reaching out with this interesting idea. I will give you a call to chat more, hopefully around midday. I look forward to talking more.
I hope you are safe and well,
AnnaLou

From: [REDACTED]@us.mufg.jp<mailto:[REDACTED]@us.mufg.jp>>
Date: Wednesday, January 13, 2021 at 6:41:53 PM
To: "Tirol, AnnaLou [SES]" <[REDACTED]@fincen.gov>>
Subject: [EXTERNAL] Bouncing an Idea off You

Confidential

Analou, I hope you are well. We live in interesting times. As you might imagine, our bank, and I expect many others, are thinking hard about how we can support the Bureau's efforts to address the acute threat of domestic terrorism we are facing at the moment.

I wanted to bounce an idea off you. Would FincEN have an appetite (assuming you feel you have the authority) to, in SARs filed in relation to the current acute threat of domestic terrorism, identify whether the suspicious activity being reported involves a customer of another institution in the U.S. and, if so, make a 314(a) request, perhaps under a specific code, for such subjects? In other words, Bank A files a SAR for suspicious transactions involving John Doe, a customer of Bank B (an FI in the US). However, Bank B is unaware of the concern surrounding its customer (unless Bank A utilized 314(b) authorities—but even then, the delay would be unworkable when addressing an acute terror threat). FincEN, by doing a 314(a) request for that subject, will trigger an internal review in Bank B (most banks will open an investigation following a 314(a) match). If the 314(a) request is coded under a project name, all the better.

I'm happy to explain myself more in a call. [REDACTED] I'm also curious if FincEN is planning anything independently (i.e., red flags circular). I'm sure that BSAAG members would be happy to contribute thoughts and ideas that could be shared more broadly - even with other BSAAG members.

Anyhow, we are open to assisting however we can, within the existing authorities. Take care and say hi to Ken and congratulations to you both on the passage of the NDAA. That's a big accomplishment!



[Description: cid:image001.jpg@01CF8EF0.2C3F39B0]

1

2

3

4

5 COMMITTEE ON THE JUDICIARY,
6 U.S. HOUSE OF REPRESENTATIVES,
7 WASHINGTON, D.C.

8

9

10

11

12

13 INTERVIEW OF: JIMMY KIRBY

14

15

16

17

18

Thursday, July 18, 2024

19

20

Washington, D.C.

21

22

23

The interview in the above matter was held in room 2237, Rayburn House Office

24

Building, commencing at 10:04 a.m.

25

1 Appearances:

2

3

4

5 For the COMMITTEE ON THE JUDICIARY:

6

7 ██████████ COUNSEL

8 ██████████ SPECIAL COUNSEL

9 ██████████ DIGITAL ASSISTANT

10 ██████████ LAW CLERK

11 ██████████ DEPUTY CHIEF COUNSEL FOR OVERSIGHT

12 ██████████ MINORITY CHIEF OVERSIGHT COUNSEL

13 ██████████ MINORITY PROFESSIONAL STAFF MEMBER

14

15

16 For the SUBCOMMITTEE ON CRIME AND

17 FEDERAL GOVERNMENT SURVEILLANCE:

18

19 ██████████ MINORITY DETAILEE

20

21

22 For the U.S. DEPARTMENT OF TREASURY:

23

24 ██████████ COUNSEL

25 ██████████ COUNSEL

1 [REDACTED] This is a transcribed interview of Jimmy Kirby. Chairman Jordan has
2 requested this interview as part of the committee's oversight of the Department of
3 Treasury's Financial Crimes Enforcement Network.

4 Would the witness please state your name for the record?

5 Mr. Kirby. Jimmy Kirby.

6 [REDACTED] Could agency counsel please state your name for the record?

7 [REDACTED] [REDACTED]

8 [REDACTED] [REDACTED]

9 [REDACTED] On behalf of the committee, I want to thank you for appearing here
10 today to answer our questions. The chairman also appreciates your willingness to
11 appear voluntarily.

12 My name is [REDACTED] and I'm with Chairman Jordan's staff. I'll now have
13 everyone else from the committee who's here in the room introduce themselves as well.

14 [REDACTED] [REDACTED] with Chairman Jordan.

15 [REDACTED] [REDACTED] with Chairman Jordan.

16 [REDACTED] [REDACTED] Chairman Jordan.

17 [REDACTED] [REDACTED] with Ranking Member Nadler.

18 [REDACTED] [REDACTED] with Ranking Member Nadler.

19 [REDACTED] [REDACTED] with Ranking Member Nadler.

20 [REDACTED] [REDACTED] Chairman Jordan.

21 [REDACTED] I'd like to now go over the ground rules and guidelines that we will
22 follow during today's interview.

23 Our questioning will proceed in rounds. The majority will ask questions first for
24 1 hour, and then the minority will have an opportunity to ask questions for an equal
25 period of time if they choose. We will alternate back and forth until there are no more

1 questions and the interview is over.

2 Typically, we take a short break at the end of each hour. If you would like to take
3 a break apart from that, please just let us know.

4 As you can see, there is an official court reporter taking down everything we say to
5 make a written record, so we ask that you give verbal responses to all questions.

6 Do you understand?

7 Mr. Kirby. Yes.

8 [REDACTED] So the court reporter can take down a clear record, we will do our best
9 to limit the number of people directing questions at you during any given hour to just
10 those people on the staff whose turn it is.

11 Please try and speak clearly so the court reporter can understand and so the folks
12 down at the end of the table can hear you.

13 It is important that we don't talk over one another or interrupt each other if we
14 can help it, and that goes for everybody present at today's interview.

15 We want you to answer our questions in the most complete and truthful manner
16 as possible, so we will take our time. If you have any questions or you do not
17 understand one of our questions, please just let us know.

18 Our questions will cover a wide range of topics, so if you need clarification at any
19 point just say so.

20 If you honestly don't know the answer to a question or do not remember, it is best
21 not to guess. Please give us your best recollection, and it is okay to tell us if you learned
22 information from someone else. Just indicate how you came to know the information.

23 If there are things you don't know or can't remember, just say so, and please
24 inform us who, to the best of your knowledge, might be able to provide a more complete
25 answer to the question.

1 You should also understand that although this interview is not under oath, that by
2 law you are required to answer questions from Congress truthfully.

3 Do you understand that?

4 Mr. Kirby. Yes.

5 ██████████ This also applies to questions posed by congressional staff in an
6 interview.

7 Do you understand this?

8 Mr. Kirby. Yes.

9 ██████████ Witnesses that knowingly provide false testimony could be subject to
10 criminal prosecution for perjury or for making false statements under 18 USC Section
11 1001.

12 Do you understand this?

13 Mr. Kirby. Yes.

14 ██████████ Is there any reason you are unable to provide truthful answers to
15 today's questions?

16 Mr. Kirby. No.

17 ██████████ Finally, I'd like to make a note that the content of what we discuss
18 here today is confidential. We ask that you not speak about what we discuss in this
19 interview to any outside individuals to preserve the integrity of our investigation.

20 For the same reason, the marked exhibits that we will use today will remain with
21 the court reporter so that they can go in the official transcript, and any copies of those
22 exhibits will be returned to us when we wrap up.

23 That is the end of my preamble. Is there anything that my colleagues from the
24 minority would like to add?

25 ██████████ We thank the witness for appearing voluntarily today.

1 I also note that this interview is being video'd. The practice has been that the
2 Republicans have not been video'ing current agency employees, and I'm not sure if there
3 was a discussion in advance.

4 I know we are -- the minority staff is usually taken off of emails, so if there was a
5 discussion we might've been excluded from it, but I don't know if there was an agreement
6 reached. I do know that this is not practice for the way that the majority has been
7 proceeding.

8 [REDACTED] Counsel, do you have anything?

9 [REDACTED] I mean, it wasn't flagged for us beforehand. I don't think we
10 have any objection to proceeding this way, but --

11 [REDACTED] Okay.

12 [REDACTED] Then I would also note that, again, the minority has not had any of
13 the videos made available to them. I understand the quality is not very good, so that
14 might be part of the reason. But we have not had any videos made available to us, and
15 that does create concerns about transparency.

16 [REDACTED] The clock now reads 10:08. We will start the first hour of
17 questioning.

18 [REDACTED] We do -- sorry, beforehand, just like we flagged before, we do
19 want to, given the content and the nature of this investigation, want to sort of, again, put
20 on the record with all of you that the BSA provides the suspicious activity reports and a
21 number of other reports, and any information that would reveal the existence thereof is
22 confidential.

23 Unauthorized disclosure of this information is a violation of Federal law. It's
24 subject to civil and criminal penalties. It also can cause, frankly, unjustifiable and
25 irreparable harm to people who are named in these and to national security and to law

1 enforcement interests.

2 So to the extent there is any testimony today concerning a particular SAR -- again,
3 I don't anticipate that there will be -- or any testimony that would reveal the existence of
4 a SAR or lack thereof, we would ask that the committee redact those portions of the
5 transcript, not make them publicly available, as, again, we think any type of disclosure of
6 that nature would cause harm to ongoing law enforcement equities and to national
7 security.

8 Mr. Kirby. And could I start with making an opening statement? Is
9 that permissible?

10 [REDACTED] Yes.

11 Mr. Kirby. Okay. It's short. I promise.

12 So good morning. My name is Jimmy Kirby, and I serve as deputy director of the
13 Financial Crimes Enforcement Network.

14 FinCEN is a bureau of the Treasury Department and a key component of Treasury's
15 Office of Terrorism and Financial Intelligence, or TFI.

16 I have been with Treasury for almost 18 years, virtually all of that time supporting
17 Treasury's national security and counter-illicit finance mission set.

18 I started my Treasury career in the Department's Office of General Counsel in
19 2006 supporting Treasury's Office of Foreign Assets Control, or OFAC, and I served in the
20 Legal Division until September 2020.

21 I spent more than 8 years in the OFAC counsel's office focused on a range of
22 priority national security matters, including enforcing Iran and North Korea-related
23 sanctions, as well as sanctions targeting global narcotics trafficking networks.

24 In late 2015, I was detailed to lead the FinCEN Chief Counsel's Office, and I served
25 as FinCEN's chief counsel from July 2016 to September 2020.

1 opportunity to do more of that work on behalf of the Department.

2 Q And what is your current position?

3 A I am the deputy director of FinCEN.

4 Q And can you describe your role and responsibilities as the deputy director of
5 FinCEN?

6 A I support the director in her management of the bureau's operations, and as
7 well as sort of supporting leadership -- again, the director -- in terms of ensuring FinCEN
8 meets our sort of mission goals and mission sets.

9 Q How many people do you oversee in your role?

10 A I believe our current head count is approximately 280, give or take a few
11 either direction, so approximately 280. So I support -- I manage, for all intents and
12 purposes, the senior executives principally that oversee the sort of different divisions of
13 the organization and the workforce.

14 Q And in 2021 what was your position?

15 A In 2021 I was the associate director of the then-Intelligence Division of
16 FinCEN.

17 Q And how long were you the associate director of the Intelligence Division?

18 A So I started that job in October of 2020, and I moved out of the role in the
19 summer of 2022, I think July of 2022, to serve as acting deputy director. So that's, I
20 guess, about a year and a half, maybe a little more, give or take.

21 Q And when you were in that role, what were your responsibilities?

22 A To sort of manage the operations of the Intelligence Division and to, again,
23 sort of support the other components of FinCEN with regard to their analytic research
24 needs of -- based on our -- the reporting that comes to FinCEN under the Bank Secrecy
25 Act.

1 Q And can you describe the organizational structure of the Intelligence Division
2 and how it fits within FinCEN?

3 A Sure. Then or now?

4 Q Then.

5 A Then.

6 So then, when I took that job in late 2020, if my recollection is correct, I believe
7 the position had been vacant essentially for the prior 2 years-ish, and at the time it was
8 divided into, I think, three offices.

9 So there was a deputy associate director and then three office directors that
10 reported to that deputy director, and there was an Office of Western Hemisphere Affairs,
11 an office of transnational issues, and then a -- I believe the last one was an analytic and
12 research office.

13 Q And who is your direct supervisor as the associate director?

14 A When I started the position, the deputy director of FinCEN at the time was
15 Michael Mosier.

16 At some point early -- relatively early in the current administration, Michael
17 moved out of that job, I think it was in Q1 of 2021, and AnnaLou Tirol moved into that
18 position. So AnnaLou became -- Ms. Tirol, my apologies -- became my supervisor.

19 Q And when did she become your supervisor?

20 A I think it's approximately December 2021, around in there. I mean, I'm
21 sorry, February 2021. I've gotten my calendars backwards in my head.

22 Q That's okay.

23 A There you go. Sorry.

24 Q And how many employees did you oversee in the Intelligence Division?

25 A I would say approximately 50, maybe a little more -- maybe a little more at

1 times. But I think approximately 50 to 55.

2 Q And is it a similar head count now?

3 A I think so, yes. I think their head count is in the 50s now. I'd have to sort
4 of confirm that. But it's about the same size.

5 Q And what was the mission of the Intelligence Division?

6 A So FinCEN's overall mission is to protect the U.S. financial system from illicit
7 finance. We do that in a number of ways, and one of them is through research and
8 analysis of the information filed with FinCEN pursuant to the Bank Secrecy Act.

9 And so a key function of the Intelligence Division is it's staffed with analysts who
10 are knowledgeable in terms of that data and different ways to support the mission set.

11 So, for instance, at the moment, a big part of their function is supporting our work
12 to sort of counter fentanyl in support of law enforcement.

13 So it would be very common for analysts in the then-Intelligence Division and now
14 Research and Analysis Division to be working sort of like very closely with law
15 enforcement on sort of priority issues or individual cases with a particular law
16 enforcement agent.

17 Q And why did the name change?

18 A I think a couple reasons for that.

19 One was our function -- FinCEN's functions were substantially modified by the
20 Anti-Money Laundering Act of 2020. And so y'all are probably familiar with we have a
21 new beneficial ownership reporting program that was contained in that statute.

22 There are also other things contained in that statute. Congress established an
23 analytic hub at FinCEN, which is now housed in this division. They set forth certain -- a
24 requirement that we regularly publish certain trends information based on information
25 filed with us, which I think we're required to do that at least twice a year.

1 And so we've been doing that since the statute was enacted in 2021 on sort of any
2 number of priority issues -- ransomware, other financial exploitation, and the like.

3 So the name change, one, reflected some of the changed responsibilities in the
4 division post this congressional act, and also to give a little bit more clarity as a practical
5 matter on what the division does.

6 FinCEN is not part of the intelligence community, the Intelligence Division was not
7 part of the intelligence community, and it wasn't always clear to folks what that term
8 meant. Whereas, research and analysis I think is a little more transparent in that regard
9 in terms of what the folks sitting in that division are doing on a day-to-day basis.

10 ██████████ And just so the record is clear, what role were you in when the
11 name change took place?

12 Mr. Kirby. I was the acting deputy director. I think that happened late last
13 year. We could confirm that if that's necessary, but I'm pretty sure it was late last year
14 when that happened.

15 BY ██████████

16 Q How frequently did you interact with FinCEN leadership as the associate
17 director?

18 A I would say pretty regularly.

19 So there's sort of a series of standing meetings, check-ins with leadership. There
20 would be, if I'm correctly recalling, sort of regular senior staff meetings.

21 And then on -- if there was certain particular like individual -- I would say, yes,
22 pretty regularly. That's kind of a mumbling answer, but I think that's the best answer I
23 have.

24 Q Would you say weekly? Daily?

25 A I would say, yeah, weekly. I don't know about daily.

1 Q Okay.

2 A Most of the time that I was in that role -- I changed into that role during
3 COVID. And so we weren't sitting around a table like this talking to each other, which
4 had been the practice prior to COVID during that period of time. But still, yes, regular
5 interaction with senior leadership.

6 Q And that would include the then-director of FinCEN?

7 A Correct, yes.

8 Q Okay. And how often did you interact with the Department of Justice?

9 A Me directly? Actually, me directly, I wouldn't say actually that was all that
10 common. That would've been more common, for example, in my prior role, the role I
11 had before the associate director position as chief counsel, because a key portion of that
12 job was actually supervising litigation involving FinCEN.

13 So in the run-up to me changing jobs in 2020, then numerous -- I wouldn't say
14 numerous -- we'll say three -- two or three substantial litigations in which we were in
15 regular contact with the Justice Department because of the need to file briefs, do case
16 coordination, strategy, that sort of stuff. I certainly did not have that kind of regular
17 interaction with the Justice Department when I moved out of the Legal Division.

18 Q And now how often do you interact with the Justice Department?

19 A Again, I would say it's not a regular thing for me in terms of my current
20 day-to-day job. If there's an interagency meeting where I'm attending, someone from
21 the Justice Department is attending, those are not very common for me. But, yeah, I
22 would say it's not a frequent occurrence.

23 [REDACTED] And just to clarify, when you were talking about your prior role
24 interacting with DOJ in connection with these litigation matters, what parts of DOJ would
25 you generally be interacting with?

1 Mr. Kirby. Oh, so principally the Civil Division. So the office -- the Federal
2 Programs Branch in the Civil Division represented us in one of the litigations I'm recalling,
3 and then also the Civil Division of U.S. Attorney's Offices, because, again, these were all
4 civil litigations that I'm thinking of at the moment.

5

BY [REDACTED]

6 Q And prior to joining the Department of Treasury, you said that you worked in
7 private practice?

8 A Correct.

9 Q And were there any other positions before private practice?

10 A I clerked for a Federal judge after leaving law school for a little over a year in
11 Dallas, and then I -- when finishing that I went back to school, did an additional degree,
12 before coming and joining the law firm here in D.C., which was about 3 years there.

13 Q And what was that additional degree?

14 A Public international law at a law school in London.

15 Q Are you a licensed lawyer?

16 A I am, yes.

17 Q When did you become licensed?

18 A So I took the bar in 2001, so I'm going to go with 2001 is when I became
19 licensed.

20 Q And were you a lawyer throughout your tenure at Treasury and FinCEN?

21 A Yes. I am still a lawyer, so technically yes, though I do no longer work in a
22 legal role.

23 [REDACTED] Have you worked for any financial institutions?

24 Mr. Kirby. No.

25

BY [REDACTED]

1 Q Is the associate director of the Intelligence Division functionally the head of
2 the division?

3 A Yes.

4 Q And how did your role relate to the operation of the FinCEN Exchange?

5 A So the FinCEN Exchange was codified in the Anti-Money Laundering Act of
6 2020 that I mentioned before.

7 Management of that function is actually housed in a different division and was
8 housed at the time in a different division of FinCEN, the Strategic Operations Division.

9 The predecessor to the current FinCEN Exchange program -- so we had a program
10 in this space prior to the AML -- was also housed in that Strategic Operations Division.

11 Q And what program was that?

12 A It was still called FinCEN Exchange.

13 Q Okay.

14 A But it was sort of codified and formalized by Congress in the Anti-Money
15 Laundering Act of 2020.

16 Q And the Strategic Operations Division is primarily responsible for the FinCEN
17 Exchange?

18 A Yes, that's correct.

19 Q And that is separate and apart from the Intelligence Division?

20 A That is correct.

21 Q And so your role in relation to the FinCEN Exchange was limited?

22 A Yes, that is correct.

23 Q How does the FinCEN Exchange influence operations at FinCEN?

24 A Hmm.

25 So the FinCEN Exchange is probably our premier public-private partnership, and

1 it's a way for the private sector and different parts of government to come together and
2 share information on priority topics.

3 So a good example of that at the moment is our Project Protect FinCEN Exchange
4 series, which we are doing across the country this year in connection with the Treasury
5 Counter-Fentanyl Strike Force as a way of bringing regional and local banks together with
6 law enforcement and others as a way of sharing typologies and other information to sort
7 of help more broadly -- help financial institutions and others recognize transactions that
8 may involve fentanyl trafficking, but also just to sort of share information and practices.

9 That's a current example of how it is used. Combating fentanyl trafficking is
10 obviously a very high priority for us at the Treasury Department.

11 But it could sort of be on any number of priorities like that where the idea is to
12 sort of share knowledge and expertise. And so we've also done them on countering
13 Russian sanctions evasion. We've done them on different types of money laundering
14 typologies. So it is meant to be a venue that people could come together and share
15 information.

16 Q And where does that information typically originate from?

17 A I don't know if there's a typical. Based on my understanding of the
18 program, sometimes it's -- it may be law enforcement coming and giving a presentation
19 on -- again, going back to fentanyl -- different aspects of fentanyl trafficking; or it may be
20 a financial institution sharing expertise about different ways they analyze the information
21 they have to sort of identify illicit finance threats.

22 Q Would those materials ever come from the Intelligence Division?

23 A Yes. It is not uncommon for -- going back to my fentanyl Project Protect
24 example -- analysts that work on the fentanyl mission set do regularly participate in the
25 FinCEN Exchanges.

1 Q And when material was exchanged with the FinCEN Exchange that came
2 from the Intelligence Division, would you have a role in reviewing and approving those
3 materials?

4 [REDACTED] Can you be a little more specific with that? Like, we're talking
5 in sort of very high generality. So is there something specific you want to ask him about,
6 some specific materials, or, like, more specificity with that question?

7

BY [REDACTED]

8 Q I'm just asking for process. So if the Intelligence Division is sharing material
9 to the FinCEN Exchange, which you've testified that it has, what was your role in getting
10 that material approved and out the door?

11 A I think it would -- I actually -- I think it would depend. Again, given the
12 timeframe is the reason that I'm here, I had been in the position about 90 days when the
13 FinCEN Exchanges that I understand are one of the focuses of this investigation began.

14 So to the extent there were materials that had already been sort of approved, like
15 developed and approved, I would not have expected those necessarily to come back to
16 me for additional approval if they were something that was essentially on the shelf, for
17 lack of a better way of putting it.

18 And I don't think -- sort of, like, this is old recollection at this point, but my
19 recollection is that it wouldn't necessarily be there for every exchange. Something that
20 the Intelligence Division analysts may be presenting in that environment would've come
21 to me for clearance beforehand.

22 Q How does -- how did your role relate to the operation of the Bank Secrecy
23 Act Advisory Group?

24 A So the Bank Secrecy Act Advisory Group is another function that is actually
25 principally housed then and now in our Strategic Operations Division. It's another form

1 of essentially public-private partnership. So my role then would've been actually quite
2 minimal in connection with the sort of operations of that function.

3 Q And are you more involved with that function now?

4 A Yes.

5 Q How so?

6 A So there was a BSAAG -- for example, there was a BSAAG meeting earlier this
7 year, of which I gave the opening remarks in connection with that event. So that is not
8 something that I would've done in a prior and I did not do in a prior role. That is
9 different in the role that I'm in now.

10 Q And how does the Bank Secrecy Act Advisory Group influence operations at
11 FinCEN or the Department of Treasury?

12 [REDACTED] Can you explain what you mean by influence?

13

BY [REDACTED]

14 Q Change. I mean, it's an advisory group.

15 A Yeah. I mean, I think it's an opportunity for -- it's another way for us to sort
16 of hear from and learn from, in this case, usually actors that are actually subject to the
17 requirements of the Bank Secrecy Act in terms of their views and perspectives on any
18 number of sort of regulatory or enforcement or things like that.

19 And influence is sort of hard for me to sort of define one way or the other, but in
20 its, I think, proper form, in its current form, it's an avenue for us to hear views from the
21 sector.

22 I don't know if that answered your question.

23 Q I think so.

24 A Okay.

25 Q Do you know AnnaLou Tirol?

1 A Yes.

2 Q And what was her role in operations at FinCEN?

3 A When she arrived at FinCEN she arrived as the associate director for the
4 Strategic Operations Division. And I'm sorry, but I can't actually recall the date on that.
5 I think I cut you off though from something else.

6 Q What was your professional relationship with her?

7 A So when she arrived at FinCEN, my recollection, I think it was still when I was
8 the chief counsel, so she would've been my, for all intents and purposes, my client at the
9 time. And then when I moved over to the Intelligence Division in late 2020, she
10 would've been my peer. And then in early 2021, she became my manager.

11 Q And do you know [REDACTED]?

12 A I do know [REDACTED] yes.

13 Q And what was her role in operations at FinCEN?

14 A If I remember correctly, [REDACTED] came to FinCEN as the chief of staff. At the
15 time, I was the chief counsel, so, again, she would've been my client. And then we both
16 transferred to the Intelligence Division around the same time in October of 2020, and at
17 that point she would've served as my deputy.

18 Q And do you know [REDACTED]?

19 A I do know [REDACTED], yes.

20 Q And what was your relationship with [REDACTED]?

21 A [REDACTED] was an employee in FinCEN's Strategic Operations Division or its
22 predecessor, I think, for the entirety of our -- he's no longer with FinCEN, but I think for
23 the entirety of his time at FinCEN that we overlapped, I think he was in that division the
24 entire time.

25 Q Do the different divisions within FinCEN that you've described, do they

1 interact frequently, or would you say they're more siloed?

2 A Yes, they do interact. My current and prior understanding is that teams
3 interact regularly.

4 Q And does each division interact with the private sector?

5 A Do you mean in like a regulatory sort of like supervisory way?

6 Q Just in terms of contact with the private sector.

7 A So I think it would vary based on division, would probably be the best
8 answer I could give you.

9 So, for instance, our like Management Division, the folks that sort of run HR and
10 run like services and that sort of stuff, I would think of their private sector interaction as
11 more like managing contractors and managing contracts, dealing with vendors, that sort
12 of stuff.

13 Whereas the more like policy-facing operations at FinCEN -- the Policy Division,
14 the Strategic Operations Division, the Enforcement and Compliance Division, and the
15 Research and Analysis Division, probably along with our Chief Counsel's Office as well -- in
16 different ways, in different fora, not necessarily uncommon for them to interact with
17 different parts of the private sector.

18 Q And did you work closely with the Office of Stakeholder Integration and
19 Engagement?

20 A No, I don't think so. I was aware of what they did, their function at the
21 agency, but I wouldn't say that I worked with them a lot.

22 Q Did you interact with [REDACTED]

23 A Yes.

24 Q How frequently?

25 A I would not actually say it was that frequent, because at least my normal

1 interactions with that division, if my recollection is correct, [REDACTED] was sort of a mid-level
2 manager in that division. I would've probably interacted with his more senior managers
3 when I was interacting with that division more than I interacted with him directly.

4 Q And who would that have been?

5 A That would've probably been, again, AnnaLou in the first instance.

6 AnnaLou was the head of that division when I moved to the Intelligence Division.

7 Q And just so we have a clear record, which division was that?

8 A I moved to the Intelligence Division, and AnnaLou was the head of the
9 Strategic Operations Division at that time.

10 Q And did your office, the Intelligence Division, rely on the Office of
11 Stakeholder Integration to share Intelligence Division material?

12 A Yes, in the context of things like if employees were participating in
13 the -- actually, maybe not. I'm not actually sure.

14 So let me answer your question as I understand it, because I'm not sure my "yes"
15 is 100 percent right.

16 They would have interacted with that office if they were participating in a FinCEN
17 Exchange or if they were doing a presentation at a Bank Secrecy Act Advisory Group
18 meeting.

19 [REDACTED] I'm sorry, who's the "they" in this?

20 Mr. Kirby. Intelligence Division employees.

21 [REDACTED] Thank you.

22 Mr. Kirby. I'm sorry. I'm slipping into pronouns and acronyms quite a bit, so
23 please stop me when I do that.

24 So it would have not been uncommon for them to interact with that office if they
25 were participating in a public-private partnership like that. And it would not have been

1 uncommon for them to share what they were going to be presenting with that office.

2 Does that answer your question?

3

BY [REDACTED]

4

Q Yes.

5

A Okay.

6

Q Would you ever share materials with the Office of Stakeholder Integration

7

and Engagement for distribution with the private sector?

8

A I don't know that that was a common -- I don't know that that was

9

necessarily common. But I also don't know that it's not something that would've

10

happened, particularly with regard to -- for instance, if you're talking to folks on the Bank

11

Secrecy Act Advisory Committee, you might share information with them for the

12

presentation so that folks are speaking from sort of a common set of facts, and it can give

13

a more robust -- that's sort of me speculating. But that's one scenario in which I could

14

see that playing out.

15

Q And when you were the associate director of the Intelligence Division, did

16

you interact with private sector entities?

17

A Yes.

18

Q And what types of private sector entities did you work with?

19

A So I did participate in a -- so one example would be I did -- I did participate in

20

FinCEN Exchange.

21

Am I allowed to talk about FinCEN Exchanges? I think I am.

22

[REDACTED] Uh-huh.

23

Mr. Kirby. Okay. Thank you.

24

That's why we always have to have the lawyers nearby.

25

And so I participated in FinCEN Exchanges involving, for instance, like

1 counter-Russia illicit finance after Russia invaded Ukraine.

2 And that's actually, in the Intelligence Division, the sort of most direct
3 circumstance I remember interacting with the private sector. Again, it was different
4 than when I was the chief counsel where you'd be interacting more with like opposing
5 counsel and stuff like that.

6 But I don't remember that being a sort of frequent thing that I did in the
7 Intelligence Division compared to, for instance, my job now where it's much more
8 common for me to interact with the public and the private sector than the job I had
9 before this one.

10 [REDACTED] And were those primarily financial institutions?

11 Mr. Kirby. I think so, yes.

12 [REDACTED] What sorts of nonfinancial institutions would you work with?

13 Mr. Kirby. I actually can't recall any off the top of my head that would not have
14 been considered financial institutions under our regulations.

15 [REDACTED] Would you have interacted with law enforcement entities in this
16 role?

17 Mr. Kirby. Yes, but I'm trying to think when.

18 So, for instance, going back to my Russia example, we worked with a lot of law
19 enforcement agencies in connection with trying to identify oligarch assets or other sort of
20 illicit assets.

21 And so we have worked very closely with not just sort of like the traditional law
22 enforcement at the Justice Department, but also the Bureau of Industry and Security at
23 the Commerce Department in terms of trying to share information to counter improper
24 exports and sanctions evasion by Russian actors for U.S.-origin or U.S.-restricted goods.

25 So I think some aspects of BIS are technically -- I'm sorry, Bureau of Industry and

1 Security -- are technically considered law enforcement. So in those circumstances -- but
2 I wouldn't have been the principal interlocutor with them, but in those circumstances I
3 would expect that I would have had interaction with those folks.

4 [REDACTED] How do you decide who to partner with in the private sector?

5 Mr. Kirby. I think it kind of depends on the topic and the mission set. And so
6 going back -- and I'm sorry, I keep going back to this example, but it's one we're doing a
7 lot right now, the fentanyl set. The Protect Exchange series that were really the priority
8 for us at the moment, a lot of the financial institutions that we're inviting to those
9 sessions are sort of regional and local banks as a way of sort of, as they're closer to their
10 communities, to ensure that we're sharing information in sort of like all levels of the
11 financial sector.

12 In terms of pulling together a FinCEN Exchange, you would sort of think about who
13 are the right law enforcement partners who were working on the topic or that have
14 expressed an interest in doing an exchange.

15 So I think some of it is sort of organic around the topic, the setting, the mission
16 set.

17 Going back to my Russia example, many of the agencies I mentioned are the
18 agencies you would expect to be working in that space. BIS, the Bureau of Industry and
19 Security, they're very focused on avoiding improper shipments to folks who are not
20 supposed to get them. Same with like oligarch money-laundering assets you would be
21 working with FBI and others; fentanyl you'd be working with DEA and others.

22 So, again, there's sort of -- it can change based on the mission set and setting.

23 [REDACTED] But just to make sure so the record was clear.

24 So I think the record was, how do you decide who to partner with?

25 Mr. Kirby. Oh.

1 [REDACTED] So I just want to make sure the record is clear on, when you
2 were in the role as the AD of the Intelligence Division, would you have been making those
3 decisions?

4 Mr. Kirby. No, I would not. I'm sorry if I missed that.

5 [REDACTED] Who would have been making those decisions?

6 Mr. Kirby. Again, principally that function was housed in the Strategic
7 Operations Division, so I think in that division sort of up to FinCEN front office at the time.
8 But principally I think the Strategic Operations Division would have been the sort of
9 interlocutor and coordinator in that space.

10 [REDACTED] Were those relationships preexisting?

11 [REDACTED] Which relationships?

12 [REDACTED] The relationships with the private sector in terms of the folks that
13 the Strategic Operations Division is interacting with. Are you cold reaching out to
14 institutions, or is there a list of partners FinCEN has?

15 [REDACTED] I think to the extent he knows, since he's just said that
16 would've been housed in a different division at the time and he wasn't the one making
17 those decisions.

1

2

BY [REDACTED]

3

Q Sure. He's the deputy director now.

4

A So maybe I'll -- yeah, let me try that a couple different ways.

5

So some would be longstanding. So, for instance, we have a longstanding

6

partnership with most of your major law enforcement agencies. I don't think that would

7

surprise anyone given the nature of our mission. So we work very closely with the FBI,

8

at times we work very closely with DEA, just given the nature of our mission set.

9

And so with regard to -- so I think if you're asking like do we could call in that space,

10

I think that would probably -- my expectation would be that would be a more organic

11

exchange. Sometimes it's partners want to have a FinCEN Exchange on a topic, have an

12

idea of the topic and the location and how that would be helpful.

13

With regard to private sector components, some may be entities that have

14

interacted with FinCEN in the past. I think some may be those that haven't. And I

15

think the Project Protect series I mentioned before that's focused on fentanyl you have

16

really a focus there on trying to reach regional, local banks to sort of share information

17

with them.

18

So while I don't know specifically how much of those may have involved like

19

someone participating in the exchange had a relationship with bank A, bank B, or bank C,

20

it would not surprise me if in a space of trying to reach out to make sure we're reaching

21

broadly in these spaces that you may -- some of that may be reaching out to a bank or

22

another partner that hasn't previously been in an exchange with us.

23

So I think it may be a mix. Hopefully that answered the question.

24

Q Were there tensions with the private sector? Were there ever

25

disagreements?

1 A So that one you're going to have to help me with being a little bit more
2 specific, because we also house an enforcement function at FinCEN. So that tends to
3 not be a kumbaya space. So if, you know --

4 Q In terms of receiving material or sharing material with the private sector,
5 vice versa.

6 A I think it's important -- one aspect of the FinCEN Exchange I think sometimes
7 that gets lost is that these are voluntary exchanges. They're voluntary. We don't order
8 people to show up at FinCEN Exchanges. The people on BSAAG apply to be on BSAAG.
9 So they're not folks that we've ordered to show up for those events either.

10 So I would say, at least in those types of exchange spaces, you're already starting
11 from a space of folks have asked to be there. And so while I'm not entirely sure what
12 would count as tension, I think you're starting from a space that the people in the room
13 have raised their hand generally to be in the room.

14 Q And you've testified to this, but FinCEN has oversight responsibilities over
15 the financial institutions?

16 A That's correct. We are the administrator of the Bank Secrecy Act, which
17 sets forth a number of anti-money laundering and counterterrorism finance regulatory
18 obligations for U.S. financial institutions and others.

19 Q And did the Intelligence Division have oversight responsibility?

20 A I don't think that's how it would normally be described.

21 So I think the principal role of the financial -- the Intelligence Division in this space
22 would be the analytic expertise that the analysts bring to being able to sort of review the
23 suspicious activity reports and other information that the financial sector and others file
24 with FinCEN pursuant to the Bank Secrecy Act.

25 They may support, in an analytic sense, efforts in, say, the Global Investigations

1 Division, in the sort of 311. I don't know if you all are familiar with that authority. It's
2 a PATRIOT Act authority that allows targeting foreign financial institutions in foreign
3 jurisdictions, a primary money-laundering concern.

4 So, for example, Iran, North Korea are right now designated as foreign financial
5 institutions of primary money-laundering concern, for example. So they may
6 support -- provide analytic support for work like that in that division or they may
7 provide --

8 Q What does that analytic support look like?

9 A It might be looking at things like SARs we receive on a certain topic. So
10 if -- so the -- to take two steps back, to give you a not fentanyl example, because I feel like
11 I'm giving you that example a lot, the Cyber and Emerging Technology Office at FinCEN is
12 housed in the Intelligence Division. It's now full-blown one of the three divisions I
13 mentioned to you before in the organizational structure. That division houses a lot of
14 FinCEN's expertise in that space.

15 So to the extent the Global Investigations Division is looking at using one of our
16 targeting authorities against a foreign illicit finance threat, they may look -- and it would
17 not be uncommon for them to look -- to the analytic expertise housed in that office if
18 they're looking at illicit activity involving virtual assets, things like bitcoin, Monero, Ether,
19 things like that.

20 So that would be a regular area for them to collaborate, the employees in the
21 Intelligence -- the Research and Analysis Division supporting the work of the employees in
22 our Global Investigations Division, maybe our Policy Division, if they're putting together
23 an alert or an advisory on the topic and they're looking to discern sort of filing trends,
24 filing typologies in a certain space.

25 The analysts in the Research and Analysis Division could support that work on a

1 topic that they are already familiar with. So that's what the support would frequently
2 look like.

3 Q And just back to the original question, how does the Intelligence Division's
4 analytics support the enforcement aspect?

5 A So one aspect of that might be -- I think it was -- that one's harder for me,
6 because I'm having a hard time coming up with a specific example of that.

7 But if an enforcement case were evaluating has this financial institution filed
8 with -- SARs with FinCEN that they are supposed to file, that would not be an unusual
9 thing, in my opinion, for someone in the Enforcement Division to reach out to an
10 employee in the Research and Analysis Division or a team in the Research and Analysis
11 Division and coordinate with them, because we also have a data quality metrics team in
12 our Research and Analysis Division who is very sort of good at sort of checking those sorts
13 of things for other teams.

14 Q Coordinate and check in terms of have they filed SARs? Are they filing the
15 things that they should be?

16 A Yes.

17 Q Are they -- okay.

18 A They can also check like how many have they filed. They can also check
19 how many using certain SAR filing codes and things like that.

20 So a lot of the expertise of analyzing the filings that we get is housed in the
21 Research and Analysis Division. There may be employees in other parts of FinCEN that
22 have that expertise as well, but the real -- the sort of concentration of that expertise is in
23 our Research and Analysis Division.

24 Q And changing gears some, did you engage with Google regarding domestic
25 violent extremism?

1 A I do -- no, I do not recall doing that.

2 Q I'd like to now enter an email from Aaron Weiss, Western Union, to [REDACTED]
3 [REDACTED] dated April 19th, 2021, with the subject line "Capitol Riots/DVE" into the record
4 as exhibit 1. Take some time to review.

5 [Kirby Exhibit No. 1
6 was marked for identification.]

7 [REDACTED] It looks like this is just the first page. Is there a beginning of
8 this email, second page?

9 [REDACTED] No. This is the exchange that we're introducing.

10 [REDACTED] Okay. So for the record, is there additional context that
11 began this email chain?

12 [REDACTED] No, there's not.

13 [REDACTED] So there's no emails before the email at the very bottom of this
14 document on this chain?

15 [REDACTED] This could be a part of a larger chain.

16 [REDACTED] Okay. So you don't know one way or the other whether
17 there's any emails before this that would give this context?

18 [REDACTED] I just want to ask about this specific exchange.

19 [REDACTED] Okay, without providing the full document or the full context.
20 That's what I want to be clear on the record, especially since he's not on this email.

21 [REDACTED] And this is the document that we've been -- we've received from
22 a financial institution, and this is the relevant excerpt.

23 [REDACTED], if it's helpful, we can pull up the document production and see
24 what, I think it would be, 256 or 258 says.

25 [REDACTED] I think we just want to know for the record like is this the full

1 email or not.

2 [REDACTED] That's understood, and I think it's noted for the record. But I
3 think we should just move forward with this. I'm not prepared to get into super detail
4 with this email.

5 I just want to ask whether you can describe any conversations FinCEN may have
6 had with Google.

7 [REDACTED] Also noting for the record that he's, of course, not on this
8 email.

9 [REDACTED] Your note has been made for the record.

10 Mr. Kirby. So, yeah, not being on the email, I don't recall ever having seen this
11 email before, and I don't recall any conversations with Google on this topic.

12 [REDACTED] Are you aware of any financial intelligence received from Google
13 regarding the Capitol riots or DVE?

14 Mr. Kirby. No, not that I recall.

15 [REDACTED] Do you know why FinCEN may have been in touch with Google?

16 Mr. Kirby. Beyond what's on this piece of paper, no.

17 [REDACTED] In your role as associate director of the Intelligence Division,
18 would you have -- would Google be one of the private sector entities that you would
19 communicate with?

20 Mr. Kirby. I don't recall having communications with Google in that role. But
21 just given who Google is and what they do, like it wouldn't -- it doesn't necessarily
22 surprise me that FinCEN would have communications with Google. It's just I'm not
23 familiar with this exchange.

24 [REDACTED] We can move on.

25 Mr. Kirby. Okay.

1 Do you want this back?

2 [REDACTED] Sure.

3 [REDACTED] We'll take this back.

4 BY [REDACTED]

5 Q Shifting back again. Does FinCEN have a role in the creation and filing of
6 SARs?

7 A So I'm going to deconstruct your question a little bit, because the
8 creation -- I'm not really sure what that means. But on the filing side, we are the
9 repository for financial institutions when they file SARs. So when you say creation,
10 could I ask what you mean by creation?

11 Q Yes. Does FinCEN ever direct financial institutions to file certain kinds of
12 SARs?

13 A I think the answer to that is no, but I'm not actually sure. Maybe I can put
14 some meat on that because I don't know that's -- I want to make sure I'm complete and
15 clear.

16 We are the administrator of the statute that requires the filing of SARs. And so
17 Congress has set forth a requirement in this regard. The regulations implementing that
18 are administered by FinCEN.

19 FinCEN regularly publishes advisories, alerts, and other sort of public-facing
20 material to advise the financial sector and others of illicit finance threats.

21 So within the last couple weeks we've filed one on fentanyl. We have put -- over
22 the course of this year we have materials that we've published on elder financial
23 exploitation, online exploitation of children.

24 These are things we put out for the sector in terms of trying to share information
25 with the public, particularly the financial sector, regarding illicit finance threats in a way

1 of hopefully helping folks identify this activity, file SARs with FinCEN that are then
2 available to law enforcement to support USG and other efforts to sort of combat these
3 issues.

4 So that's how I would sort of describe our role in that space. I don't think of it as
5 creation; I think of it as we're the administrator of the statute.

6 Financial institutions have the obligation under the regulations in the statute to
7 stand up their anti-money laundering program, identify suspicious activity, file it with
8 FinCEN, and we share information to sort of help them sort of identify suspicious or illicit
9 activity in a number of areas, but not all areas.

10 Q And does the Intelligence Division help identify potentially suspicious
11 activity?

12 A So at the Intelligence Division, now the Research and Analysis Division, it
13 would not be uncommon for analysts in that division to -- so the alert advisory function is
14 principally housed in FinCEN's Policy Division.

15 It would not be uncommon for analysts in the Research and Analysis Division to
16 support their colleagues in the Policy Division with regard to evaluating filings that we've
17 received, looking for information that we could sort of push out to the public and others
18 to sort of, again, help raise awareness of illicit finance threats, but also sort of guide the
19 sector in terms of hopefully being able to identify this type of activity and to file it with
20 FinCEN.

21 Q And how does that analysis occur? What tools are they using? What
22 sorts of things are they utilizing to identify things that may be worthy of sharing a
23 suspicious activity?

24 A Okay.

25 [REDACTED] Could I just -- I think just to --

1 Mr. Kirby. That's a long answer.

2 ██████████ I was just also going to clarify what you mean by identify as
3 suspicious activity, because I think he's just testified a moment ago that that's actually the
4 banks that support suspicious activity and the now-Research and Analysis Division does
5 analysis of that reporting.

6 So when you say identify suspicious activity, can you just explain what exactly you
7 mean by that?

8 ██████████ Yeah. So he also testified that the Intelligence Division helps
9 share materials related to potentially illicit activity and administering the statute, bringing
10 things to the attention of the public.

11 And so I'm asking, when you're analyzing those materials, what does that analysis
12 look like?

1

2 [11:02 a.m.]

3 Mr. Kirby. Here's a couple. I don't want to get too, like, bogged down. I don't
4 think this is a short answer, so I apologize in advance.

5 So some of it is just their expertise in a topic. So, you know, we have -- again, to
6 go back -- sorry I keep going back to this, but I think it is one that is sort of very topical at
7 point -- fentanyl space. We have worked -- we have a close partnership with DEA in
8 terms of identifying and working closely on cases and other matters in that space. So
9 there's a -- there's a familiarity and expertise analysts may have on the topic.

10 There's also the ability to, sort of, identify via key words or the filing code that a
11 financial institution may use for us. So if we've published an -- if we've published a prior
12 document that had -- so, for instance, in the fentanyl space, we have -- there's -- you
13 know, we've previously published in that space.

14 We have a filing code from our last advisory in that space we ask the financial
15 sector to use, identifying -- looking at what we're getting in response to those, sort of,
16 public guidance documents, and evaluating those as to both -- you know, so it's not just
17 the internal piece of that. It's potentially highlighting that to our law enforcement
18 partners or sharing that internally because it may be -- you know, the Policy Division, it
19 may be useful to them in terms of, like, crafting some sort of public document.

20 And then there are other -- you're now going to, sort of, go beyond my, sort of,
21 areas of expertise in terms of the ability to, sort of, engage in data analytics and other
22 things with regard to the filings we have in front of us to identify, sort of, themes,
23 typologies, information and the like.

24

BY [REDACTED]

25

Q And was the Intelligence Division responsible for reviewing SARs?

1 A The Intelligence Division -- the then-Intelligence -- see, I get kind of caught
2 up on this, too. The then-Intelligence, now Research and Analysis Division, like, so they
3 don't review every SAR we get. We get. I think. About 55,000 filings altogether a
4 day. We are an agency of approximately 285 employees.

5 So -- but a big part of their job is -- is identifying the -- is reviewing the filings that
6 we get against the, sort of, prior- -- we have published priorities under the Anti-Money
7 Laundering Act 2020. They're on our website. The statute required us to do that.

8 And so we have -- we have identified a set of AML priorities on our website. We
9 have priorities as set forth by departmental administration leadership. These are sort of
10 long-standing, not different from one administration to the other. They each have their
11 priorities that they want us to focus on.

12 And so they are identifying our filings against these, sort of, priority mission sets
13 whom usually in the context of -- their area of assigned responsibility. So the folks that
14 work on Cyber and Emerging Technology are likely going to be focused on the filings
15 we're getting in connection with things like ransomware or the use of virtual currency to
16 engage in, you know, various illicit things on the internet, like engaging with dark net
17 marketplaces and things like that.

18 So, yes, they do review those materials. They don't review all of them that we
19 get, but it is a key part of their day-to-day function.

20 ██████████ How do employees decide which filings to review? If you're
21 getting 55,000 a day, are you just hoping the ones you review lead to something?

22 Mr. Kirby. So I think there's a couple answers to that question, too.

23 One is actually, sort of, going back to what I mentioned before with regard to the
24 filing codes. You know, one of the advantages of, you know -- pick a topic, fentanyl,
25 elder financial exploitation, ransomware, anywhere we have a published code. One of

1 the reasons we encourage financial institutions to use the code is it makes it much easier
2 for our analysts and our law enforcement partners to identify the filings that would come
3 in on ransomware, elder financial exploitation, et cetera.

4 And then the other are these, sort of, like, analytic tools -- which, again, you're
5 now escaping my -- sort of the outer bounds of my expertise in that regard. No one will
6 ever confuse me with a computer programmer. And so there are a variety of tools that
7 can be, sort of, deployed in that space.

8 [REDACTED] So is FinCEN using artificial intelligence or machine learning to
9 sort through this?

10 Mr. Kirby. I don't -- I don't -- I believe the answer to that is no. I do not believe
11 we're using artificial intelligence. That's my current understanding.

12

BY [REDACTED]

13 Q Are there any --

14 A But you may search -- just to, sort of, finish that thought. But it wouldn't
15 be inappropriate -- or it wouldn't be unusual is a better way of putting it -- for someone to
16 be searching for key words in filings.

17 So even if -- and by that I don't mean the key word the filer used. I mean a SAR
18 usually includes a narrative section, for example. So they may search the narrative
19 section for, sort of, key words, typologies, perhaps the names of certain cartels, for
20 example.

21 So, you know, there is the ability to, sort of, search across documents. You're
22 not just, sort of, like, clicking through every document that came in yesterday sort of
23 thing.

24 Q Are there any codes or typologies that aren't published?

25 A I don't know the answer to that question in a, sort of, definitive way. My

1 expectation would be that most are -- most are public. But I actually don't know if there
2 are others that may not be over time.

3 Q Do you know if financial institutions are using artificial intelligence or
4 machine learning to identify potentially suspicious activity?

5 A I don't know the answer to that in a definitive way. I know that it is an area
6 of interest, but I don't -- I don't know the degree to which -- the degree to which people
7 are varying degrees down the road in that regard.

8 Q You mentioned that it's an area of interest. Could you explain a little bit on
9 that --

10 A Well, by that I mean -- and, frankly, I'm going by just what I read in the
11 papers on that principally of, you know, there's just -- I think there is -- one of the aspects
12 of the Anti-Money Laundering Act was, sort of, a drive to think about different ways to
13 reduce regulatory burden.

14 And so, you know, just from what I read in the press, there's a fair amount of
15 discussion about different ways. AI could be deployed in not just the financial sector but
16 other sectors in the future. But I don't have any sort of specific definitive knowledge of
17 where things are in that regard.

18 Q Does FinCEN ever notify law enforcement of particular SAR filings?

19 A Yes.

20 Q And how does that notification process occur?

21 A I don't know that there is a specific, sort of, definitive, it's always this way,
22 but I don't -- my understanding is that I don't think it would be uncommon. Going back
23 to my, you know, fentanyl example, if an analyst saw something they knew was relevant
24 to a DEA case that they were supporting, they might alert the DEA agent to that.

25 Similarly, you know, to the extent we receive filings on ransomware -- you know,

1 there's a fair amount of interest in combatting ransomware, so to the extent we have
2 relevant filings to that mission set, making the relevant law enforcement agencies aware
3 of that fact is something that I understand happens.

4 [REDACTED] We can go off the record.

5 [Recess.]

6 [REDACTED] We are back on the record.

7 EXAMINATION

8 BY [REDACTED]

9 Q Mr. Kirby, you mentioned that you were FinCEN's chief counsel for
10 approximately five years. Is that correct?

11 A Altogether, including actings, yeah, almost five years.

12 Q And so I imagine that you are then well-versed in statutory and regulatory
13 authorities pursuant to which FinCEN operates?

14 A I would like to think so, yes.

15 Q I would certainly hope so. And also the ones that --

16 A You know, we'll see.

17 Q As well as the authorities that FinCEN helps to administer that you discussed
18 earlier?

19 A Yes.

20 Q And you used the term financial intelligence a few times during the previous
21 hour. Can you explain exactly what financial intelligence is.

22 A So when we use that term at FinCEN, we tend to be referring to the
23 information that is filed with us pursuant to the Bank Secrecy Act. So that would be
24 things like suspicious activity reports, forensic transaction reports, you know, those types
25 of reports that financial institutions and others file with FinCEN under the BSA.

1 And when I say BSA, Bank Secrecy Act. I'm trying to watch the acronyms, so --

2 Q Thank you. And just so you know, I'll be saying BSA regularly.

3 A Okay. Okay. Good.

4 Q Can you explain at a high level how the BSA and the financial intelligence
5 that FinCEN obtains through it, how does that help keep Americans safe?

6 A Well, the overarching purpose of the Bank Secrecy Act is set forth in the
7 statute to essentially -- to, sort of, generate reports helpful to law enforcement, helpful to
8 regulatory exams, you know. The purposes are expanded under the AMLA. It also
9 includes, sort of, like, tracing criminal proceeds and things like that.

10 So, you know, I think in terms of keeping people safe, suspicious activity reports,
11 we hear pretty consistently from our law enforcement partners, are a critical tool for
12 them in terms of combatting an array of financial crimes. I'll sort of come back to a
13 topic I mentioned before, you know, be it elderly -- elder financial exploitation. You
14 know, we've done -- we have a lot out in the space.

15 That's an area where, you know, a lot of financial institutions really are on the
16 front line with regard to the risk of things like so-called grandparent scams or romance
17 scams or things like that.

18 And we've worked hard to get information out to the sector in that topic and
19 some others to sort of alert, you know, the folks who may encounter that firsthand,
20 things they could be on the lookout for in terms of red flags, typologies of how that
21 works, et cetera.

22 Q But illicit finance doesn't just refer to crimes that are themselves financial,
23 but also just transactions that further other crimes, like violent offenses or drug
24 trafficking, for example. Is that fair to say?

25 A Yeah, I think that's fair to say.

1 Q Okay. We had a witness from the FBI tell us an example of a situation
2 where he was able to use SARs to identify somebody who was making, I believe it was,
3 bond-making equipment and was able to prevent what seemed like it could have been a
4 very serious tragedy.

5 Does that surprise you that SARs would be helpful in that regard?

6 A No. I mean, my understanding is they are -- they are useful and helpful in a
7 wide array of efforts to combat criminal activity.

8 Q I want to take a step back and ask you about FinCEN's mission. I believe
9 you stated the mission during the previous hour, but I missed some of what you said.
10 So if I could ask you to repeat that, I'd appreciate it.

11 A Sure. And I probably gave you the truncated version. I'm not sure I
12 always get the full thing from memory, but it's -- you know, our principal goal is to
13 support safeguarding U.S. financial system from illicit and criminal use and to support,
14 you know, law enforcement and other efforts to, sort of, combat those actions through
15 the strategic analysis of financial intelligence and other information. That's, essentially,
16 in a nutshell, what we do.

17 Q Your website -- or FinCEN's website. I'm not going to give you ownership of
18 it -- says that FinCEN's mission is to safeguard the financial system from illicit use and
19 combat money laundering and its related crimes, including terrorism, and promote
20 national security through the strategic use of financial authorities and the collection,
21 analysis, and dissemination of financial intelligence.

22 Does that sound right to you?

23 A Yes. That's much more articulate than the way I put it.

24 Q Well, it's a lot easier when you're -- when you have the time to sit and type it
25 up or copy it from -- from the internet, as I just did.

1 So one of the things that FinCEN focuses on is combatting the use of financial
2 systems to finance terrorism, correct?

3 A Yes.

4 Q And that is often referred to by the acronym of CFT, combatting the
5 financing of terrorism?

6 A Yes.

7 Q And FinCEN's Anti-Money Laundering activities are referred to often as AML
8 or --

9 A Correct.

10 Q -- generally in the field of -- in this field that acronym is used.

11 In FinCEN's work in countering the financing of terrorism applies to international
12 terrorism but also domestic terrorism here in the United States, correct?

13 A Yes.

14 Q FinCEN is not a new bureau or agency? I mean, it was established by
15 Congress in 1990. Is that right?

16 A We were initially established, I think, by the Department and then
17 Congress -- I think it was in the Patriot Act, but don't -- we can confirm that -- formally
18 established us as a bureau within the Department reporting to the Under Secretary for
19 Terrorism and Financial Intelligence.

20 Q Okay. My understanding is that in 31 United States Code Section 310 in
21 1990 FinCEN was codified as a bureau within --

22 A I will take your word for that then.

23 Q -- the Treasury Department. Thank you.

24 Separate and apart from FinCEN's regulatory function, in terms of its
25 information-sharing function, would you say that FinCEN essentially works as, sort of, a

1 clearinghouse for law enforcement, the Treasury Department, and financial institutions to
2 share information about trends and issues that they're seeing in illicit finance?

3 A I think that's a fair description. Yes.

4 Q And you talked during the previous hour a little bit about FinCEN's work or
5 collaboration with law enforcement agencies.

6 Why is it important for FinCEN to work with law enforcement agencies?

7 A You know, I think that's, sort of, one of the key functions that Congress has
8 set out for us in the Bank Secrecy Act.

9 When you look at the purposes of the statute, many of them involve combatting
10 criminal and other illegal activity in terms of making information available to them, you
11 know, that's the -- the sort of -- that's sort of embedded into our statutory, sort of,
12 overlay and construct.

13 So it's set forth for us as a key portion of our mission in our statutory -- in our, sort
14 of, overall statutory construct is at least in my mind how I would think about it.

15 Q So is it fair to say that Congress has directed FinCEN to work with law
16 enforcement to help in combatting illicit finance and the various crimes we've talked
17 about?

18 A Yeah. I see that as a key component of our underlying statutory structure.

19 Q And would you say that it's also a key component of your underlying
20 statutory structure to work with financial institutions and share information with them to
21 help them identify illicit transactions or suspicious activities that -- that could be related
22 to illicit conduct?

23 A I do. I see that sort of connecting back in a couple of different ways. You
24 know, one is we are the administrator of the statute, and the goal of the statute is -- at
25 least with regard to SAR filings is, you know, for the -- you know, the statutory construct

1 sets out, you know, the types of information that should be filed with FinCEN in this
2 regard, and as administrative statute see this, sort of, consistent with that in terms of the
3 sharing information that can help those subject to these rules better comply with them.

4 And then, as I said before, you know, the overarching, sort of, purposes section of
5 the statute lays out a number of purposes that involve combatting criminal activity as,
6 sort of, the key functions of the overall statute.

7 Q And --

8 A I'm missing my statute book right now because, as a lawyer, that's what I
9 would be, like, reaching for to actually read it back to you. So I'm -- I'm sorry in that
10 regard.

11 Q I've got Section 310 here. I can --

12 A Actually, the section I was referring to is actually 5311, which lays out the
13 purposes of the overall statute and will sort of lay out all of these different functions that
14 the reporting is meant to support.

15 Q Thank you. And we're going to talk about some of the other statutes
16 briefly as well.

17 But FinCEN is required by statute to maintain a database as a repository for SARs,
18 correct?

19 A Yes, that is correct.

20 Q And to make that database available to law enforcement?

21 A Yes, that is correct.

22 Q And FinCEN is required by statute to analyze and disseminate the data it has
23 and to issue guidelines to help identify criminal activity to appropriate federal, state,
24 local, and tribal law enforcement authorities, correct?

25 A Yes. That is correct. It looks like you have our statute in front of you. So

1 that all sounds right to me.

2 Q And FinCEN is required by statute to establish and maintain a financial
3 crimes communication center to furnish law enforcement authorities with intelligence
4 information related to emerging or ongoing investigations, correct?

5 A Yes.

6 Q And all of this work FinCEN is doing by statute in the interest of detection,
7 prevention, and prosecution of terrorism, organized crime, money laundering, and other
8 financial crimes, correct?

9 A Yes.

10 Q And you've talked about some of them at length during the previous hour, in
11 particular fentanyl, which seems to be a big focus.

12 But there's a wide range of crimes that FinCEN helps to -- helps financial
13 institutions to identify transactions that support those crimes, correct?

14 A Yes, that is correct.

15 Q You mentioned financial abuse of elders, I believe you mentioned some sort
16 of child sexual abuse?

17 A Online child sexual exploitation and child sexual abuse material.

18 Q Obviously, we have international and domestic narcotics trafficking --

19 A [Nonverbal response.]

20 Q -- terrorism?

21 A Yes. I'm sorry. I caught myself as soon as -- no nodding. Yes.

22 Q And I'm the only person who didn't catch it.

23 So I want to ask you a couple questions about the Bank Secrecy Act and how it
24 functions.

25 First of all, Bank Secrecy Act has been around for over 50 years. Is that right?

1 A Yes. I think -- I believe the, sort of, initial statute is an early 1970s statute.

2 Q And it's the Bank Secrecy Act that requires financial institutions to file
3 suspicious activity reports, or SARs, correct?

4 A The statute, in conjunction with regulations that have been promulgated by
5 the Treasury Department over the years.

6 Q And under those statutes and regulations, banks are legally obligated under
7 the Bank Secrecy Act to file a SAR for certain transactions that are relevant to a possible
8 violation of criminal law, including terrorism, correct?

9 A That's correct, but it's actually a little broader than that. It's possible -- a
10 relevant or possible violation of law or regulation.

11 Q Thank you for that.

12 A I actually don't think there's a criminal qualifier in front of law. So it's any
13 potential violation of law or regulation would meet the standards set forth in the statute
14 or regulation.

15 Q It could be a civil law?

16 A It could involve civil enforcement. And there's a -- and you may be getting
17 to this, but there's a conjunction to that.

18 There's the mandatory requirement and then there's the ability to voluntarily file,
19 as the statutory construct laid out by Congress really is to encourage filing. So
20 you -- there's the ones you're required to file, but there's also very much an
21 encouragement for people to voluntarily file beyond what they're required to file.

22 Q And -- but there is that first section, which is mandatory, correct?

23 A Correct, yes.

24 Q And that means that if a bank fails to appropriately identify transactions that
25 fall within those mandatory requirements, they could face penalties?

1 A Correct, yes.

2 Q And it would be FinCEN that would make that determination?

3 A Yes. And FinCEN -- and at least with regard to banks and credit unions, we
4 would normally be in close consultation with the relevant functional regulator in that
5 space for the financial institution in question.

6 Q Okay. Law enforcement agencies use information that they obtain from
7 FinCEN's database from the SARs in both proactive investigations in terms of helping to
8 prevent crime and also reactive investigations, helping to -- once a crime has occurred,
9 helping to identify the perpetrators. Is that correct?

10 A That sounds correct to me, yes.

11 Q And that's across all of these different types of offenses and threats to
12 national security that we've discussed?

13 A That is my understanding, yes.

14 Q Based on your experience and over nearly 20 years at the Treasury
15 Department, what would happen, in your opinion, if Congress were to roll back the Bank
16 Secrecy Act and stop requiring or even permitting banks to file suspicious activity reports?

17 A So that's a hard question for me to answer in the sense that, you know,
18 those are -- those are policy decisions that I often, sort of, feel like are beyond my
19 agreement in the first instance without, sort of, consultation above. So I'll sort of start
20 with that qualifier.

21 You know, I maybe would answer your question, if it's okay, a slightly different
22 way and would go back --

23 Q Sure.

24 A -- to what you said before about the role of these filings that we hear pretty
25 consistently from law enforcement are incredibly useful to them in a variety of

1 investigatory ways.

2 And, you know, we -- one of the, I think -- could be safe to say that one of the
3 goals of the Anti-Money Laundering Act of 2020 was to, sort of, put on us as an agency
4 the obligation to, sort of, provide more, sort of, public visibility and feedback into the
5 utility of the information that we're getting.

6 So over the last couple of years, you've seen FinCEN start publishing things, like a
7 year in review, that lays out, with input from law enforcement, you know, the different
8 ways they use the information that's made available to them from -- you know, from our
9 holdings. Or a relatively new product line for us, another sort of AMLA obligation, our
10 financial trend, financial threat analysis reports that are also available on our website, and
11 that is, sort of, walking through, you know -- and we're required to at least two a year,
12 but I think we're ahead of the two this year.

13 And that's where we're -- things like -- we published one earlier this year on online
14 child sexual exploitation. We published one on elder financial exploitation, I believe it
15 was this year as well. We've published them on ransomware and other things like that.

16 So, you know, one of the things that is, sort of, incumbent upon us under our
17 statutory authorities now is actually, I think, to show more, sort of -- to give more public
18 visibility into the value of the information that we get. We're trying to do that in a
19 variety of ways.

20 Q Those year in review reports, do they provide examples of, here's an
21 investigation where SARs were helpful? This is --

22 A I don't know if they go quite that far. But we have another publication that
23 does some of that, and that is every year -- there may have been a hiccup during COVID.
24 But usually most years -- let me phrase it that way -- FinCEN does the director's law
25 enforcement awards where there's an effort actually -- law enforcement agencies can,

1 essentially, highlight cases where BSA filings have been instrumental to the underlying
2 investigation, and we publish summaries of those on our website. So, again, to give
3 some visibility to the different ways the information is used.

4 Q And so in that situation, the director is awarding law enforcement for --

5 A Yes.

6 Q -- their service in --

7 A The law enforcement agency may get, like, an award recognition
8 from -- from the FinCEN director in response to those nominations that we receive.

9 Q You stated in the earlier hour that typically the process with SARs is a
10 financial institution files a SAR with FinCEN, and then it goes into a database where it's
11 made available to law enforcement, correct?

12 A Correct.

13 Q And FinCEN itself is not investigating the potential crime to which the SAR
14 relates?

15 A So FinCEN is not a criminal law enforcement agency. So we would not be,
16 in the first instance, investigating criminal activity. However, our analysts do provide a
17 lot of support on those -- on, sort of, priority topic areas.

18 -- and, again, to go back to fentanyl, you know, so our analysts may be doing
19 analysis of the information we get in that space both in support of our law enforcement
20 partners, but also, you know, Treasury is the -- Treasury -- sort of above us Treasury is the
21 administrator of the sanctions programs in the narcotics space. And we -- we have our
22 own, sort of -- as the department efforts to combat fentanyl trafficking and things like
23 that.

24 So FinCEN analysts can be supporting law enforcement, and that work could also
25 support the department's broader efforts in this space as well.

1 Q Thank you for that clarification. I want to go back to something that we
2 talked about a few minutes ago.

3 You mentioned there's the mandatory SARs reporting and then the voluntary SARs
4 reporting.

5 The voluntary SARs reporting allows banks to report any transaction that may be
6 potentially relevant to any violation of law or regulation regardless of how small that
7 transaction is. There's no -- there's no threshold for voluntary reporting, correct?

8 A That -- that is my recollection, yes. I think that's correct.

9 Q And you also stated --

10 A And I should add, actually, the safe harbor applies to both.

11 Q Can you explain what that means?

12 A So the statute sets forth a safe harbor for mandatory filings, the ones you're
13 required to make, and the statute extends the safe harbor to any that you -- really, again,
14 going back to the, sort of, encouraging filings. So you can't -- I don't have the exact
15 language in front of me, and I should have the exact language in front of me before I
16 speak to it.

17 But it, essentially, provides legal protection for any institution that chooses to file
18 suspicious activity with us if it's required or not.

19 Q So, essentially, is it fair to say that it means the banks can't be held liable for
20 disclosing that information?

21 A I think that's correct. That's probably a concise way of putting it.

22 Q Now, SARs are made available to law enforcement agencies, but they are
23 also subject to strict confidentiality provisions under the law, correct?

24 A Yes.

25 Q And FinCEN takes those -- its responsibilities to maintain the confidentiality

1 of SARs very seriously?

2 A Yes. That's -- it's very important for us to do that.

3 Q And I believe you stated earlier that FinCEN is receiving approximately, did
4 you say, 55,000 SARs a day?

5 A I think we receive 55,000 BSA filings a day, which is all forms. And as I say
6 that out loud, that may be an old stat.

7 But we get a decent number of filings per day across all the filing sets that we
8 have.

9 Q Can you explain what some of the other filing sets are?

10 A So we also receive currency transaction reports. Those are the -- for folks
11 who may not be familiar with them, if you go to a bank and clunk down \$11,000 in cash,
12 they will fill out this -- it's the one I feel like people are most familiar with with FinCEN
13 because they've seen it in, like, movies and stuff. So that's one.

14 There is a -- the form when you cross the border with more than X number of
15 dollars, that's also a FinCEN form. And there's a nonbank counterpart to the currency
16 transaction report that requires the reporting of certain transactions by nonbanks in
17 excess of \$10,000 as well.

18 Q With respect to those currency transaction reports, that's a requirement that
19 any transaction in excess of \$10,000 be reported, correct?

20 A Yes. And there's a requirement to aggregate in connection with that. So
21 if you go to three branches of the same bank in the same day, the bank would aggregate
22 those up, and if it exceeds the 10,000, they would file a currency transaction report.

23 Q And that's different than a suspicious activity report, correct?

24 A Different from a suspicious activity report, yes.

25 Q But you could have a situation where the requirement of a currency

1 transaction report evolves into something that triggers a suspicious activity report. For
2 example, somebody goes to the bank to deposit \$10,000. They're told they have to fill
3 out this report, and then they say, I'll just do 9,000. How about that? That might --

4 A Yes. That would be called a structuring SAR, and -- I'm sorry. That would
5 be called structuring. And a financial institution would normally file a SAR with someone
6 indicating they're seeking to avoid a regulatory obligation.

7 Q And you stated during the previous hour that FinCEN does not review all of
8 these -- I mean, there's millions per year, correct?

9 A Correct. Yes, we do not review all of them.

10 Q And law enforcement does not review all of them?

11 A That is correct.

12 Q So it's fair to --

13 A That is my understanding, I should say. I've never actually worked at a law
14 enforcement agency, so I'll say that is my understanding.

15 Q The Bank Secrecy Act is the legal process that authorizes banks to file
16 suspicious activity reports, correct?

17 A The Bank Secrecy Act and the regulations implementing the Bank Secrecy
18 Act, yes.

19 Q And that also allows the -- the Bank Secrecy Act and its implementing
20 regulations also allow financial institutions to provide the supporting documentation
21 underlying a suspicious activity report --

22 A Yes, that is correct.

23 Q -- to FinCEN or law enforcement?

24 A To -- I know for FinCEN, yes. I think for law enforcement, too, but I also
25 know that law enforcement has their own, sort of, authorities in that space as well, sort

1 of, separate from ours.

2 BY [REDACTED]

3 Q A couple minutes ago you were asked about the confidentiality protections
4 for SARs. Do you recall that quick line of questioning?

5 A Yes.

6 Q And you were asked SARs are subject to strict confidentiality protections
7 under the law, and you said yes. You recall that?

8 A Yes.

9 Q Could you explain your understanding of what those confidentiality
10 provisions or protections are?

11 A The statute sets forth very broad protection for -- to prevent the
12 unauthorized disclosure of SARs. And so, basically, any use beyond the official purposes
13 and official purpose, and the prohibition applies to financial institutions, their employees,
14 their directors. It also applies to government employees and contractors as a means of
15 safeguarding the data, given the sensitivity of the data as a means of safeguarding the
16 data.

17 Q And with respect to FinCEN in particular, does FinCEN have particular
18 structures or procedures or regulations in place that pertain specifically to FinCEN
19 employees that -- to protect these -- protect the confidentiality of these SARs?

20 A So with regard to partner agencies, they enter into MOUs with us in terms
21 of -- and they sort of agree and recognize the sort of -- the need to protect the
22 confidentiality of the information.

23 And then with regard to employees, yes, it's part of the, sort of, conduct
24 obligations that would attach to any FinCEN employee that you have to respect the
25 confidentiality of this information. I believe -- but I should double-check this. I believe

1 that all employees that have access to the database have security clearances. And,
2 again -- and a sort of background investigation comes along with that in terms of ensuring
3 they should have access to this and other, you know, sensitive information.

4 So there are a variety of, sort of, technological but also just policy-based
5 restrictions on people's activities in this regard.

6 Q And are you familiar with what might happen to an employee if they are
7 careless with a SAR or if they intentionally were to leak a SAR or to make a SAR available
8 outside of the group of individuals that should have access to it?

9 A I am familiar with that. So -- and this is a space where, you know, if we
10 have concerns like that, we refer the matter to our Office of Inspector General and our
11 office of inspector general has taken action in the past in connection with potential
12 improper conduct in this regard.

13 Q And could that action include, for example, an employee losing their job?

14 A Yes, it could.

15 Q Thank you.

16

BY [REDACTED]

17 Q Now, you talked about this a little bit earlier, but I want to get into it in some
18 more detail.

19 It's the financial institution's responsibility to determine when, pursuant to the
20 BSA and its implementing regulations, they must file a SAR, correct?

21 A Yes, that is correct.

22 Q It's not FinCEN's responsibility to tell a financial institution -- and I'm going to
23 use the word bank to mean financial --

24 A Right.

25 Q -- institutions generally just because that's a mouthful.

1 It's not FinCEN's responsibility to tell a bank, you have to file a SAR for X
2 transaction or X pattern?

3 A That is correct.

4 Q And in order to meet this responsibilities under the Bank Secrecy Act,
5 financial institutions are required to have their own anti-money laundering and
6 countering the financing of terrorism programs, correct?

7 A Yes, that is correct.

8 Q And that's actually a requirement that is codified by statute?

9 A Yes. It's both in the statute and in regulations implementing the statute.

10 Q And those AML and CFT programs must be designed, among other things, to
11 ensure the institution's compliance with the BSA and to assist them in detecting and
12 reporting suspicious activity, correct?

13 A Yes, that is correct.

14 Q And while FinCEN provides general guidance and oversight of banks
15 concerning what constitutes an effective AML/CFT program, it's ultimately the bank's
16 responsibility to ensure that those programs are effective, correct?

17 A Yes, that's correct.

18 Q And it's the bank's responsibility to ensure that they file SARs in accordance
19 with the law?

20 A Yes, that is correct.

21 Q And it's the bank's responsibility to ensure that their programs effectively
22 detect and report suspicious activity on their networks, correct?

23 A Yes.

24 Q And most financial institutions, at least the larger major ones, have entire
25 units dedicated to their anti-money laundering and countering finance of terrorism units,

1 correct?

2 A That is my understanding, yes.

3 Q I mean programs. Excuse me. And those institutions have investigators,
4 people whose job it is, to analyze their customers' data, regularly search and monitor
5 them to identify suspicious activity --

6 A Yes, that's my understanding.

7 Q -- is that fair to say?

8 And based on your understanding of the applicable statutes and regulations, that
9 type of monitoring by a bank of its own customers' activity is -- that's entirely legal,
10 there's no issue there?

11 A I'm not aware of any legal issue with a bank doing that.

12 Q And you're aware, I imagine, that nearly 50 years ago the Supreme Court
13 ruled that the Fourth Amendment, for example, does not apply to bank records,
14 customers' bank records, because those records are the property of the bank, not the
15 private records of the accountholder, correct?

16 A That is my -- that is my recollection of that holding, yes.

17 Q And you stated earlier that banks can incur civil penalties or have civil
18 penalties and fines imposed on them for failing to file SARs.

19 In the appropriate circumstances they can also face penalties for, generally
20 speaking, not having an effective program design to root out suspicious activities,
21 correct?

22 A That is correct, yes.

23 Q So I want to talk about -- move on to talk about FinCEN exchanges a little bit
24 and how they work with banks to help banks meet their responsibilities under the BSA.

25 Information-sharing between banks and agencies through FinCEN exchanges and

1 other means help -- helps to inform banks about law enforcement priorities and identify
2 current trends in terrorist financing, money laundering, and other offenses, like fentanyl
3 trafficking, correct?

4 A Yes. I think that is correct. And the Project Protect series of exchanges
5 that we're doing this year in the fentanyl space, I think, is a good example of that.

6 Q So -- and in those exchanges, sometimes -- well, let me back up.

7 Those exchanges are often a two-way street in terms of information-sharing,
8 correct?

9 A Yes. The goal is for it to be a -- for it to be a sharing of experience and
10 information.

11 Q So the banks are sharing what they're seeing in their own customers' data,
12 and law enforcement is sharing with the banks the trends and the methodologies that
13 they're seeing. Is that fair to say?

14 A I think that's a fair statement, yes.

15 Q And the goal is that this information-sharing will help lead to more effective
16 and efficient SARs reporting by banks, correct?

17 A Yes, I think that's also a fair statement. Again, the Project Protect series in
18 the fentanyl space, I think, is a good example of that.

19 Q And those types of exchanges help if you have more effective, more
20 targeted, more efficient reporting by banks, that's going to help law enforcement detect
21 and deter criminal activity more effectively. Is that fair to say?

22 A I think that is our goal, yes.

23 Q Okay. And you stated earlier that, while the FinCEN Exchange program was
24 codified in 2020, just a few years ago, FinCEN exchanges have been operating before
25 that? There was a prior iteration?

1 A Yes, that is correct.

2 Q And can you explain a little bit about how those prior iterations worked or
3 how they differ from the current FinCEN exchange program?

4 A Let me see when they started. I think they started about two-ish, give or
5 take, years prior to the codified one -- the current codified version. I don't actually
6 know that there is a substantial difference in terms of what the goal of the exchange is
7 than in the way they function now.

8 But my understanding is that the perception was that these were a very positive
9 way of having public-private partnership, and that was one of the things that led Congress
10 to pick up the program and codify it in the statute, in the Anti-Money Laundering Act of
11 2020.

12 Q So, essentially, Congress thought it was valuable enough to make it a
13 statutory requirement so that FinCEN couldn't just decide one day we don't have the time
14 or the resources to do this?

15 A My understanding is that they were generally viewed as a very positive
16 thing, and that's how they got picked up and added to the statute. But that's a -- that's
17 a -- that's old memory at this point, so I need to add that qualifier.

18

BY [REDACTED]

19 Q When you say they were generally viewed as a positive thing, who viewed
20 them as a positive thing? Was it the government? Was it the private sector? Was it
21 law enforcement? Some combination thereof?

22 A Our law enforcement partners, my understanding, we get pretty positive
23 feedback on the ability to have these exchanges. I think we've heard similarly positive
24 feedback from the financial sector.

25 But also, I would say, maybe taking a step back from that, I don't remember if it

1 was y'all's questions or y'all's questions, but we -- one of the things we talked about
2 earlier is that one of the goals if the statute is to, sort of, create more public-private
3 feedback.

4 So there's conversations, there's -- there's some of the other materials we're
5 putting on our website with regard to the value of the data, sort of, throughout the
6 Anti-Money Laundering Act are different ways that FinCEN is being asked to either, you
7 know, engage in more public-private partnership or share more output with regard to the
8 value and utility of the data that we're getting.

9 So it's sort of, in my mind, kind of part and parcel with a lot of the other things
10 that are set forth in the statute for us to do.

11 Q Understood. I think -- my point is just that when you say that the exchange
12 is reviewed policy, the private sector viewed them positively, as well as law enforcement,
13 as well as government entities?

14 A I think that's right. And the fact that they've always been voluntary. So,
15 you know, the only people who show up are people that want to be there. So if you
16 don't want to be there, you don't come is sort of my view -- would be my view at the end
17 of the day.

18 So the fact that people continue to use the space and continue to sort of share
19 information in the space, to me, that is a testament to the perceived continued value of
20 the exchange.

21 Q Thank you.

22

BY [REDACTED]

23 Q Now -- well, before I -- I want to follow up on that voluntary nature of it, but
24 I just want to step back for a minute.

25 The Anti-Money Laundering Act of 2020 -- which I believe you referred to earlier

1 as AMLA. You used that acronym.

2 A That's the acronym we used for that, yes.

3 Q That was passed in December of 2020, correct?

4 A Either that or, like, the first or second day of January 2021. It was like --

5 Q It was effective in --

6 A -- right in that -- right in that end of year, right at the beginning of the next.

7 Q So it actually went into effect just days before the attack on the Capitol?

8 A Yes, I think that's correct.

9 Q And you're aware that that bill had broad bipartisan support?

10 A Yes, I am.

11 Q Now, FinCEN exchanges, including the ones that were set up in the
12 aftermath of January 6th, operate under all the permissible legal authorities, including
13 the Anti-Money Laundering Act, Section 310, Section 53 -- 53? 58? The Bank Secrecy
14 Act --

15 A Yeah --

16 Q I'm going to -- I don't --

17 A There's a bunch of weird statutes get rolled into that. But yes, I think the
18 answer to your question is, you know, the program at large does operate under these
19 various legal authorities, and FinCEN takes its responsibility under those legal authorities
20 very seriously.

21 Q Now, during the previous hour, you mentioned several times about -- I think
22 you might have been asked as well about FinCEN providing typologies to financial
23 institutions.

24 Can you explain what a typology is in this context?

25 A Sure. So maybe I'll juxtapose that with red flags because I feel like those

1 tend to be the terms people use a lot in this space.

2 At least in my own mind, typology -- and I think this is sort of laid out -- would be
3 reflected in our public documents. Typology, to me, is sort of an overall way someone
4 goes about conducting some sort of illicit activity. And, you know, to go back to a
5 document that I mentioned before, we've previously published an advisory on elder
6 financial exploitation, and one of the typologies set forth in that document is the, sort
7 of -- what I think is commonly referred to as the grandparent scam, of someone calling
8 up, purporting to be a law enforcement official, purporting to be someone else, there's an
9 emergency with regard to your grandchild, your whoever, and we need you to send us
10 money, like, ASAP to deal with this situation. That's sort of an overall typology in my
11 mind.

12 A red flag would be a data point that may be indicative of the broader typology.
13 SO in that same document you would see as a potential red flag, if you're in a financial
14 institution, the person on the other side of the counter is referencing, you know, my
15 grandchild has been arrested in X place, I need to get X number of dollars to send to, like,
16 bail him out of jail. But you notice that the email -- the, sort of, money destination
17 or -- doesn't actually look like an official destination. That could be -- that could be a red
18 flag that this broader typology of elder financial exploitation is, sort of, going on.

19 So I don't know if that answers your question. But I view the typology as the,
20 sort of, overarching way something, you know, illicit may be happening. And then the,
21 sort of, individual red flags may be data -- data points that point to the overarching either
22 typology or to the illicit conduct.

23 Q So what I took from what you just said is that the typology is almost like a
24 fact pattern of this is -- this is how this particular scheme is working or this particular
25 criminal offense is -- I mean, not all, obviously --

1 A Yeah. And there could be multiple typologies.

2 Q Of course.

3 A And so -- but I think that's a fair -- I think that's a fair statement.

4 Q And so if a financial institution or a FinCEN is sharing a list, for example, of
5 terms that could potentially be indicative of suspicious activity, that would be more of a
6 red flag in your mind as opposed to typology?

7 A That sounds right to me.

8 Q And do you think that -- or have you experienced sometimes people in this
9 space using those terms interchangeably?

10 A Yes.

11 Q So sometimes people --

12 A Which is why I wanted to juxtapose them, as I think oftentimes they get
13 interchanged for each other. At least I think it's helpful to think of them -- I think they
14 say something slightly different.

15 Q So when FinCEN provides, whether it's passing on from law enforcement or
16 through its own analysis, either a typology or a set of red flags to a bank, is it instructing
17 banks to file SARs for any transaction they see that fits that -- that information they were
18 provided?

19 A No. And something we -- I think this is pretty standard across all of our
20 public products that, sort of, lay out typologies and red flags.

21 We often have a statement before the red flags that says something along the
22 lines of no individual or even, sort of, collection of red flags is necessarily indicative of
23 illicit activity. The thought is this information is shared with the sector that they can,
24 sort of, be aware of these data points, but sort of ingest them against a broader backdrop
25 of their know your customer, the, sort of, knowledge of your customer and transaction

1 set to sort of further inform the overall picture they have in the specific situation.

2 So we try to be careful in the -- in the public space to say that in our public
3 products.

4 Q And that's important because FinCEN is aware that banks know their
5 customers far better than FinCEN does. Is that fair to say?

6 A I think that is fair to say.

7 Q And is it your --

8 A We would expect them to know their customers better than we -- than we
9 know them.

10 Q You would certainly hope so.

11 Is it your understanding that when banks are looking or trying to identify
12 suspicious activity that they consider a variety of factors, not just information that they
13 might receive from law enforcement or from FinCEN, but their own knowledge of their
14 customers, their history, their transaction patterns, that sort of information?

15 A Yes. That's my understanding.

16 Q And when FinCEN passes along typologies or red flags, these are suggestions
17 to the bank of things to look out for, correct?

18 A You know, I'm not sure I would say suggestions. I think I would say, you
19 know, this is -- you know, we're trying to share information, so sometimes it may be
20 closer to us -- going back to my -- my elder fraud example, you know, these are typologies
21 we see in this space, and we're sharing them with you so that you're aware of them.

22 I don't -- I view them as more of an information-sharing exercise than a, sort of,
23 suggestion-based exercise. I think, you know, we show this information, we make it
24 available, we -- in some documents we may suggest departments that you share it with.
25 Like, that could be an area where it sort of veers into that. So it may not be just your

1 BSA/AML department. It may be your legal department. It may be other -- I think
2 some of our ransomware products may even say, like, your IT department, like, you
3 know, sort of things.

4 But I think -- that's another old memory that we should probably qualify.

5 But -- so I think, you know, the main goal is to share the information to make folks aware
6 of it with the hope and -- with the hope that it's actually helpful in identifying the activity
7 that we're talking about.

8 Q When FinCEN shares that type of information, it does not have any
9 expectation of the financial institution of how or whether the financial institution is even
10 going to use it. Is that fair to say?

11 A I think that's fair. I think -- I think we would be surprised a little bit if, like,
12 we publish something on elder financial exploitation -- just to go back to that one again.
13 You know, if you did absolutely nothing with that and you were in a space where that's an
14 issue that may come up for you, I would be surprised if a financial institution didn't make
15 use of that in some way, even if it's just to familiarize themselves with the topic.

16 But, again, there's no specific expectation of what you're supposed to do with the
17 information that we share.

18 Q And financial institutions have to be invited to participate in a FinCEN
19 Exchange. Is that correct?

20 A Yes.

21 Q And they're free to reject that invitation?

22 A Yes.

23 Q And if a financial institution does participate, if it accepts the invitation and
24 participates, it's not required to implement any changes to its AML/CFT programs,
25 correct?

1 A Yes, that's correct.

2 Q And banks who participate in FinCEN exchanges still must use their own
3 independent judgment in assessing transactions holistically to determine whether a
4 transaction is required to be reported under the BSA?

5 A Yes, that's correct.

6 Q And they're free to use their own judgment in determining whether or not to
7 utilize any of the red flags or typologies that FinCEN provides?

8 A Yes, that's correct.

9 Q I just want to move on before we conclude this hour.
10 You were shown an exhibit in the previous hour about -- that referenced an
11 invitation from Google and Google's Financial Intelligence Unit, or FIU. And I believe you
12 said that you would not be surprised about FinCEN having communications with Google.
13 Why is that?

14 A I believe Google has a payment function, and so, you know, if they have a
15 payment function, they're a financial institution under our regulations. So they would
16 have regulatory obligations with FinCEN in that regard.

17 And so the term "financial institution" encompasses a broad array of actors in the
18 moving money space. So it's banks, it's credit unions, and people we've principally been
19 talking about. But it's also money services businesses, your Western Unions, your RIAs,
20 your people like that, casinos, you know, check cashers, you know, virtual currency
21 exchangers.

22 So there's kind of a broad array of actors that have -- that are considered financial
23 institutions for purposes of our regulation.

24 [REDACTED] I just want to clarify one -- when you say there's a broad array
25 of actors, under the BSA in our regulations, is it appropriate for some part of an entity to

1 be subject to a regulation while others may not be?

2 Mr. Kirby. That's a good flag, yes. So the fact that they're doing payments, I
3 wouldn't -- wouldn't necessarily mean, like, the totality of Google is subject to our
4 regulations. That's a good flag.

5 [REDACTED] So because Google Pay is a payment processing system or
6 platform, they -- that section of Google qualifies as a financial institution?

7 Mr. Kirby. Probably qualifies -- I would need -- again, I always want to qualify
8 that because I don't know what I don't know. But in -- sort of, in at least the threshold
9 analysis of -- if you're telling me that an entity is involved in processing payments, I think
10 there's a pretty strong argument that they are going to have at least some obligations
11 under our authority.

12 [REDACTED] Thank you. We can go off the record.

13 [Recess.]

1 [12:18 p.m.]

2 [REDACTED] We can go back on the record.

3 BY [REDACTED]

4 Q Mr. Kirby, I just want to get into a couple things that we discussed in our
5 previous hour.

6 You mentioned the different offices within the Intelligence Division.

7 A Uh-huh.

8 Q Can you describe the responsibilities of each of those offices?

9 A And you mean then --

10 Q Then.

11 A -- in the past?

12 Q Yes.

13 A Okay.

14 So, as I indicated, there were three. There was a Western Hemisphere Office, an
15 Office of Transnational Issues -- or maybe an Office of Transnational Threats. I think it
16 was Office of Transnational Issues. And then a third office that was the -- its acronym
17 was "ARO," but I'm actually struggling to recall what the acronym stood for.

18 So Western Hemisphere, I think, would've -- would've housed -- actually did house
19 things like what was then our Cyber and Emerging Technology Section, if I remember
20 correctly, was there. Also, the team that worked sort of your traditional
21 counternarcotics, Mexican cartels cases, or support to law enforcement, was there.

22 The Transnational Issues Office, if I remember correctly, housed the team that
23 supported the broader counterterrorism mission set and state actor -- I feel like that set
24 would've been there too.

25 And then the third office, the ARO office, included the data quality metrics team

1 that I mentioned before. There's a group of data scientists in that office, that are in that
2 office, that support the -- supported then and support still now the work of that overall
3 team.

4 That's sort of broadly what I recollect, how the offices were divvied up.

5 Q How many people, generally, were in each office?

6 A So we were sort of 50 to 55. I'm not sure it was quite a third/a third/a
7 third, but I don't remember with any -- I don't remember precisely how it broke up
8 between those three, to be honest with you.

9 Q And when you were in charge of the Intelligence Division, what was your
10 day-to-day like?

11 A So I think as I mentioned the prior time we spoke, the position that I stepped
12 into had been vacant for some period of time, I think actually right at about 2 years
13 before I stepped into the role. So, you know, I would say, at the beginning of my time,
14 the day-to-day was probably getting my hands around the different functions, the teams.
15 And it was a very different role than being the legal counselor, for example.

16 After the enactment of the AMLA, I would see that kind of changed a little bit, to
17 think about how we were going to meet these new obligations that had been placed on
18 us.

19 And so, you know, one example being the publication of these financial trend,
20 financial threat analysis reports. That was a new product at the time. And thinking
21 through how we were going to do that, how we were going to do that in a way that's
22 manageable -- because, you know -- and with results that we could sort of explain to the
23 reader.

24 Also, so 2021, there was -- we obviously had a change of administration in 2021,
25 and some, you know, mission sets took on sort of greater prominence. I would say, you

1 know, the ransomware mission set is one that has sort of continued to sort of tick up in
2 terms of priority. After Russia's further invasion of Ukraine, you know, that mission set
3 consumed quite a bit of my time.

4 And so, to the extent there's sort of a day-to-day, I don't know if that answers
5 your question, but maybe that's sort of the best way to divide it up. Because it
6 did change post me getting my hands around it a little bit more, the nature of the role.

7 Q Was there an office responsible for DVE issues?

8 A I don't believe we had an office for DVE. To the extent folks were working
9 on DVE, I think those were folks that had a background in working the terrorism mission
10 set. So I don't think it was a separate office or separate section or anything like that, if I
11 remember correctly.

12 Q Some people likely in that office --

13 A I would think so --

14 Q -- would be handling it?

15 A -- yes. That seems -- that's my general recollection. Yeah.

16 Q Going to the information-sharing operations at FinCEN, when the Strategic
17 Operations Division would share information with the financial institutions, what was the
18 protocol for sharing that information?

19 Would that office reach out to the Intelligence Division for approval on the types
20 of documents, the trends and typologies that they would then be sharing with financial
21 institutions and seek your approval on that or your team's approval on that?

22 [REDACTED] Can we just clarify the context?

23 So the Strategic Operations Division has a very broad mandate, right? They also
24 are the Financial Intelligence Unit. Like, they -- so I just want to make sure we're very
25 clear about what context, when you talk about, sort of, information-sharing. Are you

1 talking about FinCEN Exchange specifically?

2

BY [REDACTED]

3 Q I would say the FinCEN Exchange and other means, one-off emails of emails
4 from employees at FinCEN to financial institutions along the lines of, "We have some
5 typologies and trends that we think you might be interested in. See attached."

6 A So I don't know that there is a -- at least at that time, and I'm not really sure I
7 would think that one exists at this time either, really -- sort of a standard practice of that,
8 you know. I think it would be more sort of specific to the nature -- you know, again, to
9 the extent the folks are sharing information in anticipation of a FinCEN Exchange on what
10 that's going to look like, versus sharing in the context of maybe an advisory committee
11 meeting where they're going to be talking about something involving, like, regulatory
12 burden or something like that. So I don't know that there's sort of a -- I think it, like,
13 would be more, like, topic-, forum-specific.

14 I don't recall in my time in the Intelligence Division getting some document like
15 that, like, either be it a typologies or something document like you were referencing in
16 your exchange with [REDACTED] -- I don't recall getting a document like that to sort of evaluate
17 and clear for sort of the context of sharing in one of those venues.

18 But I also feel the need to preface that with: That was a long time ago at this
19 point, so I don't discount the possibility that I may have seen something and I just don't
20 recall having seen it.

21 Q So, as the Intelligence Division is analyzing BSA data and developing
22 typologies and trends that are then shared with financial institutions, were you sending
23 that to the office that dealt with the private sector and shared information?

24 A So I'm not quite sure I understand that description.

25 Let me sort of -- so, you know, in most circumstances, if we are sharing, you know,

1 typologies and red flags, if an analyst in the then-Intelligence Division, now-Research and
2 Analysis Division, is working on a project like that, I think in most circumstances my
3 expectation would be that that information is probably going to land in a public-facing
4 product of some kind. So that would be probably either our Policy Division or maybe
5 our Enforcement Division if it's in the context of an enforcement action. And any
6 resolved enforcement action by FinCEN ends up being placed on our website so everyone
7 can see what those are.

8 I don't -- off -- I just -- I don't recall it being sort of a standard practice that an
9 analyst would be developing, you know, sort of a typology sort of thing that you would
10 share directly with, like, one financial institution. Now, there may be needs to talk to
11 one financial institution in connection with a filing or something like that. But if we're
12 going to do the work of building out typologies and red flags, I would normally expect
13 that to be to a broader audience.

14 Q When that information was shared with the broader audience, would that
15 information have been analyzed by the Intelligence Division or maybe the Enforcement
16 Division before it is shared with a broader group of financial institutions?

17 A Again, I think it would depend.

18 So if the document you're talking about is, you know, trends and typologies in
19 terms of, you know, fraud filings, so if we have an analyst that did a lot of work on
20 analyzing fraud filings and identified typologies and trends out of that, then, yes, the
21 Intelligence Division, now-Research and Analysis Division, would play a leading role in that
22 analytic effort and would be working with the office that's sort of packaging that up into a
23 public product.

24 But, you know, to the extent that you have a FinCEN Exchange on fentanyl and a
25 non-FinCEN party is presenting on or discussing, you know, lessons they learned in this

1 space that might be useful to you, Financial Institution B, as you're looking at this same
2 mission set, that's not something I would expect the Intelligence Division to have weighed
3 in on prior to a partner agency, be it law enforcement or be it, you know, the private
4 sector potentially, sort of separately weighed in on before it's a topic of discussion in a
5 meeting like that.

6 Q Shifting gears, how many people have access to SARs and other BSA data?

7 A So FinCEN maintains this Electronic Access System that we were talking
8 about before. We have MOUs with partner agencies to be able to access that. My
9 recollection -- and we may need to confirm this -- is, I think via those partner agencies, it's
10 approximately 15,000 people, employees of those agencies, who are Federal, State, local
11 officials, who can access the data via that system.

12 I'm going to put a pin in that, though, as an estimate, because that is not
13 something I checked before we came up here.

14 There's -- I need to finish that response, because it's not complete. There is
15 another -- there is a very small subset of agencies that have the ability to ingest the BSA
16 data that is filed with FinCEN. Those are Federal agencies. Most of them are your sort
17 of usual, I think, agencies that probably wouldn't surprise you in this regard -- DEA, FBI,
18 folks like that -- who have the ability to actually just sort of take our data onto their own
19 systems. And so, you know, I don't have -- those agencies control the access to that
20 data on their systems. That's not something that I have visibility into at FinCEN.

21 So the principal way that people access the data is via the Electronic Access
22 System we were talking about earlier, but there is this other way of accessing the data
23 over here, and I want to be complete about that.

24 Q That other way is that Agency Integrated Access?

25 A That is Agency Integrated Access. And maybe I preempted your question.

1 Q We'll get into that in a little bit. The initial -- that is hosted by FinCEN, is
2 that FinCEN Query?

3 A Yes. And you access that via a system called FinCEN Portal.

4 Q Who's responsible for overseeing the access to that portal?

5 A That is also principally a function housed in our Strategic Operations Division.
6 So they manage the MOU processes with partner agencies and the coordinating with
7 those agencies.

8 Q And how is the data accessed?

9 A So my understanding -- and I will preface this with someone who has not
10 ever used this system, so -- but my understanding is that you have a unique login as an
11 external user. You come onto the system. We know it's you when you come onto the
12 system. You are able to run searches on the system. The system logs those searches
13 that you make.

14 And I think that's actually kind of it, in a nutshell. But the important part being,
15 it's a restricted system. There are expectations partner agencies have to meet in terms
16 of granting -- you know, identifying employees for access to the system. And the system
17 does -- my understanding of it is that it does track the searches, that if we let you onto
18 the system, it would track the searches that you make.

19 Q By tracking that, that's tracking the terms that are used to search?

20 A Yes. We call it an audit log. And so it maintains an audit log of the
21 searches that you would make.

22 Q And what type of data is available via these queries?

23 A So, in that system, you would have access to the sort of BSA form filing
24 information. So that would be the suspicious activity reports that we've been talking
25 about, and it would also be currency transaction reports that we hit on a little bit earlier.

1 The counterpart to the currency transaction report, what is known as Form 8300,
2 that's sort of a similar \$10,000 filing for non-bank institutions.

3 And I think the CMI -- the form when you cross the border, that's the -- I
4 don't -- I'm going to get the acronyms wrong, but the acronym is "CMIR," but don't ask
5 me what the "C" in that -- Currency Monitoring -- anyway.

6 And so all of those reports are housed in that database. Because they're all
7 collected under the broader BSA authority within -- with the sort of same purposes and
8 uses set forth in the statute, and they're available on the system for authorized users.

9 Q And when a user searches those reports, do they only see -- so if they search
10 a name, will they only see reports filed on that name? Or will they get access to the rest
11 of that individual's transaction history?

12 A So I'm going to disaggregate that a little bit, and you tell me if I answer your
13 question, please.

14 So we don't have the ability to track -- and I'll use myself as an example so I'm not
15 using anyone else's name. FinCEN does not have the ability to track, to the best of my
16 knowledge -- and I feel like I would know if we did -- the transactions that Jimmy Kirby
17 engages in at his bank, on his credit card, on whatever.

18 So, when you come into that system, what you're going to have access to, if you
19 search for "Jimmy Kirby" -- and, again, as someone who has never used the system, also
20 take this with a grain of salt, that this is how I understand the system works. When you
21 search "Jimmy Kirby," you would get -- to the extent there are SARs that have been filed
22 on me, you would be able to see those; to the extent a bank has filed currency
23 transaction reports or a non-bank has filed a Form 8300 on me, you would see those; to
24 the extent -- or any of the other BSA forms that involve me, you would be able to see
25 those, because they are all filed on me.

1 But it would be -- the universe of that would be what has been filed on me, not
2 that there is some way to access transactional history involving me across the financial
3 sector. We do not have the ability to do that.

4 Q Are there limits on what purpose a user can query the FinCEN -- the BSA
5 database?

6 A So my understanding is that, when an authorized user goes in, they actually
7 have to put a purpose in for the search they are doing, and under the MOUs and other
8 access protocols, searches are to be limited to the purposes consistent with the Bank
9 Secrecy Act. I think that's more or less the precise language the statute uses in terms of
10 information-sharing.

11 Q And have there been instances where a FinCEN Portal query has been
12 misused?

13 A We have had instances where people have unauthorized disclosed data that
14 they had access to. And in -- both at -- it's a small number of cases over the years, but
15 that has happened.

16 When we become aware of that, it's referred to our Office of Inspector General, as
17 any other sort of potential violation of law would be that we come across involving either
18 an employee of ours or, if we become aware of this involving someone in another agency,
19 we would similarly refer to our Office of Inspector General to look into it.

20 Q Have those situations ever led to access being revoked for a user?

21 A So there's a -- and I don't know if this is where you're going, but I'll just sort
22 of jump ahead. There's a rather prominent case of this at FinCEN from 2018, and it
23 actually involved an employee getting arrested.

24 So this is a space where we take our obligations very seriously. This is a space
25 where employees have been arrested for engaging in improper conduct. This is a space

1 where former employees have gone to prison for improper conduct.

2 So this is not a slap-on-the-wrist type of situation. To the best of my knowledge,
3 this is the only circumstance in which an employee of FinCEN was walked out of the
4 building by Federal law enforcement agents, for potential, like, improper activity in this
5 space.

6 So, to jump ahead to, this is something we have dealt with and we have dealt with
7 quite seriously and our Office of Inspector General has dealt with quite seriously, we take
8 our obligations to safeguard this information very seriously. It is front of mind for us,
9 this obligation, in terms of thinking about ways we can think about different ways, better
10 ways, to safeguard the data, because the data is really sensitive.

11 And it's an important thing -- I mean, it's a very fair question, because it's an
12 important thing for us to do as an agency. You probably noticed my tone shift. It's
13 something I feel really strongly about, that it's an important trust and obligation that is
14 placed on the agency. And I don't have a lot of patience if we come across
15 circumstances where people have done stuff they're not supposed to do in this space.

16 So I was there in 2018. I have seen how important this is, to take these actions.
17 It's something I take very seriously in my job still, something we take very seriously as an
18 agency.

19 Q Thank you for that.

20 You mentioned that there is an audit log of the searches --

21 A Yes.

22 Q -- of the BSA database. Are there regular audits of access to the BSA
23 database?

24 A So my understanding is, yes, that there's a team in our Strategic Operations
25 Division that, as part of their regular coordination with the, you know, partner agencies,

1 customer agencies, they regularly review the logs as, you know, part of that exercise in
2 terms of coordinating back with the agencies to make sure that they're doing what
3 they're supposed to do under the terms of our MOUs.

4 Q Are those audits memorialized anywhere?

5 A I actually don't know the answer to that question. I think yes, but I don't
6 know for sure.

7 Q Who would know the answer to that?

8 A That's something we can take back and find out. We can find out the
9 answer to that question. I just don't know it off the top of my head.

10 [REDACTED] I think there's already a request pending that --

11 Mr. Kirby. Oh, there we go.

12 [REDACTED] -- we can correspond.

13

BY [REDACTED]

14 Q So you mentioned there's approximately 55,000, give or take, BSA filings
15 each day. Is there any way to know how many people this covers?

16 A You mean, like, the subjects?

17 Q Yes, how many subjects are covered.

18 A I don't know the answer to that question. And I don't know -- I don't know
19 if that's something we track, to be honest.

20 Q Do you know who would track that?

21 A I mean, we can take that back, as well, and ask. But I don't -- I don't
22 actually think I've ever gotten that question before. I don't know the answer to it.

23 Q I assume the same answer would be to how many American subjects are
24 covered in that.

25 A So I don't know the answer to that, but I would maybe put a little more meat

1 on the bone in my response to that and at least say: If these obligations apply to
2 U.S. financial institutions, you know, I would operate on the assumption that the majority
3 of the filings -- or, actually, a substantial portion of the filings -- that's probably a better
4 way to put it -- probably involve U.S. persons, because these are financial institutions
5 operating in the United States subject to U.S. law.

6 Q Are BSA filings ever deleted from the FinCEN database?

7 A We are -- so the answer to that question now is, my understanding is, the
8 filings on the system, they are not presently deleted.

9 We are actively looking at a way to essentially remove filings in the system that
10 are older than -- it's 11 years, right? -- 11 or 12 years. That's something we're actively
11 working on at the moment -- or exploring, I should say.

12 Q Is there a timeline for implementing that procedure, or is it still in the
13 exploration phase?

14 A It's still in the exploration.

15 Q Okay.

16 So you mentioned Agency Integrated Access earlier. Once one of these agencies
17 imports this data onto their own systems, does FinCEN have any oversight over the BSA
18 data that has been imported?

19 A You know, we have a relationship with the agencies. You know, there is a
20 practical matter, I think, you know, at present at least, of the degree of oversight that we
21 can do when it's not on our system anymore.

22 We are in a broader -- if I could step back from your question, a broader exercise
23 is underway to actually update all of our access MOUs, so not the ones where you come
24 in via the FinCEN system, but also the MOUs that govern the Integrated Access space.
25 And, you know, thinking about are there changes we need to make with regard to

1 oversight in that space is sort of part of that effort at the moment.

2 So we're sort of well underway with updating the MOUs for access for agencies
3 who come in via the FinCEN system -- I don't know why I'm doing this -- for the FinCEN
4 system. If you come in via the FinCEN system, that update exercise is well underway
5 with a number of agencies.

6 The Integrated Access MOUs are ones we're still sort of, like, working on in terms
7 of -- but they will be updated, as well, as part of this broader exercise.

8 Q Can you describe the parameters of those MOUs with the agencies?

9 A So, ordinarily, they would govern things like type of data covered by the
10 MOU; respective agency obligations under the MOU; obligations with regard to if, you
11 know, you're, you know, Law Enforcement Agency A, the commitments you're making to
12 us in terms of the people that you're going to sort of put forward for access to the
13 information. For instance, there's a requirement -- I'm pretty sure there's a requirement
14 for all users, for instance, to have a background investigation.

15 I'm pretty sure that's right, right? Okay.

16 And so there's sort of that.

17 There's the obligation they take to sort of restrict access to the data that you're
18 using, given the sensitivity to it, and obligations with regard to sort of marking in certain
19 ways.

20 So it's meant to be somewhat more holistic in terms of access, protection, and
21 making sure the information is sort of adequately protected from, you know,
22 unauthorized disclosure or unauthorized dissemination.

23 I'm actually going to put a pin in and stop.

24 Is there anything I need to add to that, [REDACTED] Because you are very familiar
25 with this topic too.

1 [REDACTED] No, I was just going to --

2 Mr. Kirby. I don't know if I'm allowed to do that in my interview, but I'm going to
3 do it here.

4 [REDACTED] Just for context on this MOU discussion, since we are here
5 primarily for your role as director of [inaudible] the Intelligence Division, how much did
6 you work with the MOUs in that role --

7 Mr. Kirby. Oh.

8 [REDACTED] -- versus your current role?

9 Mr. Kirby. Actually, very little, to be honest.
10 What I'm telling you now is very much a product of the chair that I sit in at the
11 moment, not the chair that I sat in when I was in ID.

12 [REDACTED] When an agency has Agency Integrated Access, are they
13 receiving all of the inside filings, or is it limited to what is relevant to their issue area?

14 Mr. Kirby. My understanding is that they receive all BSA filings.

15 BY [REDACTED]

16 Q Is there a material difference between the AIA system and the Electronic
17 Access System you described earlier in terms of what content is in either?

18 A I don't know that there's a material difference between the content. So,
19 you know, if you're coming in -- if your agency has Integrated Access and you're coming in
20 via the traditional system, you should have access -- each of you should have access to
21 the same BSA filings.

22 What the Integrated Access allows the agency to do when they take it onto their
23 systems is look at it in conjunction with other data they may have on their system.

24 Q And so, once that data is taken onto the system -- I know you mentioned
25 you're updating it -- does FinCEN continue to have access to the agency that has imported

1 it onto their system and how they're using it? Or is that a dialogue between FinCEN and
2 the agency with the MOU to have AIA?

3 [REDACTED] Can I -- is what you're asking is, when an agency with AIA
4 brings it onto their system, do we have continued visibility into it in the same way that we
5 do FinCEN Query? Is that the question?

6 [REDACTED] Right.

7 Mr. Kirby. And I think the answer to that is, no, we don't have the -- because,
8 again, we control the FinCEN Query system, so, you know, if you're coming in via Query,
9 we could, in theory, look at what you're searching. We don't have that same degree of
10 visibility.

11 But there is still an MOU in place with the agency that's bringing it on via
12 Integrated Access, is my understanding.

13 [REDACTED] Do you know how many filings are in the database?

14 Mr. Kirby. I don't know. It's a lot. But I don't know what "a lot" is. I don't
15 know.

16 [REDACTED] Don't speculate.

17 Mr. Kirby. I don't know. I don't know the answer to that. It's more than a
18 million.

19 [REDACTED] Yeah. If it's 55,000 per day, that's going to be a few.

20 Has there been an agency that's been in violation of the MOU that had AIA access
21 remitted (ph) or revoked?

22 Mr. Kirby. I'm not aware of a determination that an agency with Integrated
23 Access violated its MOU. So I don't know -- so, to the sort of first part of your question,
24 I'm not aware of the premise that would get me to the second part of your question.

25 I think that's probably my best answer on that.

1 [REDACTED] Can FinCEN audit AIA?

2 Mr. Kirby. My understanding under the MOUs is that we still do maintain the
3 ability to sort of coordinate with that agency regarding use of the data and what it's doing
4 with the data. So my understanding is, the answer to your question is yes. It's just we
5 would not have the same degree of visibility that we would when you're coming onto our
6 own system to access the data.

7

BY [REDACTED]

8 Q I know you mentioned you've never used the Electronic Access System.
9 You do seem very familiar. How are you familiar with that system?

10 A Through briefings and the broader exercise we're undertaking, actually, to
11 update the MOU documents generally. So I have been involved in that, so I've had the,
12 you know, opportunity to learn. And through meetings and other scenarios is how my
13 understanding of how this works has been gleaned.

14 Q And does the Intelligence Division, now-Research and Analysis Division -- do
15 they use that system?

16 A I believe some do use the portal system. And then my understanding
17 is -- you know, since it's a FinCEN system, my understanding is you can also access the
18 data by just our own internal systems. So, like, you know, the portal system is built for
19 principally external users to come in and use the system, is my understanding of the
20 difference there.

21

BY [REDACTED]

22 Q You mentioned that the MOUs with respect to AIA are in the process of
23 being updated.

24 A Uh-huh.

25 Q Why are those being updated?

1 A As I indicated before, you know, safeguarding the data is a priority for us and
2 making sure we have, you know, the best practices in place. And so, across all of our
3 MOUs, we're working to make sure that they're all sort of, basically, recent, consistent,
4 and that we have taken that close look in terms of evaluating what, if any, changes need
5 to be made with regard to sort of any of the things covered by the MOU document.

6 So I think the top-line answer to your question was, frankly, I think it's time, and
7 it's a good time to do it.

8 Q Are there any specific issues that have come up, or is it just time?

9 A I think the main, if I had to pick an issue, is, you know, some of them were a
10 little dated. And so it's a good opportunity in terms of getting sort of -- you know, taking
11 a fresh look at everything and just bringing them up to date, in the sense of, you know, I
12 think there's a comfort that comes for a variety of users that, you know, the MOU you're
13 operating under is a fairly recent MOU.

14 So it's mainly driven by just, I think, a timing need to update. Some of them are a
15 little on the dated side, and it'd be helpful to bring them up more current.

16 BY [REDACTED]

17 Q Are you aware of any examples of personnel from another agency misusing
18 the data?

19 A So I don't know this for sure, so I'm going to start with that qualification. I
20 have recollection that there, again, have been sort of one-off instances in the past of,
21 actually, employees of other agencies -- you know, I talked a little bit about the incident
22 at FinCEN in 2018 -- that there may have been some similar, you know, at other -- one or
23 two maybe. But my recollection on that is a little thin. But those are the ones I'm sort
24 of -- that come to mind more front of mind for me.

25 What I understand from the team is that, in their experience, if they sort of call in

1 response to something they see on an audit log that raises a question, it's usually the
2 person just didn't -- it was an honest mistake; they didn't put in enough information.

3 So we don't see many instances of people acting inappropriately in the system.
4 But it is something that is important.

5 And, again, a goal of this MOU update exercise is just making sure everything is
6 timely and we've taken a look to make sure, you know, everything is up to date.

7 Q You described the thin recollections you have of maybe some other
8 instances. Do you recall which agencies?

9 A I don't, no. A Google search might resolve that, because if my memory is
10 correct, that should be public. We can take that back, too, if it would be helpful.

11 Q In either your current role or any of your prior roles at FinCEN, if you wanted
12 to review an audit of one of the other agencies, would you have the ability to do that?

13 A Yes. Well, I would have to ask someone to get it for me, but yes. I don't
14 have the ability to go in and just do it, but I could have someone bring it to me.

15

BY [REDACTED]

16 Q Did you ever do that?

17 A No.

18 Q I think we'll go back to your time as associate director for the Intelligence
19 Division. In that role, did you coordinate with any offices from the FBI?

20 A I don't recall doing that directly, but I'm relatively confident that members of
21 my team did, because, again, it's fairly common for us to work with the FBI, and the FBI
22 has a representative housed in our offices. So we have a number of law enforcement
23 liaisons who sit with FinCEN; FBI is one of them.

24 Q So would that be an FBI agent or employee that is detailed?

25 A Yes. I don't think it's a full-on agent. I think it's an employee. But,

1 again, it would be very common to interact with the FBI, so I am relatively confident, even
2 though I don't recollect doing it directly myself, that members of my team would have.

3 Q So would you or your team work with the Strategic Partner Engagement
4 Section at the FBI?

5 A I don't know the answer to that. I do not recall working with that section.
6 I do not know the answer as to the broader team.

7 Q Did you or your team ever interact with Peter Sullivan, who was in that office
8 at the FBI?

9 A I don't recall interacting with Mr. Sullivan, and I don't know the answer as to
10 the broader team.

11 Q What was your relationship like or your team's relationship like with the FBI?
12 Was it collaborative?

13 A You know, my impression generally over many years, not just, you know, my
14 time in the role, has been that, generally, as an agency, including the components, we
15 have collaborative relationships with our law enforcement partners.

16 And I think you see that playing out now with the Project Protect series fentanyl
17 Exchanges that I mentioned before, with, you know, our support to DEA in the fentanyl
18 space. I think you see it on a number of mission sets at the moment.

19 I think we have historically had collaborative relationships with the main law
20 enforcement agencies. So I would not expect it to have been any different in a material
21 way 4 years ago as to what I see today.

22 Q Did you or are you aware of anyone at FinCEN sending SARs directly to the
23 FBI or any other law enforcement agency?

24 A So I think so, but I don't -- again, that wouldn't necessarily strike me as
25 unusual. The FBI has access to the data.

1 And, you know, going back to a description I was giving earlier of, if you're an
2 analyst working the cyber and emerging tech space -- this is coming to front of mind for
3 me most in that space. So, if we got a SAR involving a new ransomware strain or a SAR
4 discussing some type of, you know, attack in the space that has caused -- I don't know
5 that it would strike me as unusual that an analyst working on that would share that SAR
6 with NCIJTF, for example, or another FBI field office that is responsible for that particular
7 ransomware strain.

8 There are -- again, FBI has access to -- now, that may happen not -- because I don't
9 know this for sure. It may happen to just share the ID number, as opposed to sharing
10 the SAR itself. But I don't know that I would be surprised if they shared the actual SAR if
11 they thought the -- to discuss the discussion in the sort of narrative section of the
12 document if they thought it was relevant to the mission space that they're working on.

13 That's a long-winded way of answering your question. I hope it answered your
14 question.

15 Q Did --

16 A Actually, I'm going to qualify that one more time. But I would expect them
17 to only share it with agencies that otherwise have access. And, again, since most of our
18 main Federal partners do, that's not an issue.

19 Q Okay.

20 Did the FBI coordinate with FinCEN regarding its relationship and communications
21 with financial institutions?

22 A I might need you to be a little bit more specific on that one.

23 Q So, if the FBI is working with financial institutions, sharing potential
24 typologies or investigative information into financial crimes, would they coordinate with
25 FinCEN in the course of these communications with the financial institutions?

1 A So that's a pretty general question. Maybe I'll answer it the best I can.
2 You know, it's always been my understanding, at least since coming to FinCEN -- I
3 should qualify that -- that the FBI in particular, other law enforcement agencies, sort of
4 have their own relationships, their own authorities, when it comes to the sector, the
5 financial sector.

6 So I wouldn't expect them, in at least the abstract, to sort of come to us as a
7 matter of course with regard to them engaging with, you know, members of the financial
8 sector on cases that they're working on.

9 Again, we have -- law enforcement does regularly participate in the FinCEN
10 Exchanges that we convene, and so -- and, obviously, FinCEN is there for those and part of
11 those conversations, as the convening agency. But I don't know that I would expect sort
12 of across the board that if the FBI wants to call up Bank A they would sort of loop FinCEN
13 into that.

14 But I can't say that I know that in a specific way. That's more of a higher-level
15 reaction based on my perception.

16 BY [REDACTED]

17 Q Based off of -- going a couple questions earlier, you said it wouldn't surprise
18 you if members of your team, or FinCEN, I should say, were sending SARs directly to the
19 FBI, I guess by members of your team?

20 A I would say maybe analysts in the Intelligence Division, because I think that's
21 the team most likely to be sort of in the data.

22 But, again, that could happen via -- I'm not sure that -- I don't know that they
23 would necessarily send the document. They might just send the ID number. Because
24 with the ID number, the agency with access could just pull it up themselves.

25 Q And --

1 A And so, if -- I just don't know how that would happen.

2 Q And if you got the analyst working on an issue, he or she gets to the point
3 where they think it's significant enough, for whatever reason, to share with the FBI, is
4 that a type of decision the analyst would elevate, or is that something that analysts are
5 empowered to make on their own?

6 A Again, my guess is that it's going to be sort of team- and topic-specific.
7 Because it may vary based on the sort of topic integration with a law enforcement
8 agency.

9 So where you have a team that's collaborating very closely with DEA on a, you
10 know, fentanyl matter -- and, again, we have employees who spend some time at DEA;
11 DEA has employees that spend some time at FinCEN. It's meant to promote that kind of
12 information exchange. I just don't know the means on which it would happen.

13 So I think it would be probably topic-specific, team-specific. I don't know that
14 there would be sort of a one way it would always happen.

15 Q Do you recall any instances when you were associate director where
16 someone from within your team elevated the issue to your level, about whether it was
17 appropriate to share or to highlight a SAR to another agency?

18 A I don't. But I do recall being aware that, in the context of ransomware, we
19 were very transparent with -- and I think the FBI component with NCIJTF -- with regard to
20 alerting them to information that we would see. And, again, I just don't recall if that
21 meant we sent them the SAR or we sent them the number for them to pull up the SAR
22 themselves.

23 So I think that's sort of a "yes" to your second question of being aware that
24 information was shared at times. I just don't recall knowing exactly how that was
25 happening.

1

BY [REDACTED]

2

Q Did you ever flag specific names to financial institutions for SAR filing purposes?

3

4

A I don't recall doing that, no. Yeah, I don't recall doing that.

5

6

Q Could Federal law enforcement provide a list of names to financial institutions to consider for SAR filing purposes?

7

8

A You know, with regard to what law enforcement can and can't do, I've sort of learned over the years it's probably best for me to defer to law enforcement on that question. So that's a question you might want to ask the FBI or DOJ.

9

10

And, you know, to the extent, turning to my own knowledge, you know, it may depend on who the names are. You know, again, I don't think it's uncommon for financial institutions to sort of be aware of what's in the news, in terms of informing their AML programs. So, you know, to the extent, you know, Jimmy Kirby was arrested yesterday for engaging in all sorts of fraudulent activity, you know, my bank might take a look at that if that was in the paper the next day. I don't think that would be a surprising thing for them to do.

11

12

13

14

15

16

17

Q But would it be unusual for Federal law enforcement to send a list of specific names for a bank to consider for SAR filing purposes?

18

19

A I don't know the answer to that question. I really don't, because I don't know --

20

21

Q Have you seen it before?

22

23

A I mean, in terms of, like, things I've seen, you know, over the course of this year I've seen materials in connection with the topic that we're here to talk about today, and, you know, I do recall seeing -- there may have been names of people who had been arrested, as one potential list of names that was shared with folks in terms of awareness.

24

25

1 without context, I want the record to be very clear on that point.

2 [REDACTED] Okay.

3 [REDACTED] So what's the -- so we need the answer before we proceed.

4 [REDACTED] This is the only email here from a representative at KeyBank to
5 various employees of FinCEN that we have --

6 [REDACTED] Okay. So --

7 [REDACTED] -- with this subject line.

8 [REDACTED] This is not a part of a larger thread.

9 [REDACTED] There's no other emails on this thread?

10 [REDACTED] No.

11 [REDACTED] Okay.

12 And you all are going to distribute the attachment, I assume, for context.

13 [REDACTED] Yes. And before you object, just let us enter the items into
14 evidence and let us start to ask questions.

15 [REDACTED] And then I'd now like to enter an email from [REDACTED]
16 dated January 15th, 2021, and the attachments "Jan 15 2021 compiled typologies" and
17 "KeyBank Query Logic for Active Shooters," with the subject line "Compiled typologies in
18 advance of 4:30 call," into the record as exhibit 3.

19 [Kirby Exhibit No. 3

20 was marked for identification.]

21 [REDACTED] So this is more than just a PowerPoint? This is from another
22 source, this --

23 [REDACTED] This is the email. And there were two attachments, and these
24 are the attachments.

25 [REDACTED] Thank you.

1 [REDACTED] Sorry. Just to clarify, there's a -- so, on what's been entered as
2 exhibit 2, it looks like there's an attachment, "KeyBank Query Logic for Active Shooters
3 version 01-15-2021.pptx." Is that attachment --

4 [REDACTED] That is what is in here. That's the PowerPoint that is in exhibit
5 3.

6 [REDACTED] But exhibit 3 was produced by a different -- is not actually the
7 one -- it might look the same, but it's not the one that was attached to exhibit 2. Does
8 that make sense? Because exhibit 3 is the KeyBank PowerPoint as attached to an email,
9 a different email.

10 [REDACTED] We'll just represent for the record that the slideshow that's
11 distributed by FinCEN is the same slideshow that's being sent to FinCEN from KeyBank.

12 Mr. Kirby. Okay. I'm ready.

13 BY [REDACTED]

14 Q We've just got about a minute and a half left, so --

15 A I'm sure we'll knock all of this out in 90 seconds.

16 Q Acknowledging that you are not included on this email, had you ever seen
17 these emails at this time?

18 [REDACTED] You're talking about exhibit 2, for the record, right?

19 Mr. Kirby. This one.

20 [REDACTED] Exhibit 2 --

21 Mr. Kirby. This one --

22 [REDACTED] Yes.

23 Mr. Kirby. -- is the one you're talking about.

24 BY [REDACTED]

25 Q Had you seen that at the time?

1 A I don't recall seeing this at the time, no.

2 Q You testified that [REDACTED] was a member of the Intelligence Division
3 when you were there.

4 A Yes.

5 Q She is cc'd on exhibit 3. Did you discuss this email with her at the time that
6 was sent to these financial institutions?

7 A I don't recall discussing this with [REDACTED] at the time, no.

8 Q Do you know if you or anyone in your office analyzed the information in the
9 attachments before [REDACTED] shared it with financial institutions?

10 A I don't know, no.

11 [REDACTED] Would this have been the kind of thing that would have normally
12 came to the Intelligence Division prior to it being sent out?

13 Mr. Kirby. I don't know, because it's not -- it doesn't appear to be our work
14 product. So I don't know the answer to that question.

15 [REDACTED] We can go off the record.

16 [Recess.]

1

2 [2:08 p.m.]

3 [REDACTED] We're back on the record. Thank you.

4

BY [REDACTED]

5

6 Q I want to start by asking a couple of questions about -- you were asked a lot
7 of questions during the previous hour about the confidentiality provisions and what
8 happens if somebody violates those, how those things are monitored, and you mentioned
9 an employee in 2018 who was criminally prosecuted for violating those provisions,
correct?

10 A Correct, yes.

11 Q Now, those criminal provisions apply not just to --

12 A Actually, I should stop there. I don't -- it was in relation to that, but I don't
13 know the specific prong DOJ used. So let me put that. There may have been a
14 conspiracy prong or something like that --

15 Q Fair enough.

16 A -- not the actual --

17 Q And I'm not going to ask you questions at that level of --

18 A Just to, again, make sure I'm clear on that.

19 Q Yes. I'm not going to ask at that level of specificity. I just want to make
20 clear that the criminal provisions that apply to unauthorized disclosure for dissemination
21 of Bank Secrecy Act information, those apply to anybody who is authorized to have that
22 information and then discloses it improperly, regardless of whether they work for FinCEN
23 or the FBI or anywhere else.

24 A I believe so, yes.

25 Q And, in fact, there's a criminal provision within the same chapter of the

1 United States Code 31, United States Code 5322, that makes it a felony to disclose -- to
2 violate those provisions of the Bank Secrecy Act?

3 A I'll defer to you on the number, but the provision, that sounds right to me.

4 Q Okay. Thank you.

5 Now, I want to pick up where we left off at the top of the last hour and just make
6 some clarifications about the record, because there were some exhibits introduced with
7 attachments and we raised some questions and some representations were made that I
8 just want to clarify. I'm not actually going to be asking you for any -- any questions
9 about this.

10 A Okay.

11 Q But I think it's important that we have an accurate representation, because
12 many different financial institutions produced documents to the committee in response,
13 and I want to be clear what is and is not produced by different institutions and what is
14 before you that you're being asked questions about.

15 So exhibit 2 is an email from [REDACTED]. And if you look at the Bates number,
16 it has a Bates number from KeyBank HJC 235. And I believe your counsel asked if this
17 was part of a chain, and it was represented that it was not, but you can see from the
18 email that there is an attachment of a KeyBank PowerPoint.

19 And then exhibit 3 was introduced, and exhibit 3 is not a production from
20 KeyBank; it's, in fact, an email to an employee at KeyBank and other institutions from
21 [REDACTED] and it has Bates numbers HJC 005 through 007.

22 And then there is a KeyBank PowerPoint, that does not have Bates numbers,
23 attached to exhibit 2, and it was represented during the previous hour that that is the
24 same PowerPoint that was attached to exhibit 2.

25 Now, I'm going to introduce the actual documents that were produced by

1 KeyBank as exhibit 4.

2 [Kirby Exhibit No. 4

3 was marked for identification.]

4 [REDACTED] And if you follow along, you can see that the Bates number for the
5 second page is a PDF of the KeyBank PowerPoint. It's the Bates number that follows the
6 Bates number for exhibit 2.

7 So you can see that this is the actual PowerPoint that was attached to the email in
8 exhibit 2, and it has redactions. So it is therefore not the same PowerPoint that was
9 produced in exhibit 3.

10 And now I would like to introduce the actual documents, the attachments from
11 exhibit 3. And I will state for the record that these are co-produced by Wells Fargo. So
12 now this will be exhibit 5.

13 [Kirby Exhibit No. 5

14 was marked for identification.]

15 [REDACTED] And you can see that exhibit 5, the first page has the same Bates
16 numbers. It's the same Bates numbers. It's HJC 118 dash many, many zeros 5 through
17 7. And then Bates 8 is a black and white PDF of a PowerPoint that is also redacted, and
18 that is not what was attached to exhibit 3.

19 The unredacted PowerPoint that was attached as exhibit 3 stapled together
20 representing as if it is the attachment to the email from the KeyBank employee to
21 [REDACTED] is actually a native file that was produced to the committee from Citibank,
22 completely separate institution.

23 And I'm going to introduce that for the record, just to make clear that what was
24 attached as one exhibit and introduced into the record as one exhibit as being an
25 attachment to an email that was produced to us from one financial institution actually

1 came from a different financial institution.

2 And the majority's representation that these are the same PowerPoints, I
3 understand that it's a natural assumption that they have the same title that they are the
4 same, but for the ones that were actually produced by the banks in exhibit 4 and exhibit 5
5 were redacted and we don't know that they were the same.

6 What we do know is that what was presented as the attachment to exhibit 3 was
7 not the document that was attached to exhibit 3. It was a document that was produced
8 by another bank. And we're going to introduce exhibit 6 for the record.

9 [Kirby Exhibit No. 6
10 was marked for identification.]

11 [REDACTED] So I would ask the majority, when we're being questioned -- when
12 we're questioning a witness about this PowerPoint, that we use the exhibits with the
13 emails that they were actually attached to from the institutions that actually produced
14 them.

15 BY [REDACTED]

16 Q And with that out of the way, you were asked a series of questions during
17 the previous hour about whether law enforcement ever provides a list of names to
18 FinCEN or to financial institutions and ask them to file SARs or to search for people with
19 those names. And to me that made me -- rang a bell for me in terms of Section 314 of
20 the PATRIOT Act.

21 Are you familiar with Section 314(a) of the PATRIOT Act?

22 A Yes, I am.

23 Q And what is your understanding of what Section 314(a) allows law
24 enforcement agencies to request of financial institutions?

25 A So law enforcement agencies can ask FinCEN to query financial institutions

1 for -- it's essentially a hand-raising exercise for whether they have responsive
2 accounts -- maybe transactions as well, I have to check the reg -- for targets that have
3 been identified for either like counterterrorism or anti-money laundering reasons.

4 Q And so is it correct to say that law enforcement through their own
5 investigations identifies a suspect, and then if they want to investigate that suspect's
6 financial records they need to find out where those financial records are? So they send
7 a request to FinCEN to ask financial institutions, "Do you have any records for this
8 individual?"

9 Is that correct?

10 A Yes.

11 Q And the financial institutions respond yes or no, but the 314(a) response
12 does not include the actual financial records, correct?

13 A That is my understanding, yes. It does not include the actual financial
14 records.

15 Q And so when you say it's a hand-raising exercise, did you mean that any bank
16 who has records related to the subject named in the 314(a) request says, "We have
17 records"?

18 A Yes, essentially the yes/no as you phrased it.

19 Q And the purpose of that is to allow law enforcement to then serve a
20 subpoena or a search warrant or whatever -- whatever --

21 A Whatever process they have.

22 Q -- they have to then obtain those records?

23 A Yes, that is my understanding.

24 Q So it's kind of the flip side of a suspicious activity report, whereas with a
25 suspicious activity report it's the bank who's investigating or monitoring their customers

1 and then flagging for FinCEN and law enforcement what they deem to be suspicious;
2 whereas, with 314(a), law enforcement has identified an individual who is a suspect or a
3 target in some respect, and then they are trying to get their financial records, and they
4 use 314(a) as the first step to know where to go.

5 A I think that's a fair description, yes.

6 Q Okay. Thank you.

7 And like suspicious activity reports, Section 314(a) is a tool that is available to law
8 enforcement to help them combat the financing of terrorism, as well as money
9 laundering and other offenses?

10 A Yes, that's correct.

11 [REDACTED] Okay. Thank you.

12 And with that, we can go off the record.

13 [Recess.]

14 [REDACTED] We can go back on the record.

15 BY [REDACTED]

16 Q I think where we left off in the majority's previous hour was relating to the
17 attachments sent in an email from [REDACTED] to a number of financial institutions.
18 That's the "January 15th, 2021, compiled typologies" and the "KeyBank Query Logic for
19 Active Shooters."

20 We can direct you to exhibit 5.

21 A Okay.

22 Q Let me know if you need a minute to review.

23 [Pause.]

24 A Okay.

25 Q You previously testified that [REDACTED] was a member of the Intelligence

1 Division. She's cc'd on this email.

2 Did you discuss this email or the attachments with her?

3 A I don't recall discussing the email or its attachments with her.

4 Q And do you recall if you ever received this email?

5 A I don't recall receiving this email either.

6 Q Do you know if you or anyone in your office analyzed the information in the
7 attachments before it was shared with financial institutions?

8 A I do not know the answer to that question.

9 Q Would that be the norm, the sort of thing that normally would go through
10 the Intelligence Division before being distributed?

11 A As I think I mentioned before the break, this isn't FinCEN's work product.

12 Q Well --

13 A So, I mean, the slide deck. So I don't know that there would be a sort of
14 like "usual" for that. So I don't know if it was reviewed by the Intelligence Division
15 before it was sent.

16 Q I will direct you to Bates number 6.

17 A Yes.

18 Q So if you'll notice, it says, "Lone Actor/Homegrown Violent Extremism
19 Indicators," and in parentheses says, "(developed from prior FinCEN analysis)."

20 A Yes. I'm sorry, I was referring to the slide deck in my response to the prior
21 question. My apologies for any lack of clarity on that.

22 Okay. I'm on Bates 6.

23 Q Do you know whether the Intelligence Division helped prepare these
24 indicators?

25 A I do not know.

1 Q Have you seen them before?

2 A I have in the sense of -- the questions that have arisen over the course of a
3 year, I have seen this list in connection with that effort or with those inquiries.

4 Q And on this email there's at least looks like 11 different financial institutions
5 listed.

6 Do you know how FinCEN decided that these materials would go to these financial
7 institutions and not others?

8 A I do not know, no.

9 Q Would this kind of exchange be considered a FinCEN Exchange?

10 A This is not what -- I mean, a FinCEN Exchange, at least in my mind, is when
11 sort of people convene to talk. Though it would also make sense to me that part of that
12 could be also extended to sort of include the information being shared in advance of an
13 exchange.

14 I've never really thought about it that way, but I could see it making sense in the
15 sense of, so folks are sort of talking from -- understanding the facts or the -- whatever it is
16 that's going to be discussed in the exchange.

17 But at least an exchange itself is something I tend to think of as the sort of actual
18 event of people coming together and talking.

19 Q The subject line states, "...in advance of 4:30 call." Did you participate in
20 that call?

21 A I do not recall whether I did or if I did not.

22 Q Did you participate in any calls with financial institutions in the weeks
23 following January 6th, 2021?

24 A I don't recall if I did or didn't, to be honest. I've sort of been relaying that a
25 bit in my mind in anticipation of coming here today, and it wouldn't surprise me if I did.

1 But if I did, it wouldn't have been many of these. I don't -- but I don't recall attending
2 any.

3

BY [REDACTED]

4

Q Can we take a step back a little bit?

5

6

7

So in the days and weeks following January 6th, obviously there's many law enforcement investigations going on. FinCEN is clearly sharing a lot of information -- whether that's [REDACTED] -- with financial institutions.

8

What is the atmosphere at FinCEN at that time?

9

10

11

12

13

A Hmm. The atmosphere at FinCEN? I was aware that these exchanges were going on. I think you see senior leaders copied on these emails, so this would've been something that would've, I think, gathered attention from like -- that's something folks would've been focused on in the aftermath of the event. And there was the concern of violence in connection with the sort of upcoming inauguration.

14

15

16

There was also, though, sort of separate and apart from this, there was a transition underway, and so there would've been all of the steps going on at that time in connection with transitioning from one administration to the next administration.

17

18

19

So my recollection is there also would've been the sort of -- that work going on as well of transition memos and meeting with any transition team or preparing things for a transition team.

20

21

Sort of all of that was going -- would've been going on at the same time as this. And then there was still the pandemic sort of overhang going on as well.

22

23

24

25

So I don't really recall a vibe per se, but there was a lot going on at this time and a lot going on at this time that would have sort of drawn leadership's attention because of all of the different work streams sort of associated with those things, if that answers your question.

1 Q So looking at -- we'll look at this attachment specifically. At the top it says,
2 "Bank submission."

3 Is it fair to assume that a bank likely sent that to FinCEN and then [REDACTED]
4 was sending that out to other financial institutions?

5 A So I don't know the answer to that. But if I'm looking at the first sentence,
6 it seems a fair conclusion to draw. This came not from us but came from a financial
7 institution, given the reference to searching of "Zelle payment messages."

8 Q Would you or someone in your office have analyzed this submission from
9 the bank to determine whether it was legitimate and worth sending out to other financial
10 institutions?

11 A I do not recall. I don't know if that happened. And as I think I indicated
12 earlier today, for FinCEN Exchange presentations or materials by presenters that aren't
13 FinCEN, sort of irrespective of the topic, FinCEN wouldn't necessarily -- I don't think we
14 actually have a practice of sort of reviewing and validating those products or
15 presentations or whatever they are prior to whatever discussion is going to happen in
16 that regard.

17 Q So aside from that, this appears to be just an email in anticipation of the call,
18 so likely not part of the FinCEN Exchange.

19 A Uh-huh.

20 Q That wouldn't have been analyzed by anyone in your division, any other
21 division?

22 A I'm not aware of whether this was analyzed or not.

23 BY [REDACTED]

24 Q Following January 6th, how did your team's attention change?

25 A So there were analysts working on this effort of supporting law enforcement

1 in connection with, my recollection is, requests from the FBI, which tends to be how we
2 get pulled into law enforcement support matters. So my recollection is there were
3 members of the Intelligence Division supporting requests from the FBI.

4 Q How many members?

5 A I don't know the exact number. But the terrorism team was I don't think
6 any more than six or seven employees, so it would've been almost certainly less than
7 that. I don't know that it would've been the whole -- I don't think it would've been the
8 whole team, but I don't know.

9 Q Did you have any conversations with that team in the days or weeks
10 following January 6th about where their priorities should be?

11 A I don't recall any discussions like that. This was being very much managed
12 at a leadership level within FinCEN, so I don't recall any discussions of the type you're
13 describing.

14 Q Who specifically within FinCEN leadership was involved that you can recall?

15 A Well, AnnaLou Tirol, who then became the deputy director shortly -- yeah,
16 shortly after the date of this email, again, at the time was the head of the Strategic
17 Operations Division and had a background in law enforcement.

18 And my recollection is the director at the time was also actively involved in these
19 exchanges and this effort.

20 Q Did you have meetings or discussions with AnnaLou in the days and weeks
21 following January 6th?

22 A I mean, it would have come up, I feel pretty confident, in leadership
23 meetings. But I don't remember specific conversations with her, specific meetings
24 dedicated to that purpose.

25 Q I guess just more broadly, how are you gaining this understanding of FinCEN

1 leadership's involvement?

2 A Well, as I think I mentioned a few minutes ago, I was aware that these
3 exchanges were going on, and I was aware that the senior leadership of the agency was
4 focused on this and was involved.

5 So it wasn't a secret that these exchanges were occurring, and I was aware they
6 were going on. And as I think I mentioned a few minutes ago, I feel pretty confident
7 that at least references to this work would've been raised in like senior management
8 meetings. So I was aware that it was going on.

9 Q I guess could you just walk me through a little bit more about what your role
10 was and what discussions you were having?

11 You're talking about FinCEN leadership is paying attention to this, and then there
12 are the analysts within your team that are working on this.

13 Who's talking to the analysts? Are these two separate discussions? Are they
14 intermediary? It's just it's not clear what your role is at this time.

15 A So I think I mentioned earlier today that about 90 days before this is when I
16 stepped into this role as head of this division. It was a pretty substantial change in
17 nature of responsibilities for me.

18 And also I had not been an intelligence analyst before. So this was a fairly
19 substantial change from serving as the legal adviser, and also the position I stepped into
20 had been vacant for some period of time.

21 So a fair amount of my efforts at the beginning of this job were, frankly, getting
22 my hands around the management functions, who sits where, who's -- that sort of stuff.

23 ■ had previously been chief of staff to the director, so it would not have struck
24 me as strange to have leadership working directly with her given their longstanding
25 relationship. And ■ is a very impressive individual. So, again, nothing about that

1 would've struck me as strange or unusual.

2 So I was not very involved in this sort of overall exchange effort. From where I
3 sat at the time, looking back on it, my impression was it was sufficiently staffed at a senior
4 management level that I didn't sort of see myself as adding a lot of additional value
5 beyond the managers who were already involved in that space.

6 And so maybe that's the best answer I can give you to your question.

7 Q Okay. And is [REDACTED] having regular interactions with the analysts who were
8 working on this?

9 A I don't know the answer to that question for sure, but it wouldn't -- again, it
10 wouldn't have struck me as unusual if she was.

11 Q Okay. What about like January 5th, before any of this happens, what was
12 the nature? You've only been on the job for 90 days. [REDACTED] has longer lasting
13 relationships with some of the analyst folks. Is that --

14 A I think that's probably accurate. But also we're in the middle of a transition
15 period. We've just come through the -- I mean, there's just a lot going on at that time.
16 So it's not as though people were just sort of like sitting around waiting for things to
17 happen. But then this happened and we had these requests from law enforcement and
18 others to sort of engage in this work.

19 So I don't -- it would never strike me as strange for teams to sort
20 of -- management teams anyway -- to sort of divide and conquer different topics based on
21 background or expertise or even personal relationships.

22 But I can only speak to sort of my own involvement. It was not extensive in
23 these exchanges while they were going on.

24 Q Were the analysts briefing FinCEN leadership directly?

25 A I would presume yes.

1 Q Do you recall a time period?

2 A But I don't know for sure, but I would presume yes.

3 Q Other than the six or seven folks who were on the counterterrorism team,
4 do you know of any other analysts within the team that were pulled on to work on this?

5 A Not specifically, no. It would not surprise me if some of the data quality or
6 folks like that who are just familiar with tracking stuff in the database, it wouldn't surprise
7 me if those folks were sort of pulled in to make sure any incoming filings were being seen.
8 But I don't recall specifically beyond any additional folks particularly.

9 Q For documents like the slide show, independent of this specific example, but
10 we'll say January 5th, so it's just independent of this specific example, if there was
11 incoming information that [REDACTED] receives and his job is just to interface, before he
12 then goes and shares about what he shared with us that he would send it to someone
13 else within FinCEN, was that a type of consideration that would get sent to your desk, to
14 [REDACTED] desk, to someone else? What's the nature of things that are sent to you directly?

15 A I don't know who [REDACTED] would've sent that to. [REDACTED] didn't work for me.
16 So I can't really speculate who -- I don't know who he did or did not send things to on
17 January 5th or before.

18 The FinCEN Exchange was codified in the statute right at the beginning of the year.
19 There were some number of these exchange -- exchanges like these that had gone on
20 previously, but at least the sort of exchange in its current form is sort of very much a
21 product of early 2021. But, again, I don't know who [REDACTED] would've sent what he was
22 sending to before, say, January 5th or before.

23 Q We've referenced a couple of the meeting notes. Do you recall just even at
24 a general level being on any Zoom calls or in-person meetings with FinCEN leadership
25 about analysis that was being conducted following January 6th?

1 A As I mentioned before, pretty confident this would've come up in senior
2 management meetings. At the time many of those would've been on Zoom.

3 So in that context, yes, I don't recall the particulars of the discussion, but I'm
4 pretty confident it would've come up in those discussions.

5 ██████████ And there, I just want to make -- you testified earlier about sort
6 of when -- about all of the ADs over the various divisions sort of standing -- I think you
7 said you thought they were weekly meetings. Is that what you're referring to here when
8 you sort of say senior management meetings, or are there --

9 Mr. Kirby. Yes. At the time, my recollection is we had a weekly senior
10 leadership meeting. There may have been meetings beyond that given the nature of
11 what was -- the attack on January 6th and the aftermath of that. But at the time we
12 did, my recollection, have standing senior management meetings once a week.

13 ██████████ And so in an earlier answer, based off your kind of broad
14 understanding of what was going on at the time, that analysts likely were briefing FinCEN
15 leadership, are the analysts getting pulled into the standing meeting, or is it your
16 understanding there were separate meetings going on?

17 Mr. Kirby. I think those would've likely been separate meetings if they occurred.
18 But I don't recall any sort of specific meetings in that regard. Yeah.

19 ██████████ Would an email like this have been sent without being reviewed
20 by an analyst?

21 ██████████ Just for the record, we're talking about exhibit 5?

22 ██████████ Yeah, exhibit 5, the bank submission, the attachments.

23 ██████████ So we're talking about the first attachment, bank submission,
24 on exhibit 5.

25 ██████████ Yes.

1 Mr. Kirby. And an analyst in the then-Intelligence Division?

2 [REDACTED] Correct.

3 Mr. Kirby. I don't know. I don't know if [REDACTED] sent this to someone in the
4 Intelligence Division before he sent this or not.

5

BY [REDACTED]

6 Q There wasn't a general protocol for Intelligence Division to sign off on things
7 before they were being sent out by individuals like [REDACTED]?

8 A I'm not aware of such a protocol. I mean, the events around January 6th
9 are kind of a unique circumstance, so I don't know that we would've had a standing
10 protocol in anticipation of such a thing. But I'm not aware -- I don't believe there would
11 be a protocol sort of like requiring that in all instances. I was not aware of one at the
12 time.

13 Q And you may have answered this earlier. Did the Intelligence Division
14 create these typologies on exhibit 5, the indicators developed from prior FinCEN analysis?

15 A I don't know the answer to that.

16 Q Do you know who would --

17 A Someone like AnnaLou, [REDACTED], or [REDACTED] might. If they are derived from
18 FinCEN analysis it would make sense to me that that would've come from the Intelligence
19 Division, because that's the function at the time that they performed.

20 So, for instance, I would not have expected [REDACTED] to sort of come up with
21 something like this on his own. So it would make sense that if it was developed at
22 FinCEN it was developed in the Intelligence Division.

23 Q Were these typologies or indicators made public? I know you mentioned
24 earlier that you published certain typologies.

25 A Uh-huh.

1 Q Do you know if these were made public?

2 A I don't know. I don't believe so. And, again, these may be more like red
3 flag data points if anything else. These at the bottom I don't think were ever made
4 public. I don't recall off the top of my head.

5 I'm kind of trying to mentally scan through products that I know were on our
6 website. I don't recall us putting a product like this on our website.

7 And one rationale for that, frankly, might be you don't want to alert people that
8 are thinking about doing this to necessarily how some of their activity may be seen,
9 would be one potential reason not to do that.

10 But I don't recall this being made public otherwise.

11 Q Do you know how these kinds of indicators -- what analysis would be
12 performed to create these kinds of indicators?

13 A I know in the past there has been interest in trying to figure out if there are
14 ways to anticipate lone actor attacks and if there are red flags that can be sort of
15 discerned from that.

16 If these were produced at FinCEN my guess would be that they were part of a
17 work stream of that type, but I don't know when they would've been produced.

18 Q But what are you analyzing?

19 A Oh.

20 Q When you're producing an indicator, what does that analysis look like?

21 A Going back to something we at some point today have talked about, I don't
22 know whose question it was, we talked about how financial institutions will often ingest
23 public news reporting as part of their AML program.

24 So, for instance, in the context of someone being identified as a suspect in an
25 action, like a lone shooter action, that could prompt financial institutions to check their

1 own records to see what they have on that individual, with the benefit of that new
2 information evaluate whether any of that might be suspicious activity that should be
3 reported to FinCEN.

4 And so one area of analysis in that regard could be if a bank were to file a
5 look-back SAR after learning that one of their customers were involved potentially in one
6 of these actions and then sort of evaluating.

7 So if you're asking like what is the person analyzing, one piece of data they may be
8 looking at is what types of filings are we getting on individuals that are identified as
9 having engaged in this sort of conduct and are there commonalities or other things that
10 can be drawn from that as some sort of -- that would be one potential area they're
11 looking at.

12 To the extent we're working with law enforcement on something of this type they
13 may also glean information that law enforcement may know in this space.

14 And so it could be a couple of different areas, but those are two that kind of stand
15 out to me that they could be looking at in the first instance.

16 Q And when FinCEN shares materials like this, how are they expected to be
17 used?

18 A So to be honest with you, I don't know how many examples we have of
19 sharing information like this.

20 It sounds like -- and, again, just based only on the emails -- the email, singular -- it
21 looks like the expectation is that this is going to form some portion of a conversation.

22 To the extent that's the case, it's comparing different approaches and
23 methodologies different institutions are using to the extent -- I mean, I could -- that
24 would sort of make sense to me given the table-setting email here.

25 But I don't know in the abstract that there's sort of a default expectation of what a

1 financial institution would do with something like this or information and materials like
2 this.

3 Q One of the indicators includes, quote, "The purchase of books (including
4 religious texts) and subscriptions to other media containing extremist views."

5 Do you have an idea of how FinCEN could have conducted an analysis to conclude
6 that as an indicator?

7 A I don't. I think the "extremist views" part of that I could see where if you're
8 thinking about that in terms of like jihadi materials, that could be one example of that in
9 particular potentially. But I don't know where that came from.

10

BY [REDACTED]

11 Q How would FinCEN figure out that an individual was purchasing jihadi
12 material?

13 A So I don't think it would be us that figures that out on the first instance. I
14 think it would be the filer. And I think it would depend a lot on what information the
15 filer has access to.

16 So to sort of go outside the four corners of our conversation but to go to where
17 this has come up in other circumstances, one question I've heard raised in hearings is,
18 "Well, should people be filing on purchases of Bibles and things like that?"

19 Most of the time I don't think your typical filer is going to see that. They
20 shouldn't be filing on that anyway, to be very clear. But if you go to Barnes & Noble and
21 buy "insert name of religious text," whatever text you're buying, I don't know that your
22 payment processor or anyone is actually going to see that.

23 So I think it depends on like what information -- and broadening the aperture out
24 to an AML program, all the sources of information an individual financial institution,
25 individual filer has at their disposal, they may see things in a certain context in the

1 transactional space that may prompt them to file.

2 That's not something FinCEN would necessarily see. The only thing we're going
3 to see in most instances is going to be my financial institution saw something that caused
4 them to be concerned of potential relevant to any possible violation of law or regulation.
5 You sort of go back to that standard, it's a pretty broad standard, and they may file on
6 that.

7

BY [REDACTED]

8 Q Does FinCEN have a determination of what media contains extremist views?

9 A Not that I'm aware of, no.

10 Q Do you know whether any financial institution or FinCEN expressed a
11 concern that suggesting the purchase of religious texts might encroach on Americans'
12 right to religious freedom?

13 A I don't recall any conversations of that type. I don't know that I necessarily
14 would've been included or involved in those types of discussions.

15 But at the end of the day, FinCEN is an organization that is not out, in my
16 experience, looking to suppress people's constitutional First Amendment rights. So that
17 is not something in the first instance I think any employee of FinCEN in this space
18 would've been looking to do. That's just based on my experience of working for the
19 organization. I'm relatively confident in saying that.

20 Q Do you know who would've been involved in those conversations?

21 A Again, my guess, as this was sort of centered in our Strategic Operations
22 Division, my guess would be managers in that space, up to and including Ms. Tirol and
23 possibly our Chief Counsel's Office, which I was no longer in at the time.

24 [REDACTED] But I just want to be clear from that answer, I think there's a
25 premise in your question that those conversations took place, and his testimony was

1 actually that he doesn't recall if there were any such conversations. So I want to make
2 sure that answer is clear.

3

BY [REDACTED]

4

Q Another one of the extremist indicators includes, "Donations to

5

organizations known to promote radicalism."

6

Does FinCEN have a list of organizations known to promote radicalism?

7

A Not that I'm aware of, no.

8

Q Do you know how an analysis would've concluded what organizations are

9

known to promote radicalism?

10

A I don't, no.

11

Q Are you aware of whether any SARs were generated on the basis of these

12

extremism indicators?

13

A I don't know if SARs were generated based on this.

14

BY [REDACTED]

15

Q Who at FinCEN would know where this analysis came from?

16

A I mean, I would start probably in the Strategic Operations Division, since

17

that's where the communications came from, and then work backwards from there.

18

And so I think all of these folks we've been talking about, they no longer work at

19

FinCEN, which would be a challenge in terms of working backwards in that regard

20

because they're no longer with the agency. We've had quite a bit of turnover in the

21

agency in the last couple years. But as a threshold matter that's where I'd be inclined to

22

start.

23

Q I guess, just based off your experience at the time, in mid-January 2021, if

24

you're seeing a list like this, where do you think within FinCEN someone is doing that type

25

of analysis?

1 A As I think I indicated before, if this was prepared at FinCEN I think it's a fair
2 conclusion to assume that it was likely prepared in the Intelligence Division, because
3 that's where that -- that's where I would expect -- analytic work, we're looking at filings
4 and other materials to try to generate red flags and typologies, I would expect that work
5 to happen there.

6 Q If you had follow-up questions about what some of these points mean, who
7 within the Intelligence Division would you consult with?

8 A In the first instance at the time I would've gone to [REDACTED], who is no longer at
9 FinCEN either. So I'm not sure who I would ask now about this, to be honest. I would
10 probably have to do some digging given the passage of time.

11 Q I mean, presumably this information is being shared to try to be helpful to
12 recipients on the list.

13 A That's my assumption, yes.

14 Q And if one of the recipients doesn't understand what one of the bullet points
15 means and you're the director of the Intelligence Division, we're just trying to get a sense
16 of who might know the answer to these questions.

17 A I think I answered that a minute ago. I said I would have gone to [REDACTED] at the
18 time. But [REDACTED] is not there anymore. And so I would need to figure out who to go to in
19 lieu of [REDACTED] with the passage of 3 and a half years. This didn't happen last week, with all
20 due respect.

21 Q I understand that.

22 For a list like this, when it's going to the banks -- obviously you're not copied on
23 this particular email -- are you receiving briefings?

24 We're just trying to get a sense of in the hierarchy, where you've got the analysts
25 themselves who are like maybe tip of the spear of trying to figure out the issue they're

1 working on, are you getting regular briefings? Is this too granular? Are you too new?

2 Like why is it that -- it seems, at least based off the answers, maybe not as much
3 familiarity with the meanings of these different bullet points.

4 A Uh-huh. I think it maybe is a mix of -- I was pretty new in the role. The
5 leadership at the time was working directly with members of the team. It was my
6 understanding people that they knew worked in the terrorism space.

7 We also weren't all sitting next to each other at this time because it was during
8 the COVID period, so it wasn't -- you didn't just walk down the hall and start up a
9 conversation on something like this like we do before and like we do now.

10 And it wouldn't have then nor now strike me as strange or unusual for different
11 managers to focus -- particularly senior managers -- to focus on different aspects of the
12 work stream.

13 So I think that's probably the best answer I have for you on that.

14 Q Did you ever receive any briefings about concerns, whether it was typologies
15 or kind of related issues, of whether any of that kind of work implicates the First
16 Amendment?

17 A I don't recall any briefings to that effect.

18 [REDACTED] When these indicators and search terms are sent out, what --

19 [REDACTED] I think I'll stop there. He's not testified that these are search
20 terms. He's actually testified several times that they are not search terms. He said
21 they're red flag indicators. So if you want to rephrase we can start over.

22

BY [REDACTED]

23 Q What methods could banks use to implement these red flags and monitor
24 transactions? You mentioned a moment ago that banks might be able to see things that
25 FinCEN can't.

1 A Uh-huh.

2 Q Could you elaborate a little on that?

3 A Sure.

4 I think we've talked about earlier today one of the obligations that the Bank
5 Secrecy Act imposes and our implementing regs impose on banks is the requirement to
6 have an anti-money laundering program reasonably designed to essentially sort of detect
7 this suspicious activity, improper activity, that sort of stuff.

8 So whatever system they have put in place for that -- and some of that is probably
9 going to be an automated screening system.

10 So, for instance, like the OFAC SDN list, my understanding is that a number of
11 banks have automated screening systems to run those names against transactions to
12 ensure they're not dealing with designated terrorists, designated kingpins, those sorts of
13 folks that no one wants -- they don't want to deal with, we don't want them dealing with.

14 So they have program staff in place to be able to sort of know their customers,
15 evaluate the transactions going on through their institutions.

16 And so sharing information with them for them to feed into that overall program
17 is what I was kind of referring to in that regard, is we share information with the
18 hope -- they know their customers far better than we do.

19 We share information that is potentially helpful for them in understanding
20 broader illicit finance typologies, red flags that may indicate such typologies, with the
21 hope that it's helpful for them in terms of administering their overall program and
22 hopefully driving greater reporting to FinCEN.

23 Q So let's use the examples here specifically.

24 One of the red flags is MAGA, America First. How could that get implemented
25 into the AML system?

1 A So I think, as we talked about earlier today, I think one of the things we
2 would tell folks, and we do say this in our alert and other materials, is there is usually a
3 statement that no one red flag is indicative of any problematic activity.

4 That, again, my understanding is that at the time you see a bunch of terms here,
5 many of which they're both parties, people from both parties, terms like kill, shoot, blow,
6 which I'm assuming means blow up, is one -- gun, death, murder.

7 I read these as being targeted towards combating violence, which at the time
8 there was substantial concern, my recollection is, not in the post-January 6th
9 environment, concerns about violence given the pending inauguration.

10 So you've got a number of names on this list, individual data points, that if
11 someone is talking about violence in the context of any of these folks, that's how I'm
12 reading this broadly.

13 It's hard for me to sort of speak specifically as to one-offs of these terms, how
14 they might be implicated -- incorporated into a financial institution's overall AML
15 program, because at least the way I think of this, we generally tell financial institutions
16 that no one term is meant to be indicative of necessarily something.

17 You're sort of supposed to take these terms holistically and look at them against
18 sort of your sort of broader knowledge about the customer.

19 But I can't answer that specific, "How are they supposed to take that one term?"
20 I don't view it as just one term. They're sharing a list of terms, many of which are aimed
21 at violent activity.

1 [3:11 p.m.]

2

BY [REDACTED]

3

Q That statement of one term alone isn't included in this.

4

A It's not included in that. I appreciate that.

5

Q Moving to the red flags or the indicators portion, how could a bank

6

incorporate, again, donations to organizations known to promote radicalism, the

7

purchase of books, including religious texts and subscriptions to other media containing

8

extremist views, how does that get incorporated into an AML program?

9

A I'm going back to the conversation we just had. I think you would sort of

10

look at them holistically because there's also discussions in here of, you know, purchase

11

of precursor chemicals, potential bomb-making equipment, ammonium nitrate, you

12

know, sudden account closures, asset liquidation, disbursements.

13

Any one of those things may not stand out, but if you're seeing holistically

14

multiple indicators of this, I could see where an analyst may have been thinking -- and,

15

again, I don't know the underlying material they were looking at, but against a backdrop

16

of this suggests it was developed in the context of, sort of, attempting to combat lone

17

actors and how -- you know, trying to think about it, if there are indicators that folks

18

would be looking for that on the front end instead of just on the back end, it's obviously

19

easier when you know who the person is that did it after the fact to look back on there

20

what they did, you know.

21

[REDACTED] [REDACTED] is your question more a mechanical one, like, how would

22

a bank actually -- what would a bank actually do with any of these? I just want to make

23

sure we're, like, understanding the question there.

24

[REDACTED] My question is FinCEN is sharing materials that are, ostensibly,

25

useful to the bank. I'm asking how they're useful to the bank, how they can actually be

1 implemented.

2 [REDACTED] Because I think to the -- what I was going to say, to the
3 mechanics of that, is, like, you may be able to speak to that in a general term. But he
4 testified earlier, like, he never worked at a financial institution, right? And, like,
5 wouldn't have been engaging with the financial institutions on a regular basis in the role
6 that he was in during this time period.

7 So, like, to the extent he has, sort of, general knowledge of that, he can answer.
8 But, like, I think those are sort of questions about -- for the mechanics of how a bank
9 takes whatever these documents are and integrates them, I think it's going to vary widely,
10 and it's not something that's necessarily, like, his primary knowledge.

11 [REDACTED] Can we go off the record for a second.

12 [Discussion off the record.]

13 [REDACTED] All right. We can go back on the record.

14 I'd like to introduce two email threads. We have the full thread. The first one
15 involves MUFG sending an email to AnnaLou -- or to [REDACTED], and
16 AnnaLou Tirol, with the subject line "Major D.C. Transportation Vendor Lists."

17 And the second is a thread -- only interested in the top email -- from [REDACTED]
18 to various financial institutions, sending that "Major D.C. Transportation Vendor Lists"
19 Excel sheet. And this is exhibit 7.

20 [Kirby Exhibit No. 7

21 was marked for identification.]

22 Mr. Kirby. Okay.

23 [REDACTED] I will also introduce the vendor list that was attached, the Excel
24 sheet, as exhibit 8. I'll just note for the record that these were sent as native documents
25 so they're not Bates stamped. They were printed off of Excel. We're not going to go

1 through this individually.

2 [Kirby Exhibit No. 8

3 was marked for identification.]

4 [REDACTED] And the different sections, there's different tabs of the Excel
5 worksheet?

6 [REDACTED] They were separate, yes.

7 Mr. Kirby. Okay.

8 [REDACTED] Have you seen this email or this Excel document before.

9 Mr. Kirby. So in connection with the questions that have been coming up over
10 the course of this year, I have previously seen the -- I think I've seen this list. I don't
11 know that I've seen the email before, but I -- I do recall at some point over the course of
12 this year having seen a vendor list, the airport -- I don't know if I've seen the email before.

13 [REDACTED] Just so the record is clear, when you refer to that -- did you
14 come and voluntarily provide a briefing on behalf of FinCEN to the committee in
15 connection with this inquiry?

16 Mr. Kirby. Yes.

17 [REDACTED] Is that what you're referring to --

18 Mr. Kirby. Yes.

19 [REDACTED] -- when you say "in connection with these questions"?

20 Mr. Kirby. Yes. I think you were both -- most of y'all were in the briefing earlier
21 this year.

22 [REDACTED] I don't know that we got that on the record yet.

23 Mr. Kirby. Okay.

24 [REDACTED] So I just want to make that clear.

25 Mr. Kirby. Yes. I was here in March and briefed on, I think, your committee

1 staff and House Financial Services committee staff on similar questions in this space. So
2 we did some work in this space.

3 And, again, I don't recall if I've seen this before, but I -- I don't know if it was the
4 same list, but I have seen a vendor list at the three airports.

5

BY [REDACTED]

6 Q And did you see this in the weeks after January 6th, or was the first time you
7 saw it this year when you were preparing for the briefing?

8 A The first time I recall seeing it is earlier this year when I was preparing for the
9 briefing. I think that was in March.

10 Q If I can just ask generally, how would a list like this, vendors at the three
11 airports in D.C., Union Station, bus stops -- bus stops, how is that useful for financial
12 institutions?

13 A My assumption would be that this was a means of identifying transactional
14 activity in the region around that time. So if you saw transactional activity involving
15 these vendors, that could be an indicator that -- and at the airport, that the person was
16 traveling in or out during that period.

17 Q Traveling to D.C., eating at Chick-Fil-A or Dunkin' Donuts, that's not -- that
18 doesn't have any nexus to criminal activity. Is that correct?

19 A I agree with you in that going to Chick-Fil-A is not indicative of anything
20 criminal or improper.

21 My guess would be this context is they're feeding into that broader email program
22 that they're seeing, sort of, other potential indicia of involvement in the activity.
23 Perhaps this is a way of confirming whether the person was here during that time.

24 That would just be my, sort of, very high-level guess, is it would be a confirmation
25 of a location as opposed to the individual place the person went. That's how I would

1 read it.

2 Q In sharing this list with financial institutions, was FinCEN directing those
3 financial institutions or encouraging those financial institutions to track and scrutinize all
4 purchases made at those vendors?

5 A So I wasn't involved, to the best of my recollection, whatever comms
6 happened at the time, so I can't speak to that. We would normally not -- again, sort of
7 hard to draw normal in the space that we're referring to at the moment.

8 But, like, we would not -- when we share information with financial institutions, it
9 would normally not be as an instruction to here are four red flags of X, go, like, search
10 everything you have for that. That's not how we would normally communicate
11 something.

12 However, I was not -- I have no recollection of being involved in any
13 back-and-forth with FIs on -- I'm sorry -- financial institutions on this, and so I can't speak
14 to this circumstance specifically.

15 BY [REDACTED]

16 Q [REDACTED] is on this email. Do you remember ever discussing this with
17 her?

18 A I do not, no.

19 Q Do you know who may have approved of sharing the vendor list?

20 A I don't. AnnaLou is the most senior manager, at least that I can see on at
21 least the top-level email. The print, as we go into the later ones, gets a little small, AND
22 it's kind of packed in together.

23 So I can't see if there are other -- it looks like for most of these, AnnaLou is the
24 most senior manager on the chain.

25 BY [REDACTED]

1 Q Would AnnaLou have been in a position to provide permission to share this
2 type of information with financial institutions?

3 A I mean, she over- -- she was the head of our strategic operations division in
4 January of 2021, and one of their principal functions is this information exchange, this
5 FinCEN Exchange, the BSAAG that I've mentioned -- the Bank Secrecy Act Advisory Group
6 that I mentioned before, responsibility for both of those functions is housed in that
7 division. So I don't know if she approved this, but I would assume she could
8 approve -- could have approved such a thing if she had -- if she had been asked.

9 Q If a bank is searching transactions made at transportation -- vendors at
10 airports like this, is that likely to sweep in lots of people totally removed from any
11 criminal activity if they're looking to see who might have been in D.C. on these dates?

12 A So I can't -- it's hard for me to speak to what banks are doing in their own
13 programs because, you know, they have the obligation to, sort of, know their customer,
14 have an AML program, all of that sort of stuff.

15 If I go back -- we talked about -- I think we talked about this before. If we go
16 back to the standard that's in the -- that's in the statute for suspicious activity, it's
17 relevant to any possible violation of law or regulation.

18 So, you know, to the extent one aspect of relevance is was someone at a certain
19 location, it's hard for me to say that that, across the board, would be something that a
20 financial institution wouldn't look at depending upon what kind of questions they're
21 getting, depending upon what else they have in -- in front of them.

22 I wouldn't -- I would not assume that any of these would be something that a
23 financial institution, in and of itself, would file on. That just would be my, sort of,
24 after-the-fact guess.

25 But, you know, it's hard for me to speak with deep specificity as to what bank A or

1 bank B, with all the other information they may have had before them, how they made
2 use of this information one way or the other.

3 Q Would you say that BSA filings taken as a whole are overinclusive?

4 A Overinclusive?

5 Q If the standard is any possible violation?

6 A So I don't know that overinclusive is the word I would use. But I would say
7 the statute -- you go back to the statutory language. The statute lays out a program that
8 very much leans in in terms of encouraging reporting.

9 On top of leaning in and encouraging reporting, the statute builds a number of
10 protections around both the filers and the information they file. And so, you know,
11 we've already talked to some extent about, you know, the penalties for improper
12 disclosure, the safe harbors that go around reporting of the information to FinCEN.

13 On top of that, we have, you know, MOUs that govern, you know, access to the
14 information given the sensitivity of the information.

15 So the entire statutory construct is very -- I read very much -- others may read it
16 differently, but I read very much as sort of leaning in on the question that, you know, it
17 errs in favor of having them report because it's not evidence -- SAR -- we're very clear on
18 this. We've said this in lots of different fora. SAR filings are not evidence of anything.
19 They are tip-and-lead information. That's why they're -- among the reasons they're so
20 protected.

21 But just because someone files a SAR on me for whatever reason, that in and of
22 itself is not proof of anything I did or did not do. There are other ways that investigatory
23 agency needs to determine that information. It's not through using the SAR.

24 [REDACTED] We can go off the record.

25 [Recess.]

1 [REDACTED] We can go back on the record. It's 3:38 in the afternoon.

2 BY [REDACTED]

3 Q Mr. Kirby, I want to return to exhibit 5. You were asked a number of
4 questions about that exhibit. I just want to make sure that none of your words get kind
5 of twisted afterwards.

6 A Okay. I have it.

7 Q And this is an email. We've been through it in a couple different iterations,
8 but this is an email dated Friday, January 15th, 2021, time stamped 4:00:25 p.m. And
9 it's Bates stamped HJC118, a lot of zeros, and 5. You see where it says that?

10 A Yep.

11 Q I realize there are redactions in the emails, but you are not on this email list,
12 correct?

13 A I do not see myself on this email.

14 Q Okay. And, in fact --

15 A Unless it's hidden under one of these redactions, I don't see it.

16 Q And, in fact, the FinCEN names are not redacted, correct?

17 A Correct.

18 Q So if you were on this --

19 A I would probably be able to see it.

20 Q -- it would probably be evident, correct?

21 And you said that you don't recall having seen this before, correct?

22 A No.

23 Q Okay. So to the extent that you commented on it, it was kind of your best
24 guess or speculation, but you don't actually have any knowledge of how this email came
25 to be or the contents of it outside of, you know, what's in front of you?

1 A That's correct.

2 Q Okay.

3 A Or in connection with preparing for the briefing I did earlier this year.

4 Q Okay.

5 A So some of this stuff I -- I think I saw the slide deck in connection with
6 preparing for that.

7 Q Okay. But you weren't aware of it in January of 2021, correct?

8 A That's correct. Not that I recall, no.

9 Q Okay. I want to look at -- on page 6 under section 2. It says, "Lone actor,
10 homegrown violent extremism indicators developed from prior FinCEN analysis." You
11 see where it says that?

12 A Yes.

13 Q And it says developed from prior FinCEN analysis. It doesn't actually say it's
14 taken directly from prior FinCEN analyses, correct?

15 A That's correct, yes.

16 Q Okay. And, actually, turning back to the prior page, the email is from
17 [REDACTED] -- it's somebody named [REDACTED]. Presumably, it's [REDACTED] who is listed on the
18 from line, correct?

19 A Yes.

20 Q And [REDACTED] says, "In advance of the 4:30 call, please find attached indicators
21 shared by two institutions, as well as indicators developed from prior FinCEN analysis on
22 lone actors, homegrown violent extremists."

23 You see where it says that?

24 A Yes.

25 Q And it specifically says "indicators developed from," correct?

- 1 A Yes.
- 2 Q That's the passive voice, correct?
- 3 A Yes.
- 4 Q In other words, we don't know who developed these, correct?
- 5 A That is correct, yes.
- 6 Q And we don't know how they were developed?
- 7 A I do not know how they were developed, no.
- 8 Q Okay. And so we don't actually know if it was -- if these are FinCEN bullet
9 points or if they're summaries of some documents or if -- or who put them together,
10 correct? We just don't know?
- 11 A Yeah, that makes sense.
- 12 Q So you agree with me, we don't know?
- 13 A Yes. Sorry.
- 14 Q And I think the -- because I think the comment was made earlier that these
15 are FinCEN's bullets, and I think there's actually not evidence of that, correct?
- 16 A Other than what's on the form here, the developed from prior FinCEN
17 analysis.
- 18 Q But, again, it says "developed from," it doesn't say taken from directly,
19 correct?
- 20 A Yes.
- 21 Q And it doesn't say who developed them?
- 22 A That's correct.
- 23 Q Or how they did that?
- 24 A That's correct, yes.
- 25 BY [REDACTED]

1 Q I want to take a step back and just talk about the context in which all of
2 these emails -- which, again, you are not on -- were sent and what was happening in the
3 country in that time period.

4 These emails were sent in the weeks following the violent assault on the Capitol
5 on January 6, 2021, correct?

6 A Yes.

7 Q Okay. And are you aware that the director of the FBI has referred to the
8 events of that day as an act of domestic terrorism?

9 A Yes.

10 Q And is that how FinCEN approached this investigation into the events of
11 January 6th, that it was investigating a domestic terrorism attack?

12 A At the time, yeah, I think that was -- that was my understanding at the time,
13 yes.

14 Q And FinCEN was aware that law enforcement agencies, including the FBI, in
15 mid-January of 2021 had issued public warnings about a substantial risk of violence in
16 connection with the upcoming inauguration, correct?

17 A Yes, that's -- again, that is my recollection at the time, there was a lot of
18 concern around the upcoming inauguration.

19 Q And is it your recollection that Federal law enforcement agencies, as well as
20 FinCEN, were focused on preventing similar violent attacks on our domestic institutions?

21 A Yes. That sounds -- that sounds right based on my recollection at the time.

22 Q And the inauguration of President Biden was scheduled for just two weeks
23 after January 6th, for January 20th, 2021. Does that sound --

24 A That sounds right.

25 Q -- correct?

1 Okay. And FinCEN was working with law enforcement and with financial
2 institutions to try to prevent the type of violence we saw on January 6th at the
3 inauguration. Is that a fair statement?

4 A That was my understanding of a key goal of this effort.

5 Q And the FinCEN exchanges related to January 6th that were set up in those
6 days and weeks afterwards were geared towards that effort of preventing future
7 violence, as well as identifying those who were responsible for the attack on January 6th.
8 Is that a fair statement?

9 A I mean, that generally is my understanding. Like I said, I wasn't very
10 involved in them. I was aware they were going on, but at a big-picture level, that -- that
11 comports with my general understanding at the time.

12 Q Okay. Now, I want to take you back -- if I could have exhibit 5. I want to
13 ask you some different questions about exhibit 5.

14 On the second page, the one with Bates number 6 -- well, my first question is,
15 when [REDACTED] sent this email to the banks, in this email did he ask the banks to conduct
16 any searches based on these terms?

17 A Not that I can see from the document.

18 Q Did he ask the banks to file a SAR for any transaction that had one of these
19 terms associated with it?

20 A Not that I can see from the document.

21 Q So if someone were to look at this email and say that FinCEN was telling
22 banks to flag Zelle transactions that use the word Trump, for example, as a suspicious
23 transaction, that would not be accurate, would it?

24 A That's -- the document doesn't say that, that's correct.

25 Q And it's the same for any one of the terms on that list?

1 A Yeah. The document doesn't say that for any of the terms on the list.

2 Q Now, the majority has cited this email as evidence of FinCEN targeting bank
3 customers with conservative viewpoints. But as you pointed out in the previous hour,
4 there are words on this list that -- that address both parties. For example, the fourth
5 term is Kamala, correct?

6 A Correct, yes.

7 Q And the fifth term is Biden?

8 A Correct, yes.

9 Q The term Antifa is on there?

10 A Correct, yes.

11 Q And Pelosi is one of the terms?

12 A Correct, yes.

13 Q And Schumer is the last one?

14 A Correct, yes.

15 Q And I believe you've said this many times, but I think it bears repeating,
16 generally speaking, when FinCEN talks about red flags or typologies, it does not intend
17 any one of them to, standing alone, be sufficient to file a SAR?

18 A Yes, that's correct.

19 Q And that is true with respect to the lone actor/homegrown violent
20 extremism indicators portion of this email as well?

21 A I would read them as consistent with how we say this in other contexts, so,
22 yes.

23 Q And nowhere in this email, whether it's with respect to the first list or the
24 second list, is there any request for any transactions to be flagged in any way or any SARs
25 to be filed?

1 A That's correct.

2 Q Now, I would like to turn to exhibits 7 and 8, in conjunction.

3 There is no request in this email for financial institutions to file SARs or otherwise
4 flag transactions for the vendors listed in exhibit 8?

5 A Not that I see in the email chain, no.

6 Q And if someone were to look at this email chain and say that FinCEN was
7 telling banks to file SARs or otherwise flag transactions for anybody who frequented the
8 Dunkin' Donuts at whichever airport is at 1 Aviation Circle -- I'm assuming that's Dulles
9 based on the phone number -- that would be incorrect?

10 A I don't read the email as saying that, no.

11 Q And that's true of any one of the vendors listed here. Is that fair to say?

12 A The gist of the email seems to focus on the location of the three airports, the
13 train station, and the bus stops.

14 Q But the email does not say, we want you to identify any customer who --

15 A Correct.

16 Q -- frequented one of these establishments?

17 A That's correct. It doesn't say that.

18 Q And would you expect, based on your experience with FinCEN typologies and
19 red flags and based on your experience with how banks determine whether or not to file
20 SARs, that this is one of many, many, many types of indicators that would be considered
21 before a bank decided to file a SAR?

22 A I would assume so, yes.

23 Q And, again, your focus -- FinCEN's focus. I don't mean you
24 personally -- FinCEN's focus in January of 2021 was preventing the type of violence that
25 we saw on January 6th?

1 A Yes. My understanding is safeguarding the inauguration was one of the
2 principal goals of this effort.

3 Q And one way to safeguard it would be to try to identify people who
4 participated in that violent assault on the Capitol and intended to return to the
5 inauguration to complete their mission of disrupting the peaceful transfer of power,
6 correct?

7 A That would make sense, yes, the legitimate focus of law enforcement.

8 [REDACTED] Thank you. We can go off the record.

9 [Recess.]

10 [REDACTED] We can go back on the record.

11

BY [REDACTED]

12 Q So we've discussed a number of these emails that were sent from [REDACTED]
13 [REDACTED] from [REDACTED], many of which included [REDACTED], but that haven't
14 included you.

15 Is there a reason why you would have been left off of these emails?

16 A I think it's hard for me to answer that question in the abstract. I think it is a
17 reflection of the fact that I was not very involved in this particular work stream. So
18 there were others involved in the work stream at a senior management level, so that
19 would be my assumption and guess.

20 Q And that would have been [REDACTED], AnnaLou that were the senior
21 executives on these emails?

22 A So AnnaLou was a senior executive. [REDACTED] was not, but was a GS-15.
23 AnnaLou was actually a senior executive. But, yeah, they're both senior managers.

24 Q And at this time she was your deputy?

25 A Correct.

1 BY [REDACTED]

2 Q [REDACTED] was?

3 A [REDACTED] yes. Sorry.

4 Q When you came, you know that you were relatively new, only about 90 days
5 in. When did [REDACTED] come in as your deputy?

6 A I think we actually both started the same day. Both -- both of us, I think,
7 were October of that prior year. We may have actually started on the same day in our
8 respective roles.

9 Q At that time did you sort of split some leadership roles given her experience
10 as the chief of staffs and time at the -- at FinCEN? Would you split some of that? Is
11 that why she was on these emails and you weren't?

12 A I don't remember anything quite that formal, but it sort of seems organically
13 that is how it worked out, you know, at least here.

14 Again, my -- our respective backgrounds and experiences were fairly different,
15 which actually, I think, is a good thing in a management team. And so -- but I don't
16 remember anything, kind of, this formal as what you're suggesting.

17 BY [REDACTED]

18 Q So were there ever any conversations about the division of labor, who was
19 going to handle what work stream?

20 A Again, I don't recall anything quite that specific. You know, [REDACTED] had been
21 in the front office as chief of staff prior to this role and had an excellent relationship with
22 leadership. So there's nothing about leadership dealing directly with her that would
23 have struck me as kind of unusual or odd.

24 I think very highly of [REDACTED]. So she -- nothing about that would have stood out to
25 me as something I needed to be worried about.

1 Q Were you both responsible for the post-January 6th action items, or was she
2 more focused on the post-January 6th investigations, and you were getting your --

3 A As a practical matter, she was more involved both, I think, by -- but, again,
4 I'm the manager of this, so I kind of -- I don't want to be -- I want to be clear about that.

5 But, you know, I think it just -- as I said before, I don't think there was anything,
6 sort of, formal in terms of, like, dividing up the role, so to speak. I just think, based on
7 background, experience, prior roles, it just sort of organically developed this way.

8 And this was a relatively short period of time that is my understanding that these
9 exchange -- you know, exchanges of information and the, sort of, corresponding FinCEN
10 exchanges were actually going on. So we're talking a matter of a couple weeks, not, sort
11 of, an extended -- you know, everything we're talking about is a, sort of, short period of
12 time.

13 So nothing -- even with the benefit of hindsight, there's -- I don't -- nothing strikes
14 me as, sort of, like, unusual about people going directly to [REDACTED] on anything.

15

BY [REDACTED]

16 Q Moving to, I think it's Exhibit 7 --

17 A I just had that one, didn't I? Yeah.

18 Q It's Bates stamped 662.

19 A Wait. Oh, the emails inside that. Okay.

20 Q Yes.

21 A Oh, wait.

22 [REDACTED] It's two emails together. It's one exhibit.

23 Mr. Kirby. Okay. I'm there.

24

BY [REDACTED]

25 Q Just wanted to direct your attention to the top email. That was sent on

1 Friday, January 22nd, 2021. That would have been post-inauguration.

2 A Uh-huh.

3 Q Do you have any idea why the transportation vendor list was being shared
4 after the fact?

5 A I don't recall discussing this at the time. But, you know, I am aware that
6 since the events of January 6th there's been a substantial amount of law enforcement,
7 you know, activity in connection with prosecutions and other, you know, activity of that
8 type.

9 So given that, you know, my understanding is that a lot of the work done at this
10 time was done in coordination with law enforcement, it wouldn't necessarily -- to the
11 extent law enforcement folks are identifying suspects involved in the initial event on
12 January 6th, it wouldn't necessarily surprise me if they continued to, sort of, engage in
13 information exchange related to that.

14 And, you know, weaving down the chain a little bit more, you know, it looks like
15 [REDACTED] also shared, like, a Pacer link to defendants that had been charged, which would,
16 again, sort of be consistent with at least some of the focus at this time being in terms of,
17 sort of, supporting law enforcement efforts with regard to folks who had been actually
18 charged as having, you know, allegedly engaged in criminal activity.

19 [REDACTED] But this was no longer about identifying potential threats to
20 inauguration? This was now supporting law enforcement in their investigations of
21 January 6th. Is that fair to say?

22 Mr. Kirby. I mean, I guess that would sort of make -- I'm not sure it was always
23 just one even at the beginning. I mean, I think there were -- I mean, I don't know this.
24 I'd have to go back and check. But I suspect there were people arrested prior to the
25 inauguration for their activity on that day.

1 So I would imagine there was a fair amount of overlap in those work streams until
2 the inauguration part of it was, sort, of safely squared away. So I don't know that it was
3 just one and then the other. I would imagine it may well have been both and very much
4 then transitioned into this, sort of, pretty much law enforcement in the response to as
5 opposed to the protection of, to your point.

6 ██████████ We can go off the record.

7 [Whereupon, at 4:00 p.m., the interview was concluded.]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Certificate of Deponent/Interviewee

I have read the foregoing ____ pages, which contain the correct transcript of the answers made by me to the questions therein recorded.

Witness Name

Date

From: [REDACTED]
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Briefing follow up
Date: Wednesday, May 29, 2024 10:47:41 AM

[REDACTED] – as requested, the following agencies have AIA access: CBP, FBI, ICE, IRS, NCTC, NSA, OCDETF, USSS. As I previously stated, we consider this information to be sensitive and would expect the Committee to treat it confidentially.

[REDACTED]
Office of the Director
Financial Crimes Enforcement Network
[REDACTED]

-----Original Message-----

From: [REDACTED]@mail.house.gov>
Sent: Tuesday, May 28, 2024 10:18 AM
To: [REDACTED]@fincen.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov>
Subject: [EXTERNAL]RE: Briefing follow up

Good morning [REDACTED],

Checking in here, thanks!

[REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: Monday, May 20, 2024 12:50 PM
To: [REDACTED]@fincen.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov>
Subject: RE: Briefing follow up

Good morning [REDACTED],

Checking in here. Thank you!

[REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: Monday, May 13, 2024 4:52 PM
To: [REDACTED]@fincen.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov>
Subject: RE: Briefing follow up

Thanks [REDACTED] for getting back to me. With respect to the eight that are law enforcement sensitive, are you able to transmit those in an unclassified setting? I will reach back out later this week with the best arrangement for us to review the classified material.

[REDACTED]

-----Original Message-----

From: [REDACTED]@fincen.gov>
Sent: Friday, May 10, 2024 11:10 AM
To: [REDACTED]@mail.house.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov
Subject: RE: Briefing follow up

[REDACTED] -

Following up on this.

Of the 9 agencies that have AIA access with FinCEN, 1 is classified and we would consider the other 8 law enforcement sensitive information. Accordingly, we can transmit the list on the high side. Could you provide a classified email address, or should we arrange to have the email printed for you by House Security?

Thanks.

[REDACTED]
Office of the Director
Financial Crimes Enforcement Network
[REDACTED]

-----Original Message-----

From: [REDACTED]@mail.house.gov>
Sent: Thursday, May 2, 2024 2:59 PM
To: [REDACTED]@fincen.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov
Subject: [EXTERNAL]RE: Briefing follow up

Thanks, [REDACTED]. Yes, this is very helpful. What nine federal law enforcement and national security agencies are those?

[REDACTED]

-----Original Message-----

From: [REDACTED]@fincen.gov>
Sent: Thursday, May 2, 2024 2:44 PM
To: [REDACTED]@mail.house.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov
Subject: RE: Briefing follow up

[REDACTED] -

Currently, FinCEN shares BSA data with nine federal law enforcement and national security agencies. The agencies with integrated access work with FinCEN to establish internal controls for how they store, access, and use BSA data in their systems. Those agencies integrate BSA data into their existing systems and manage access to those systems – including which authorized users have access to BSA data. Because the agencies manage these user accounts, FinCEN does not have an exact contemporaneous count of the number of users. However, as of September 2023, there were approximately 27,000 authorized agency users who had access to BSA data through AIA agencies. We note that many of those users may also have access to BSA data through FinCEN Query.

Hope this is helpful.

[REDACTED]

[REDACTED]
Office of the Director
Financial Crimes Enforcement Network
[REDACTED]

-----Original Message-----

From: [REDACTED]@mail.house.gov>
Sent: Monday, April 29, 2024 12:37 PM
To: [REDACTED]@fincen.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov
Subject: [EXTERNAL]RE: Briefing follow up

Thanks [REDACTED], this is helpful. However, we would still like to know how many individuals have access pursuant to AIA. Additionally, we would also like to know how many, and which agencies have MOUs with FinCEN. Does FinCEN have any oversight of the use of BSA data once the agency imports the data onto their own systems?

[REDACTED]
[REDACTED]
Committee on the Judiciary
U.S. House of Representatives

-----Original Message-----

From: [REDACTED]@fincen.gov>
Sent: Thursday, April 25, 2024 5:03 PM
To: [REDACTED]@mail.house.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov
Subject: Re: Briefing follow up

Here you go, sorry about the delay.

For a limited number of federal law enforcement and national security agencies, FinCEN has entered into "Agency Integrated Access" Memoranda of Understanding that permit those agencies to import BSA data onto their own systems and integrate it into their own secure databases rather than search BSA information in FinCEN Query. The goal of AIA is to increase the recipient agency's ability to use BSA Information by allowing the agency to utilize its own analytic tools. The agencies with AIA MOUs manage user access for the relevant agency database(s) directly, consistent with the terms of their MOU with FinCEN and the BSA. The authorized users who access BSA data through an agency with an AIA MOU are in addition to the users who have access to BSA data through FinCEN Query.

From: [REDACTED]@mail.house.gov>
Sent: Thursday, April 25, 2024 12:41:55 PM
To: [REDACTED]@fincen.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov>; [REDACTED]@treasury.gov
Subject: [EXTERNAL]RE: Briefing follow up

[REDACTED]

Checking in here again. Thanks!

[REDACTED]

From: [REDACTED]@fincen.gov>
Sent: Friday, April 19, 2024 9:29 AM
To: [REDACTED]@mail.house.gov>; [REDACTED]@mail.house.gov>
Cc: [REDACTED]@mail.house.gov> [REDACTED]@treasury.gov
Subject: RE: Briefing follow up

[REDACTED]

I just tried you at the Committee office but only get voicemail.

Feel free to give me a call [REDACTED]

[REDACTED]

[REDACTED]

Office of the Director

Financial Crimes Enforcement Network

[REDACTED]

[fincen]

From: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>
Sent: Friday, April 19, 2024 9:23 AM
To: [REDACTED]@fincen.gov<[REDACTED]>>; [REDACTED]
[REDACTED]@mail.house.gov<[REDACTED]@mail.house.gov>>
Cc: [REDACTED]@treasury.gov<[REDACTED]@treasury.gov>>; [REDACTED]@mail.house.gov<[REDACTED]@mail.house.gov>>; [REDACTED]@treasury.gov<[REDACTED]@treasury.gov>>
Subject: [EXTERNAL]RE: Briefing follow up

[REDACTED]

Following up here. Thanks.

[REDACTED]

[REDACTED]

[REDACTED]

Committee on the Judiciary

U.S. House of Representatives

[REDACTED]

From: [REDACTED]
 Sent: Wednesday, April 10, 2024 11:56 AM
 To: [REDACTED]@fincen.gov<[REDACTED]@fincen.gov>>; [REDACTED]
 [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>
 Cc: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>;
 [REDACTED]@treasury.gov [REDACTED]@treasury.gov>
 Subject: RE: Briefing follow up

Thanks [REDACTED]. Can you clarify what Agency Integrated Access is? How many individuals have access pursuant to AIA? Is that in addition to the users 14,415 users that have registered access to the BSA database?

Best,

[REDACTED]

[REDACTED]

Committee on the Judiciary

U.S. House of Representatives

[REDACTED]

From: [REDACTED]@fincen.gov [REDACTED]@fincen.gov>>
 Sent: Monday, April 8, 2024 10:48 AM
 To: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>
 Cc: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>; [REDACTED]
 [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>;
 [REDACTED]@treasury.gov [REDACTED]@treasury.gov>

Subject: RE: Briefing follow up

Sorry for the delay on this. Answers embedded below your original questions in red.

Let us know if you need anything else.

[REDACTED]

[REDACTED]

Office of the Director

Financial Crimes Enforcement Network

[REDACTED]

[fincen]

From: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>

Sent: Monday, April 1, 2024 9:42 AM

To: [REDACTED]@fincen.gov [REDACTED]@fincen.gov>>

Cc: [REDACTED]@mail.house [REDACTED]@mail.house.gov>>; [REDACTED]

[REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>

Subject: [EXTERNAL]Re: Briefing follow up

Hope you had a good Easter weekend. Wanted to circle back on this before the week got away from me.

Thank you,

[REDACTED]

[REDACTED]

On Mar 19, 2024, at 2:52 PM, [REDACTED]@fincen.gov<[REDACTED]@fincen.gov>> wrote:

[REDACTED]

We actually just had an internal follow up discussion on these this morning. Working to get answers out the door to you soon.

[REDACTED]

[REDACTED]

Office of the Director

Financial Crimes Enforcement Network

[REDACTED]

<image001.jpg>

From: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>

Sent: Tuesday, March 19, 2024 2:50 PM

To: [REDACTED]@fincen.gov [REDACTED]@fincen.gov>>

Cc: [REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>; [REDACTED]

[REDACTED]@mail.house.gov [REDACTED]@mail.house.gov>>

Subject: [EXTERNAL]Briefing follow up

[REDACTED] wanted to touch base about two questions that FinCEN was going to follow up on

1) how many people have access to the BSA database (Mr. Kirby suggested ~15k people. Does this track?

In FY23, there were an average of 14,415 authorized registered to access the BSA database through FinCEN Query, in addition to authorized users who have access through Agency Integrated Access (AIA).

2) how many searches of the BSA database were conducted in 2023?

In FY23, there were 3,362,735 million BSA searches conducted in FinCEN Query.

3) what are the minimum qualifications for a 314(a) search. Could it be all purchase in a general area or does it HAVE to obtain name/DOB/etc?

FinCEN does not process 314(a) requests based solely on geographical data. When FinCEN receives a 314(a) request, it ensures that the request includes sufficient specific identifiers, such as date of birth, address, and social security number, that would permit a financial institution to differentiate between common or similar names. If

FinCEN received a request that contained no identifiers and only included a geographic location alone, it would not process the request. The request would lack sufficient information to allow the receiving banks to identify any relevant accounts or activity.

Thank you,

[REDACTED]

[REDACTED]



SAR Command

Battle Plans to Safely and Effectively Curb
Excessive Filing Volumes

Moderator:

[REDACTED], Senior Vice President, BSA Executive Director,
Wintrust Financial Corporation

Panelists:

[REDACTED] Deputy Director of Financial Crime, Senior Vice President,
Truist Financial Corporation

[REDACTED], Financial Crimes Strategic Intelligence Director, Wells Fargo

[REDACTED], Head of Strategy & Marketing, AML, NICE Actimize

Polling Question #1

What industry are you from?

- 1) Bank, Credit Union, Financial Institution
- 2) Fintech
- 3) Money Service Business
- 4) Securities/Futures
- 5) Gaming
- 6) Regulator
- 7) Law Enforcement
- 8) Consultant

Why Does “Effectiveness” Matter?

- BSA program requirement but no agreement on program goals
- FinCEN proposed definition in September, similar to Wolfsberg 2019 proposal
 - Assesses and manages risk as informed by a financial institution’s own risk assessment process, including consideration of national AML priorities
 - Provides for compliance with BSA requirements
 - Provides highly useful information to government authorities
- How does this relate to SAR volumes?

Polling Question #2

How much have annual SAR filings increased since 2014 (thru 2022)?

- 1) 18%
- 2) 58%
- 3) 88%
- 4) 118%
- 5) 148%

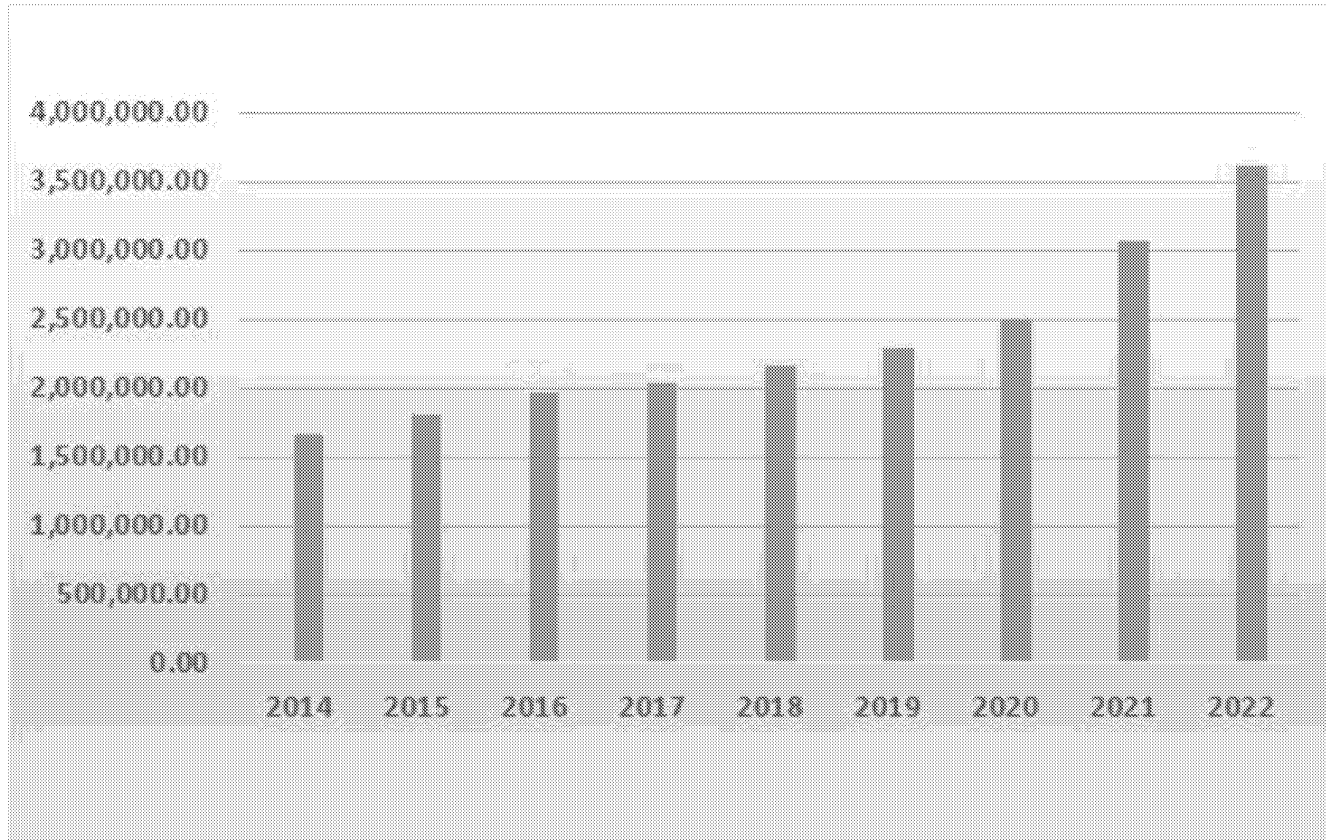
The need to change how we file SAR's

- Increasing SAR numbers
- Increasing financial crime proceeds
- Limited success of law enforcement

SARs need to inform law enforcement, not just tick a box

- What does law enforcement need to know
 - 5WH (Who, What, Where, When, Why and How!)
- How do we as FIs get that information?
- What does law enforcement need our help with?
- A decision needs to be made, do law enforcement want to know everything or do they want intelligent SARs?

Annual SAR Filings Increased by 118% since 2014



What needs to happen to lead to better SAR's?

- Technology improvements
- Enhanced data
- Better understanding of customers
- Collective approach (information sharing)
 - Especially feedback from regulatory authorities and law enforcement
 - Super SARs
- Change in expectations and a reduction in 'defensive filing' – this should come with a better intelligence-led approach

Reducing Repeat Filings

- 314(b) requests
- Conducting additional research and analysis
- Obtaining rationale for activity
- Recommended corrective actions taken
- Link to broader business policy change
- Exiting relationship

Takeaways

- Could file less SARs and be just as, if not more, effective [REDACTED]
- Automation opportunities for less complex issues [REDACTED]
- Lean into a regime focused on outcomes, redeploy resources to higher risk/value activities [REDACTED]
- There needs to be greater collaboration between private and public sector for more effective and intelligent SARs ([REDACTED])
- Technology can play a key role in increasing SAR value by improving the SAR information quality ([REDACTED])
- Understand your institution's risk appetite – How to avoid over filing, while accepting you may be leaving SARs on the table [REDACTED]



Thank You

Dear panelists,

Your planning call will take place on **Friday, February 24th at 12 PM EST**

**Tuesday, May 9, 2023
Main Conference Day One**

4:10 PM – 5:10 PM

SARs

SAR Command: Battle Plans to Safely and Effectively Curb Excessive Filing Volumes

To paraphrase a saying about the weather, everybody complains about high SAR volumes, but nobody does anything about it. Maybe it's time — beginning with this lively, thought-provoking and interactive panel. Led by seasoned compliance veterans, the forum-style session will debate and rate your questions and suggestions on safely reducing filing volumes. Whether it's exiting SAR-heavy accounts, reducing "defensive SARs" through stronger KYC or maybe just chatting with examiners, bring your theories and queries on changing, if not the weather, the current climate of escalating SAR filing volumes.

Moderator:

██████████ CAMS, Senior Vice President, BSA Executive Director, **Wintrust Financial Corporation**

Presenters:

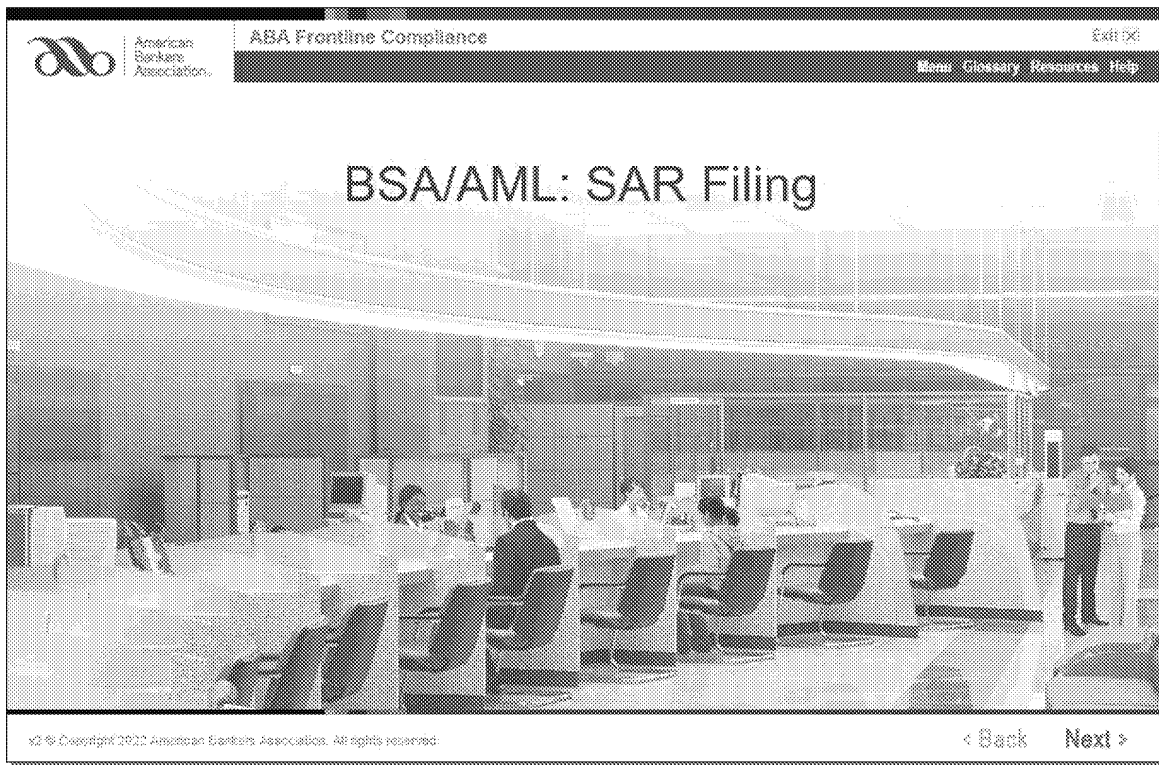
██████████ Deputy Director of Financial Crime, Senior Vice President, **Truist Financial Corp.**

██████████ Regional Head of Risk Assessment, **HSBC**

██████████ Head of Strategy & Marketing, AML, **NICE Actimize**

Session Planning Call Agenda:

- Discuss Content Focus (see description above)
- Establish Speaker Order/Session Format (discussion vs. individual presentations)
- Moderator to review Presentation Guidelines / Identify 4 Key Takeaways (PPT due April 3rd)
- Schedule follow up call, if needed



BSA/AML: SAR Filing

ABA course content is not a substitute for professional legal advice.



Menu

Introduction

Suspicious Activity Reports (SARs)

SAR Confidentiality

Five Key Components

Identifying the Suspicious Activity

Managing Alerts

Decision-Making

Completion and Filing

Monitoring and SAR Filing on Continuing Activity

Wrap-Up

The screenshot shows a web browser window displaying the ABA course page for "BSA/AML: SAR Filing". The page features the American Bankers Association logo in the top left, the course title in the top center, and navigation links (Menu, Home, Resources, Help) in the top right. The main content area includes an introductory paragraph, version and update information, a note about the Anti-Money Laundering Act of 2020, a photograph of a man in a suit, and a disclaimer box stating "ABA course content is not a substitute for professional legal advice." The footer contains copyright information, page number (Page 1 of 53), and navigation arrows.

Introduction

This course describes the Bank Secrecy Act (BSA) requirements surrounding the filing of Suspicious Activity Reports (SARs) and why federal law limits sharing information about SARs. It covers the components of SAR monitoring and reporting systems and how to answer the essential questions that comprise the basis of SAR narratives.

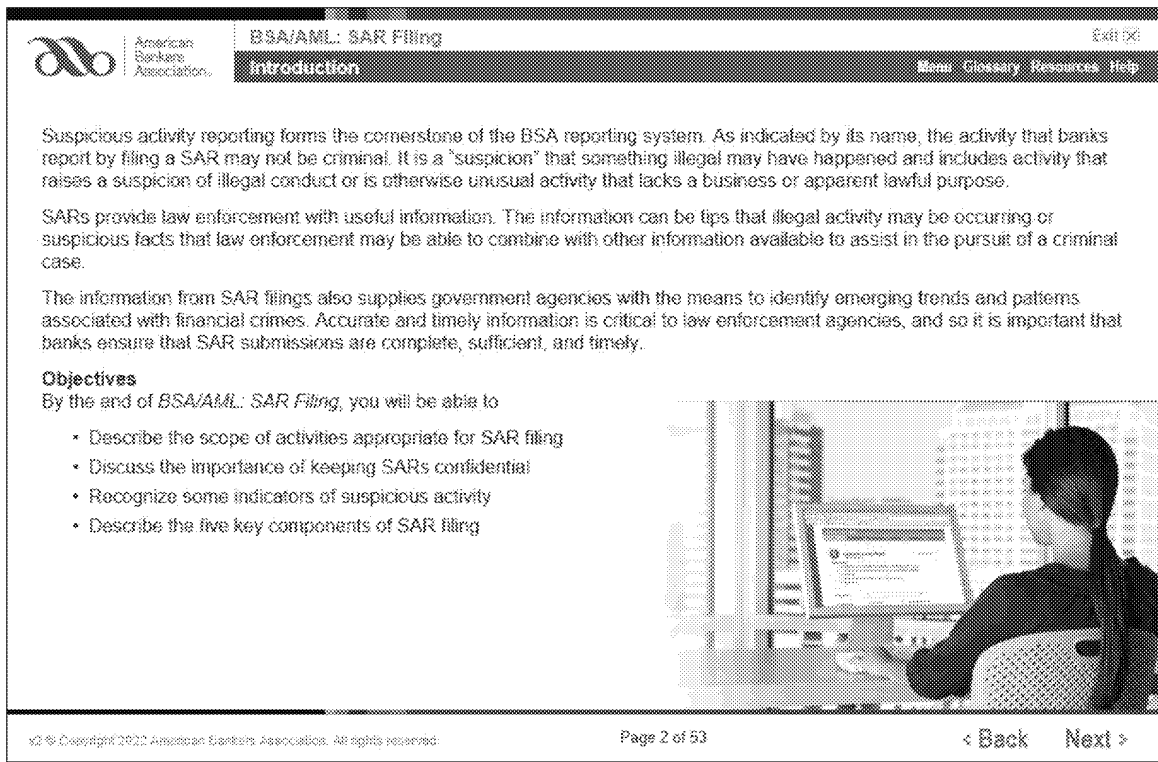
Version: 2.0

Update: July 2022. Added the Office of the Comptroller of the Currency's (OCC's) final rule on exemptions to SAR requirements.

Note: The Anti-Money Laundering Act of 2020 contains provisions to update and streamline SAR reporting. The Financial Crimes Enforcement Network (FinCEN) has not yet acted on these provisions.

Banks are required to report certain suspicious activities. Banks are also encouraged to report other possibly suspicious transactions that may be relevant to a possible violation of law or regulation. Suspicious transactions are those seemingly intended to launder money or finance terrorist activities or are connected to criminal activity. A suspicious transaction may also be one that apparently has no lawful purpose or is extremely unusual for a particular customer and has no reasonable explanation.

ABA course content is not a substitute for professional legal advice.



Suspicious activity reporting forms the cornerstone of the BSA reporting system. As indicated by its name, the activity that banks report by filing a SAR may not be criminal. It is a "suspicion" that something illegal may have happened and includes activity that raises a suspicion of illegal conduct or is otherwise unusual activity that lacks a business or apparent lawful purpose.

SARs provide law enforcement with useful information. The information can be tips that illegal activity may be occurring or suspicious facts that law enforcement may be able to combine with other information available to assist in the pursuit of a criminal case.

The information from SAR filings also supplies government agencies with the means to identify emerging trends and patterns associated with financial crimes. Accurate and timely information is critical to law enforcement agencies, and so it is important that banks ensure that SAR submissions are complete, sufficient, and timely.

Objectives
By the end of *BSA/AML: SAR Filing*, you will be able to

- Describe the scope of activities appropriate for SAR filing
- Discuss the importance of keeping SARs confidential
- Recognize some indicators of suspicious activity
- Describe the five key components of SAR filing

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 2 of 53 < Back Next >

Introduction

Suspicious activity reporting forms the cornerstone of the BSA reporting system. As indicated by its name, the activity that banks report by filing a SAR may not be criminal. It is a "suspicion" that something illegal may have happened or may be happening and includes activity that raises a suspicion of illegal conduct or is otherwise unusual activity that lacks a business or apparent lawful purpose.


SARs provide law enforcement with useful information. The information can be tips that illegal activity may be occurring or suspicious facts that law enforcement may be able to combine with other information available to assist in the pursuit of a criminal case.

The information from SAR filings also supplies government agencies with the means to identify emerging trends and patterns associated with financial crimes. Accurate and timely information is critical to law enforcement agencies, and so it is important that banks ensure that SAR submissions are complete, sufficient, and timely.

Objectives

By the end of *BSA/AML: SAR Filing*, you will be able to

- Describe the scope of activities appropriate for SAR filing
- Discuss the importance of keeping SARs confidential
- Recognize some indicators of suspicious activity
- Describe the five key components of SAR filing



BSA/AML: SAR Filing

Suspicious Activity Reports (SARs)

Exit DC

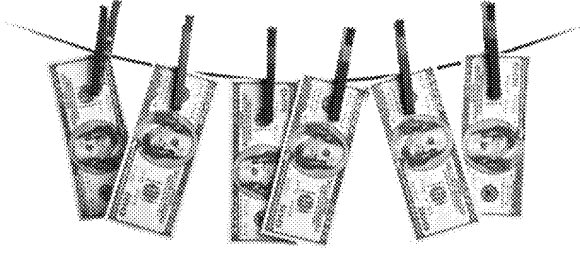
Home Glossary Resources Help

Money laundering

Banks are targets of money laundering efforts because they provide ready access to the payment system and afford potential cover due to the large volume of daily transactions occurring at any given bank. Because of the large volumes of daily transactions, individuals involved in money laundering may believe their laundering efforts will go undetected.

Federal investigators who try to stop money laundering find it a never-ending process. After they discover criminals' latest money laundering schemes, the criminals respond by creating even more inventive and complicated methods to launder money. These methods range from smuggling funds to the creation of intricate networks using wire transfers and shell companies.

Because the banking industry is also complicated and in a constant state of change, law enforcement officials and bankers face a huge challenge identifying and investigating money laundering. The process of tracking the money is tedious and lengthy because investigators are dealing with the continuous changes and complexities of new money laundering schemes.



© 2022 American Bankers Association. All rights reserved.

Page 3 of 53

< Back Next >

Suspicious Activity Reports (SARs)

Money laundering

Banks are targets of money laundering efforts because they provide ready access to the payment system and afford potential cover due to the large volume of daily transactions occurring at any given bank. Because of the large volumes of daily transactions, individuals involved in money laundering may believe their laundering efforts will go undetected.

Federal investigators who try to stop money laundering find it a never-ending process. After they discover criminals' latest money laundering schemes, the criminals respond by creating even more inventive and complicated methods to launder money. These methods range from smuggling funds to the creation of intricate networks using wire transfers and shell companies.

Because the banking industry is also complicated and in a constant state of change, law enforcement officials and bankers face a huge challenge identifying and investigating money laundering. The process of tracking the money is tedious and lengthy because investigators are dealing with the continuous changes and complexities of new money laundering schemes.

Glossary term:

Shell companies

The term "shell company" generally refers to a business entity with no significant assets or ongoing business activities. Shell companies—formed for both legitimate and illicit purposes—typically have no physical presence other than a mailing address, have no employees, and have little to no independent economic value. Shell companies often can be used in money laundering operations.

Page 3

The screenshot shows the American Bankers Association website page for BSA/AML: SAR Filing. The page title is "BSA/AML: SAR Filing" and the sub-header is "Suspicious Activity Reports (SARs)". The main content area contains the following text:

Bank employees who encounter suspicious transactions that may relate to terrorist activity must notify the appropriate person at their bank immediately.

In September 2001, immediately following the terrorist attacks on the World Trade Center in New York and the Pentagon in Washington, DC, FinCEN established a FINANCIAL INSTITUTIONS HOTLINE that operates 7 days a week, 24 hours a day, to facilitate the immediate transmittal of this information to law enforcement when such information appears to relate to terrorism. This HOTLINE provides law enforcement and other authorized recipients of SAR information with details of the suspicious activity in an expedited fashion.

Using the HOTLINE is voluntary and is not a substitute for a bank's responsibility to file a SAR in accordance with applicable BSA regulations.

Below the text is a screenshot of the FinCEN Financial Institutions Hotline website. The FinCEN logo is prominent, and the text reads "FINANCIAL INSTITUTIONS HOTLINE Relating to Terrorist Activity".

The footer of the page includes the copyright notice: "© 2012 Copyright 2012 American Bankers Association. All rights reserved." and page navigation: "Page 4 of 53" with "< Back" and "Next >" links.

Suspicious Activity Reports (SARs)

Bank employees who encounter suspicious transactions that may relate to terrorist activity must notify the appropriate person at their bank immediately.

In September 2001, immediately following the terrorist attacks on the World Trade Center in New York and the Pentagon in Washington, DC, FinCEN established a FINANCIAL INSTITUTIONS HOTLINE that operates 7 days a week, 24 hours a day, to facilitate the immediate transmittal of this information to law enforcement when such information appears to relate to terrorism. This HOTLINE provides law enforcement and other authorized recipients of SAR information with details of the suspicious activity in an expedited fashion.

Using the HOTLINE is voluntary and is not a substitute for a bank's responsibility to file a SAR in accordance with applicable BSA regulations.

The screenshot shows a webpage with the following content:

- Header:** American Bankers Association logo, "BSA/AML: SAR Filing", "Suspicious Activity Reports (SARs)", and navigation links (Home, Glossary, Resources, Help).
- Main Text:** "Federal regulations require banks to file a completed SAR by sending the report to FinCEN in the following circumstances:"
 - Insider abuse of any amount
 - A total of \$5,000 or more where a suspect can be identified
 - A total of \$25,000 or more regardless of potential suspects
- Additional Text:** "In addition, a bank must file a SAR on transactions conducted or attempted that total \$5,000 or more if the bank suspects or has reason to suspect that the conduct displays the following characteristics:"
 - Involves possible money laundering or illegal activity
 - Is designed to evade BSA requirements
 - Has no business or apparent lawful purpose or is not the type of transaction in which the customer would ordinarily engage
- Note:** A bank is not required to file a SAR for a robbery or burglary that it reports to appropriate law enforcement officials.
- Image:** A man in a suit sitting at a desk with a laptop, with a thought bubble saying "Do I need to file out a SAR for this transaction?".
- Footer:** Copyright 2022 American Bankers Association, Page 5 of 53, and navigation buttons "< Back" and "Next >".

Suspicious Activity Reports (SARs)

Federal regulations require banks to file a completed SAR by sending the report to FinCEN in the following circumstances:

- Insider abuse of any amount
- A total of \$5,000 or more where a suspect can be identified
- A total of \$25,000 or more regardless of potential suspects

In addition, a bank must file a SAR on transactions conducted or attempted that total \$5,000 or more if the bank suspects or has reason to suspect that the conduct displays the following characteristics:

- Involves possible money laundering or illegal activity
- Is designed to evade BSA requirements
- Has no business or apparent lawful purpose or is not the type of transaction in which the customer would ordinarily engage

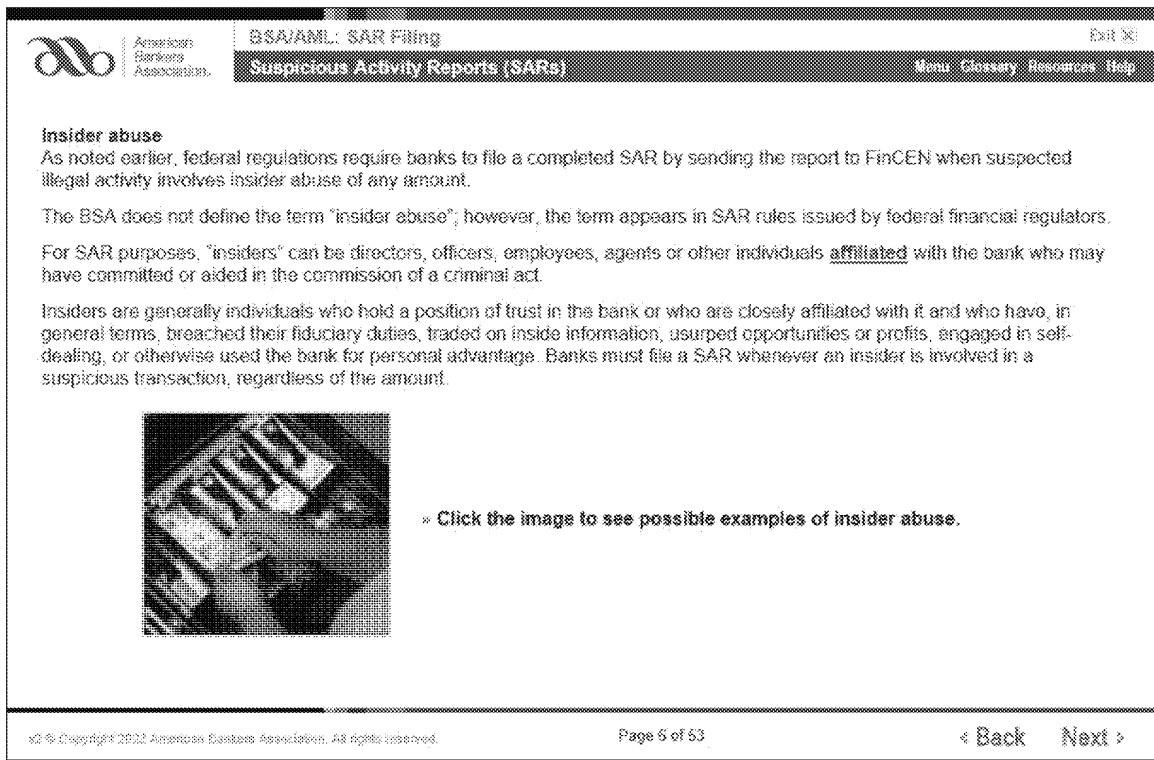
Note: A bank is not required to file a SAR for a robbery or burglary that it reports to appropriate law enforcement officials.

Sidebar:

Bank filing

The decision to file a SAR is inherently subjective. Examiners focus on whether a bank has an effective SAR decision-making process, not individual SAR decisions. Regulatory examinations and third-party audit procedures may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process; however, in those instances where a bank has an established SAR decision-making process; has followed existing policies, procedures, and processes; and has determined not to file a SAR; it should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

Page 5

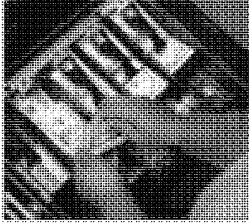


Insider abuse
As noted earlier, federal regulations require banks to file a completed SAR by sending the report to FinCEN when suspected illegal activity involves insider abuse of any amount.

The BSA does not define the term "insider abuse"; however, the term appears in SAR rules issued by federal financial regulators.

For SAR purposes, "insiders" can be directors, officers, employees, agents or other individuals affiliated with the bank who may have committed or aided in the commission of a criminal act.

Insiders are generally individuals who hold a position of trust in the bank or who are closely affiliated with it and who have, in general terms, breached their fiduciary duties, traded on inside information, usurped opportunities or profits, engaged in self-dealing, or otherwise used the bank for personal advantage. Banks must file a SAR whenever an insider is involved in a suspicious transaction, regardless of the amount.

 » Click the image to see possible examples of insider abuse.

© 7/2022 American Bankers Association. All rights reserved. Page 6 of 53 < Back Next >

Suspicious Activity Reports (SARs)

Insider abuse

As noted earlier, federal regulations require banks to file a completed SAR by sending the report to FinCEN when suspected illegal activity involves insider abuse of any amount.

The BSA does not define the term "insider abuse"; however, the term appears in SAR rules issued by federal financial regulators.

For SAR purposes, "insiders" can be directors, officers, employees, agents, or other individuals affiliated with the bank who may have committed or aided in the commission of a criminal act.

Insiders are generally individuals who hold a position of trust in the bank or who are closely affiliated with it and who have, in general terms, breached their fiduciary duties, traded on inside information, usurped opportunities or profits, engaged in self-dealing, or otherwise used the bank for personal advantage. Banks must file a SAR whenever an insider is involved in a suspicious transaction, regardless of the amount.

» Click the image to see possible examples of insider abuse.

Possible examples of insider abuse may include the following actions:

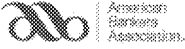
- Use bank funds for personal vacations or to buy personal automobiles, clothing, and art
- Pay consulting fees to insiders or their companies
- Put friends and relatives on the bank's payroll
- Steal money from a teller's cash drawer or vault, often followed by forced balancing
- Open new accounts for fraudulent or nonexistent customers to qualify for performance goals or employee incentive programs
- Improperly credit overdraft fees and other service charges to themselves and others

Glossary term:

Institution-affiliated party

An institution-affiliated party is any director, officer, employee, controlling stockholder (other than a bank holding company [BHC]), agent, shareholder, or independent contractor (including an attorney, appraiser, or accountant) who knowingly or recklessly participates in the conduct of the affairs of an insured depository institution.

Page 6



BSA/AML: SAR Filing

Suspicious Activity Reports (SARs)

Exit

Home | Contact | Resources | Help

Identified suspects

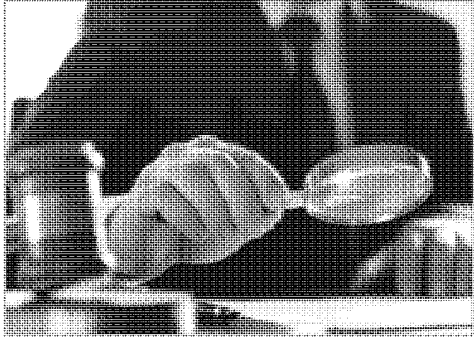
Federal regulations require banks to file a completed SAR by sending the report to FinCEN. Banks are required to file SARs when the dollar amount of the suspicious activity aggregates to \$5,000 or more where a suspect can be identified. This threshold applies when the bank knows the suspect or is able to identify the suspect, even if that person is not a customer of the bank.

Unidentified suspects

Banks must file a SAR when the suspicious activity involves amounts of \$25,000 or more regardless of potential suspects. This might happen in instances where transactors are noncustomers, when there are multiple transactions across the bank's branch network, or where the activity involves use of ATMs or night depositories.

It is recognized that with respect to instances of possible terrorism, identity theft, and computer intrusion, the dollar thresholds for filing may not always be met. Banks are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce.

Even when the dollar thresholds of the SAR regulations are not met, banks have the discretion to file a SAR and are protected by the statute when doing so.



© 2022 American Bankers Association. All rights reserved.

Page 7 of 53

< Back Next >

Suspicious Activity Reports (SARs)

Identified suspects

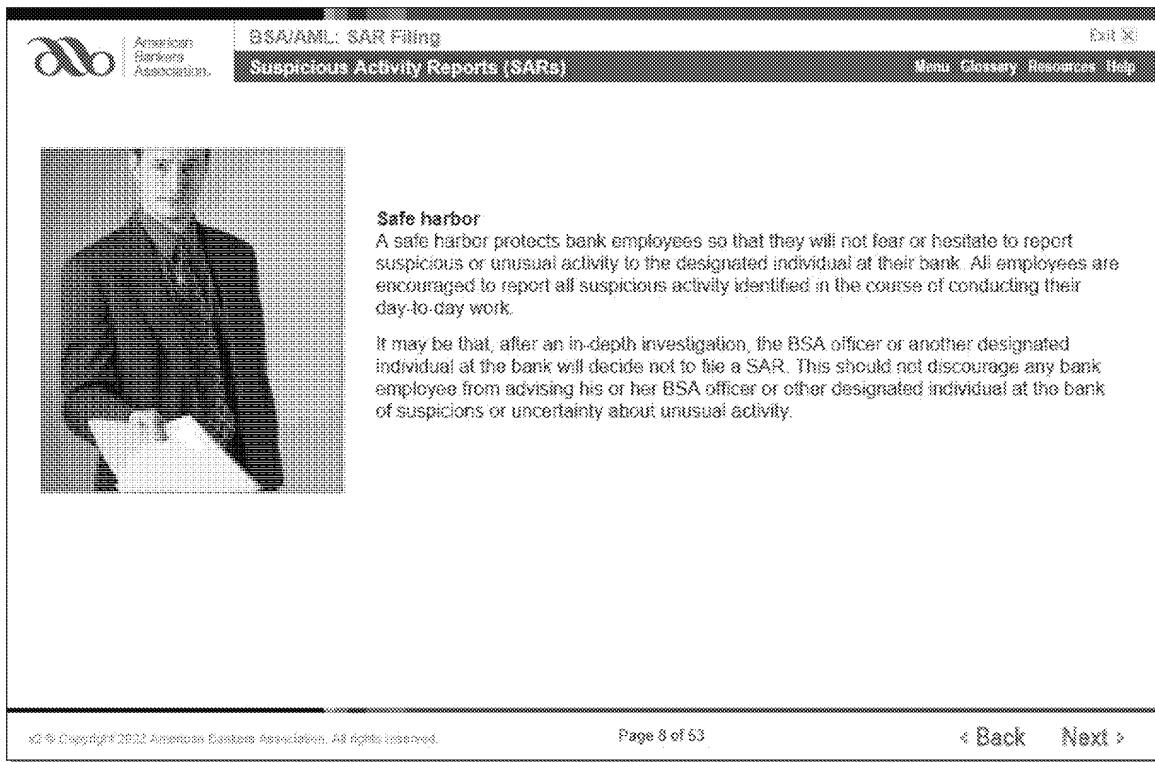
Federal regulations require banks to file a completed SAR by sending the report to FinCEN. Banks are required to file SARs when the dollar amount of the suspicious activity aggregates to \$5,000 or more where a suspect can be identified. This threshold applies when the bank knows the suspect or is able to identify the suspect, even if that person is not a customer of the bank.

Unidentified suspects

Banks must file a SAR when the suspicious activity involves amounts of \$25,000 or more regardless of potential suspects. This might happen in instances where transactors are noncustomers, when there are multiple transactions across the bank's branch network, or where the activity involves use of ATMs or night depositories.

It is recognized that with respect to instances of possible terrorism, identity theft, and computer intrusion, the dollar thresholds for filing may not always be met. Banks are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce.

Even when the dollar thresholds of the SAR regulations are not met, banks have the discretion to file a SAR and are protected by the statute when doing so.



BSA/AML: SAR Filing
Suspicious Activity Reports (SARs)

Safe harbor
 A safe harbor protects bank employees so that they will not fear or hesitate to report suspicious or unusual activity to the designated individual at their bank. All employees are encouraged to report all suspicious activity identified in the course of conducting their day-to-day work.

It may be that, after an in-depth investigation, the BSA officer or another designated individual at the bank will decide not to file a SAR. This should not discourage any bank employee from advising his or her BSA officer or other designated individual at the bank of suspicions or uncertainty about unusual activity.

© 7/2022 American Bankers Association. All rights reserved. Page 8 of 53 < Back Next >

Suspicious Activity Reports (SARs)

Safe harbor

A safe harbor protects bank employees so that they will not fear or hesitate to report suspicious or unusual activity to the designated individual at their bank. All employees are encouraged to report all suspicious activity identified in the course of conducting their day-to-day work.

It may be that, after an in-depth investigation, the BSA officer or another designated individual at the bank will decide not to file a SAR. This should not discourage any bank employee from advising his or her BSA officer or other designated individual at the bank of suspicions or uncertainty about unusual activity.

Page 8

BSA/AML: SAR Filing
Suspicious Activity Reports (SARs)

Persons involved in money laundering or other types of financial crime are often aware of the reporting requirements of the BSA and will try to get around the law whenever possible. It is critical, therefore, for bank employees to know their customers and the type of transactions they normally conduct.

In addition to the required SAR reporting thresholds, a bank can file a SAR anytime regardless of the dollar amount if the bank feels law enforcement could benefit from the information. Any transactions that seem out of place or unusual and cannot be reasonably explained with a legitimate business reason should be reported according to bank policy.

Aside from unexplained suspicious activity that may indicate money laundering, human trafficking or smuggling, or even terrorist financing, the SAR process is also intended to detect and report activity that constitutes more direct types of financial crimes such as credit card fraud, identity theft, check kiting, and insider abuse—just to name a few.

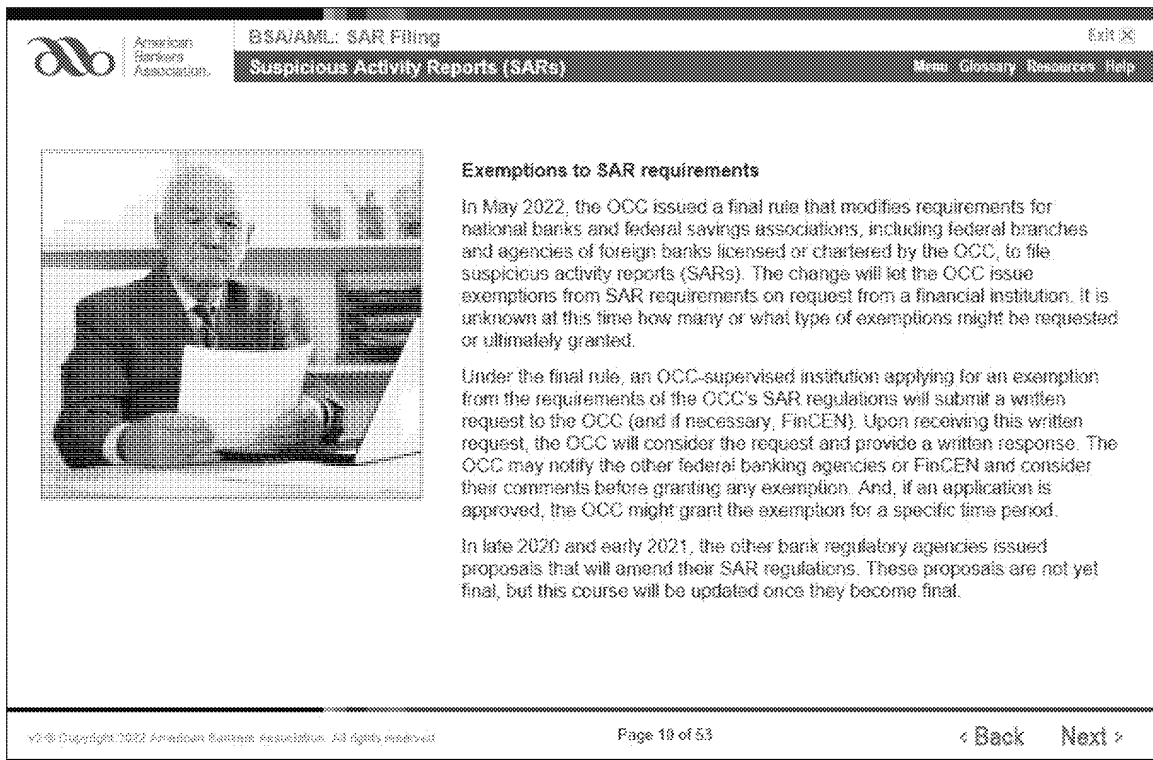
© 7/2022 American Bankers Association. All rights reserved. Page 5 of 53 < Back Next >

Suspicious Activity Reports (SARs)

Persons involved in money laundering or other types of financial crime are often aware of the reporting requirements of the BSA and will try to get around the law whenever possible. It is critical, therefore, for bank employees to know their customers and the type of transactions they normally conduct.

In addition to the required SAR reporting thresholds, a bank can file a SAR anytime regardless of the dollar amount if the bank feels law enforcement could benefit from the information. Any transactions that seem out of place or unusual and cannot be reasonably explained with a legitimate business reason should be reported according to bank policy.

Aside from unexplained suspicious activity that may indicate money laundering, human trafficking or smuggling, or even terrorist financing, the SAR process is also intended to detect and report activity that constitutes more direct types of financial crimes such as credit card fraud, identity theft, check kiting, and insider abuse—just to name a few.



Exemptions to SAR requirements

In May 2022, the OCC issued a final rule that modifies requirements for national banks and federal savings associations, including federal branches and agencies of foreign banks licensed or chartered by the OCC, to file suspicious activity reports (SARs). The change will let the OCC issue exemptions from SAR requirements on request from a financial institution. It is unknown at this time how many or what type of exemptions might be requested or ultimately granted.

Under the final rule, an OCC-supervised institution applying for an exemption from the requirements of the OCC's SAR regulations will submit a written request to the OCC (and if necessary, FinCEN). Upon receiving this written request, the OCC will consider the request and provide a written response. The OCC may notify the other federal banking agencies or FinCEN and consider their comments before granting any exemption. And, if an application is approved, the OCC might grant the exemption for a specific time period.

In late 2020 and early 2021, the other bank regulatory agencies issued proposals that will amend their SAR regulations. These proposals are not yet final, but this course will be updated once they become final.

Page 10 of 53

Suspicious Activity Reports (SARs)

Exemptions to SAR requirements

In May 2022, the OCC issued a final rule that modifies requirements for national banks and federal savings associations, including federal branches and agencies of foreign banks licensed or chartered by the OCC, to file suspicious activity reports (SARs). The change will let the OCC issue exemptions from SAR requirements on request from a financial institution. It is unknown at this time how many or what type of exemptions might be requested or ultimately granted.

Under the final rule, an OCC-supervised institution applying for an exemption from the requirements of the OCC's SAR regulations will submit a written request to the OCC (and if necessary, FinCEN). Upon receiving this written request, the OCC will consider the request and provide a written response. The OCC may notify the other federal banking agencies or FinCEN and consider their comments before granting any exemption. And, if an application is approved, the OCC might grant the exemption for a specific time period.

In late 2020 and early 2021, the other bank regulatory agencies issued proposals that will amend their SAR regulations. These proposals are not yet final, but this course will be updated once they become final.

BSA/AML: SAR Filing
Suspicious Activity Reports (SARs)

Self-Check Quiz

In what circumstances do federal regulations require a bank to file a completed SAR by sending the report to FinCEN?

» Select the correct answers and click Submit.

A) Insider abuse of \$5,000 or more

B) Insider abuse of any amount

C) Suspicious activity totaling \$5,000 or more where a suspect can be identified

D) Suspicious activity totaling \$25,000 or more regardless of potential suspects

© 7/2022 American Bankers Association. All rights reserved. Page 11 of 53 < Back Next >

Suspicious Activity Reports (SARs)

Self-Check Quiz

In what circumstances do federal regulations require a bank to file a completed SAR by sending the report to FinCEN?

» Select the correct answers and click Submit.

- A. Insider abuse of \$5,000 or more
- B. Insider abuse of any amount
- C. Suspicious activity totaling \$5,000 or more where a suspect can be identified
- D. Suspicious activity totaling \$25,000 or more regardless of potential suspects

B, C, and D are correct.

A is incorrect because a bank is required by federal regulations to file a completed SAR for insider abuse of any amount.

Page 11

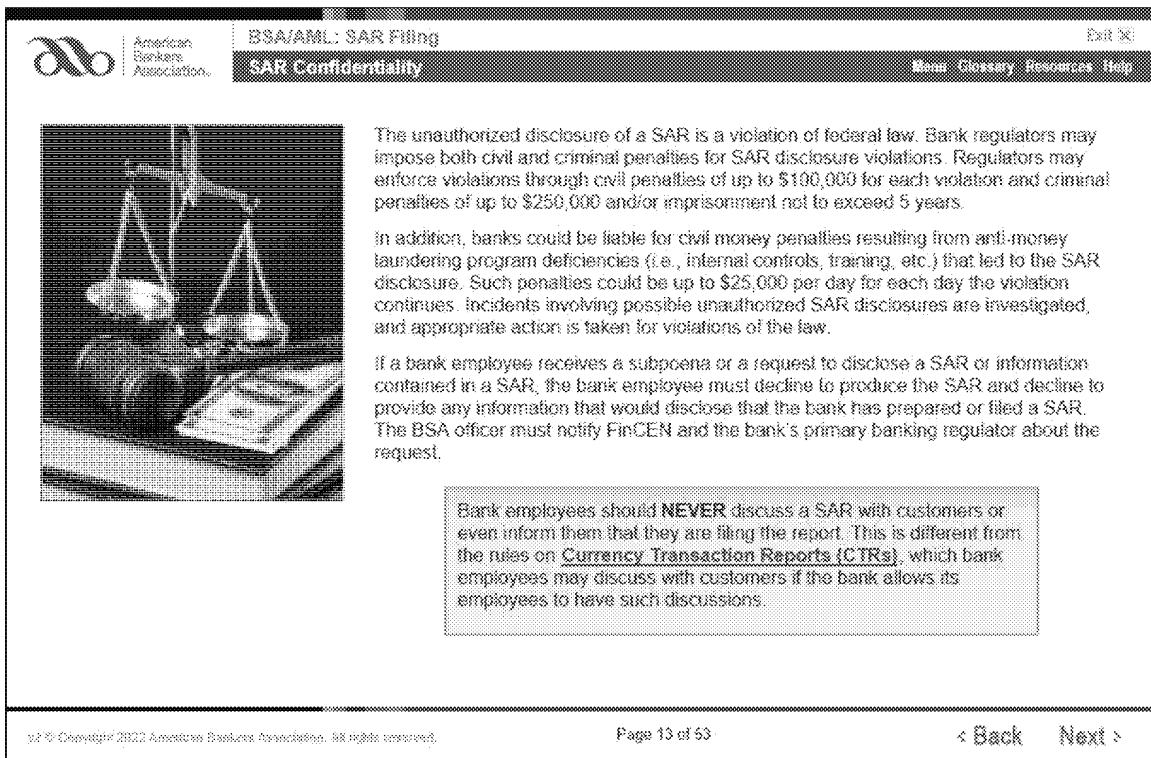
The screenshot shows the 'BSA/AML: SAR Filing' page with a sub-header 'SAR Confidentiality'. The main text explains that SAR information is unproven suspicion and federal law limits sharing. It states the general rule: no bank employee should notify anyone involved in the transaction. It also notes that banks must maintain confidentiality of SARs. Below the text is a 'Suspicious Activity Report' form with a large 'CONFIDENTIAL' stamp. The form includes instructions: '1. Complete the report in entirety with all required data known to the filer.', '2. Click "Submit" to save the report permanently and that all required fields are completed.', and '3. Sign with PIN:'. The footer of the screenshot includes '© 7/2022 American Bankers Association. All rights reserved.', 'Page 12 of 53', and '< Back Next >'.

SAR Confidentiality

Because the information in a SAR is only an unproven suspicion and to encourage banks to share information about possible criminal or terrorist activity with law enforcement, federal law strictly limits the ability to share information about a SAR or the SAR itself.

The general rule: No bank, director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the bank has reported a transaction. In addition, other bank employees should only be informed on a "need-to-know" basis.

Banks must be vigilant in maintaining the confidentiality of SARs. This includes ensuring that the bank informs all employees, agents, and individuals appropriately entrusted with information in a SAR that each person has an individual obligation to maintain SAR confidentiality. This obligation applies not only to the SAR itself, but also to information that would reveal the existence (or nonexistence) of the SAR. Likewise, the bank should inform such persons of the consequences for failing to maintain such confidentiality.



BSA/AML: SAR Filing
SAR Confidentiality

The unauthorized disclosure of a SAR is a violation of federal law. Bank regulators may impose both civil and criminal penalties for SAR disclosure violations. Regulators may enforce violations through civil penalties of up to \$100,000 for each violation and criminal penalties of up to \$250,000 and/or imprisonment not to exceed 5 years.

In addition, banks could be liable for civil money penalties resulting from anti-money laundering program deficiencies (i.e., internal controls, training, etc.) that led to the SAR disclosure. Such penalties could be up to \$25,000 per day for each day the violation continues. Incidents involving possible unauthorized SAR disclosures are investigated, and appropriate action is taken for violations of the law.

If a bank employee receives a subpoena or a request to disclose a SAR or information contained in a SAR, the bank employee must decline to produce the SAR and decline to provide any information that would disclose that the bank has prepared or filed a SAR. The BSA officer must notify FinCEN and the bank's primary banking regulator about the request.

Bank employees should **NEVER** discuss a SAR with customers or even inform them that they are filing the report. This is different from the rules on Currency Transaction Reports (CTRs), which bank employees may discuss with customers if the bank allows its employees to have such discussions.

© Copyright 2022 American Bankers Association. All rights reserved. Page 13 of 53 < Back Next >

SAR Confidentiality

The unauthorized disclosure of a SAR is a violation of federal law. Bank regulators may impose both civil and criminal penalties for SAR disclosure violations. Regulators may enforce violations through civil penalties of up to \$100,000 for each violation and criminal penalties of up to \$250,000 and/or imprisonment not to exceed 5 years.

In addition, banks could be liable for civil money penalties resulting from anti-money laundering program deficiencies (i.e., internal controls, training, etc.) that led to the SAR disclosure. Such penalties could be up to \$25,000 per day for each day the violation continues. Incidents involving possible unauthorized SAR disclosures are investigated, and appropriate action is taken for violations of the law.

If a bank employee receives a subpoena or a request to disclose a SAR or information contained in a SAR, the bank employee must decline to produce the SAR and decline to provide any information that would disclose that the bank has prepared or filed a SAR. The BSA officer must notify FinCEN and the bank's primary banking regulator about the request.

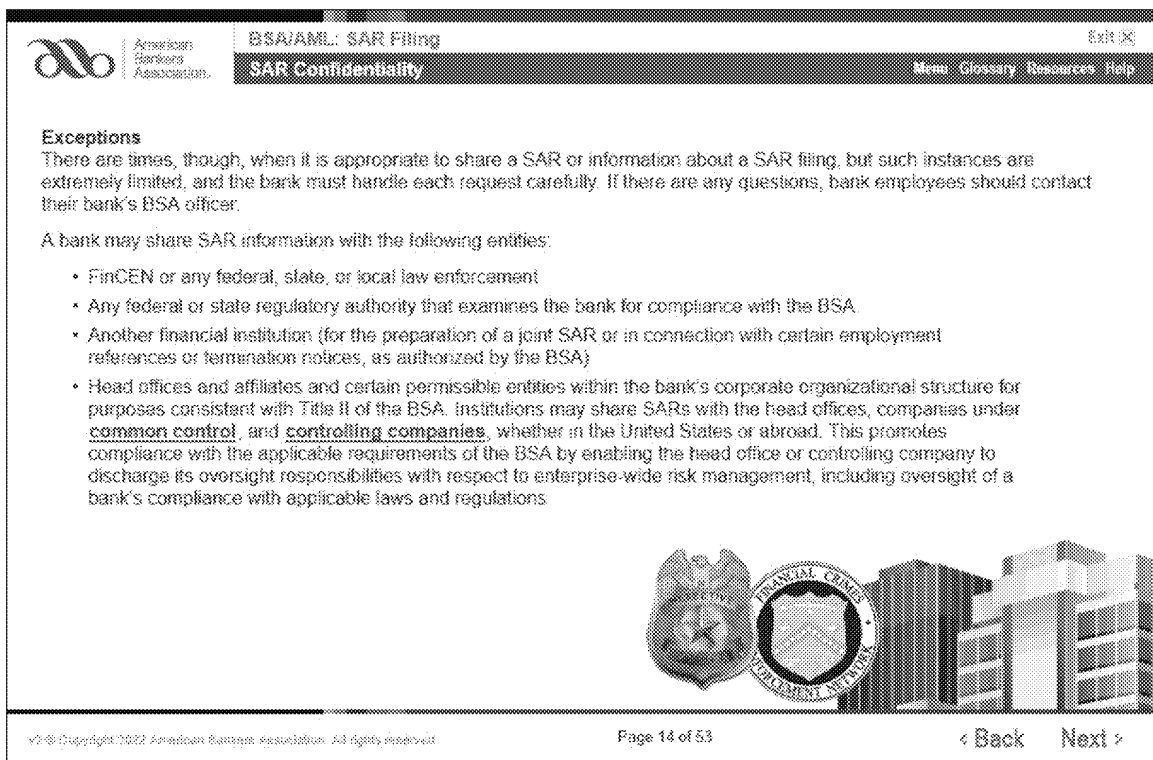
Bank employees should **NEVER** discuss a SAR with customers or even inform them that they are filing the report. This is different from the rules on Currency Transaction Reports (CTRs), which bank employees may discuss with customers if the bank allows its employees to have such discussions.

Glossary term:

Currency Transaction Report (CTR)

A CTR is a bank form used in the United States to help prevent money laundering. This form must be filled out by a bank representative whenever a customer attempts a currency transaction of more than \$10,000 cash in any 1 business day.

Page 13



Exceptions

There are times, though, when it is appropriate to share a SAR or information about a SAR filing, but such instances are extremely limited, and the bank must handle each request carefully. If there are any questions, bank employees should contact their bank's BSA officer.

A bank may share SAR information with the following entities:

- FinCEN or any federal, state, or local law enforcement
- Any federal or state regulatory authority that examines the bank for compliance with the BSA.
- Another financial institution (for the preparation of a joint SAR or in connection with certain employment references or termination notices, as authorized by the BSA)
- Head offices and affiliates and certain permissible entities within the bank's corporate organizational structure for purposes consistent with Title II of the BSA. Institutions may share SARs with the head offices, companies under common control, and controlling companies, whether in the United States or abroad. This promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a bank's compliance with applicable laws and regulations.

Page 14 of 53

SAR Confidentiality

Exceptions

There are times, though, when it is appropriate to share a SAR or information about a SAR filing, but such instances are extremely limited, and the bank must handle each request carefully. If there are any questions, bank employees should contact their bank's BSA officer.

A bank may share SAR information with the following entities:

- FinCEN or any federal, state, or local law enforcement
- Any federal or state regulatory authority that examines the bank for compliance with the BSA
- Another financial institution (for the preparation of a joint SAR or in connection with certain employment references or termination notices, as authorized by the BSA)
- Head offices and affiliates and certain permissible entities within the bank's corporate organizational structure for purposes consistent with Title II of the BSA. Institutions may share SARs with the head offices, companies under common control, and controlling companies, whether in the United States or abroad. This promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a bank's compliance with applicable laws and regulations.

Glossary terms:

Common control

Under "common control" means that another company, directly or indirectly, or acting through one or more other persons, owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution or controls in any manner the election of a majority of the directors or trustees of the company and the depository institution.

Controlling company

A controlling company is defined as the following:

- A bank holding company
- A savings and loan holding company
- A company having the power, directly or indirectly, to direct management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an industrial loan company

The screenshot shows a web page with the following content:

- Header:** American Bankers Association logo on the left. Navigation links: Home, Directory, Resources, Help. Page title: BSA/AML: SAR Filing - SAR Confidentiality. Exit button on the right.
- Main Text:**

Because the BSA regards foreign branches of U.S. banks as foreign banks for SAR filing purposes, they are affiliates that are not subject to SAR regulations. Accordingly, a U.S. bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches. Banks should maintain appropriate internal controls and arrangements with head offices, controlling companies, and affiliates to protect the confidentiality of SARs.

FinCEN and the bank's prudential regulators expect a bank's BSA officer to notify the bank's board of directors, or an appropriate board committee of the board, about the bank's SAR filings. There is no mandated format or frequency; reporting may occur monthly or quarterly or even less often depending on the volume of SARs filed. The BSA officer must stress the confidential nature of SAR data when providing information to the board.
- Note Box:**

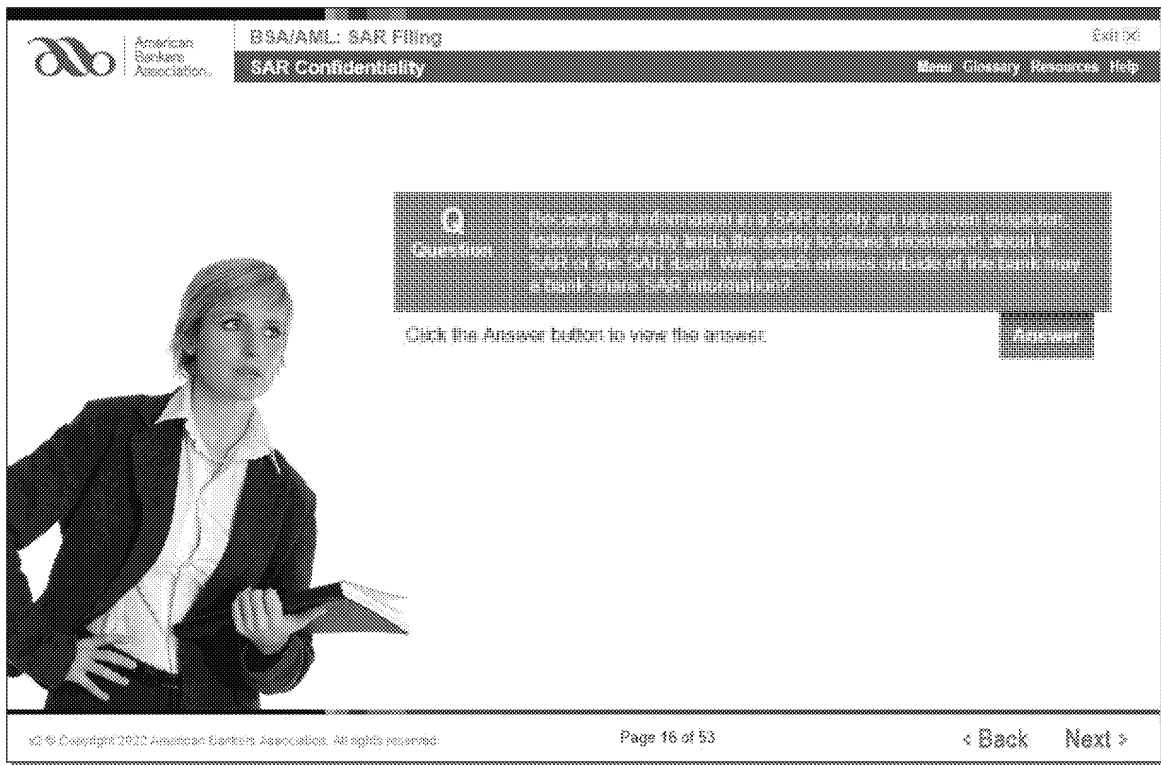
Note: Only authorized personnel such as the bank's BSA officer can make the determination regarding information sharing. Other bank personnel who know of the existence of a SAR should never take it upon themselves to share such information, even if requested to do so by law enforcement.
- Image:** A black and white photograph of a person's hands holding and looking at a document.
- Footer:** © 2022 American Bankers Association. All rights reserved. Page 15 of 53. Navigation: < Back Next >

SAR Confidentiality

Because the BSA regards foreign branches of U.S. banks as foreign banks for SAR filing purposes, they are affiliates that are not subject to SAR regulations. Accordingly, a U.S. bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches. Banks should maintain appropriate internal controls and arrangements with head offices, controlling companies, and affiliates to protect the confidentiality of SARs.

FinCEN and the bank's prudential regulators expect a bank's BSA officer to notify the bank's board of directors, or an appropriate board committee of the board, about the bank's SAR filings. There is no mandated format or frequency; reporting may occur monthly or quarterly or even less often depending on the volume of SARs filed. The BSA officer must stress the confidential nature of SAR data when providing information to the board.

Note: Only authorized personnel such as the bank's BSA officer can make the determination regarding information sharing. Other bank personnel who know of the existence of a SAR should never take it upon themselves to share such information, even if requested to do so by law enforcement.



BSA/AML: SAR Filing SAR Confidentiality

EXIT DC

Home Glossary Resources Help

Question

Because the information in a SAR is only an unproven suspicion, federal law strictly limits the ability to share information about a SAR or the SAR itself. With which entities outside of the bank may a bank share SAR information?

Click the Answer button to view the answer.

Next

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 16 of 53 < Back Next >

SAR Confidentiality

Question: Because the information in a SAR is only an unproven suspicion, federal law strictly limits the ability to share information about a SAR or the SAR itself. With which entities outside of the bank may a bank share SAR information?

Answer:

A SAR may be shared with the following entities:

- FinCEN or any federal, state, or local law enforcement
- Any federal or state regulatory authority that examines the bank for compliance with the BSA
- Another financial institution (for the preparation of a joint SAR or in connection with certain employment references or termination notices, as authorized by the BSA)

Page 16

Generally, effective suspicious activity monitoring and reporting systems include five key components. These components are interdependent and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance.

The five components of an effective SAR monitoring and reporting system include the following:

1. Identifying the suspicious activity
2. Managing alerts
3. Decision-making
4. Completion and filing
5. Monitoring and SAR filing on continuing activity

Suspicious activity monitoring and reporting are critical internal controls since proper monitoring and reporting processes are essential to ensure that the bank has an adequate and effective BSA compliance program.

The bank should have appropriate policies, procedures, and processes to monitor and identify unusual activity. The bank's risk profile will determine the sophistication of monitoring systems. These systems should pay particular attention to products, services, customers, entities, and geographies that present greater risk for money laundering, terrorist financing, or other financial crimes.

The bank should ensure that it assigns adequate staff to identify, research, and report suspicious activities. In making these determinations, management will take into account the bank's overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

For more information on risk assessment, see the ABA Frontline Compliance course, *BSA/AML: Risk Assessment and Customer Due Diligence*.

© Copyright 2022 American Bankers Association. All rights reserved. Page 17 of 53 < Back Next >

Five Key Components

Generally, effective suspicious activity monitoring and reporting systems include five key components. These components are interdependent and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance.

The five components of an effective SAR monitoring and reporting system include the following:

1. Identifying the suspicious activity
2. Managing alerts
3. Decision-making
4. Completion and filing
5. Monitoring and SAR filing on continuing activity

Suspicious activity monitoring and reporting are critical internal controls since proper monitoring and reporting processes are essential to ensure that the bank has an adequate and effective BSA compliance program.

The bank should have appropriate policies, procedures, and processes to monitor and identify unusual activity. The bank's risk profile will determine the sophistication of monitoring systems. These systems should pay particular attention to products, services, customers, entities, and geographies that present greater risk for money laundering, terrorist financing, or other financial crimes.

The bank should ensure that it assigns adequate staff to identify, research, and report suspicious activities. In making these determinations, management will take into account the bank's overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

For more information on risk assessment, see the ABA Frontline Compliance course, *BSA/AML: Risk Assessment and Customer Due Diligence*.

The screenshot shows a web page from the American Bankers Association. The page title is "BSA/AML: SAR Filing" and the sub-header is "Identifying the Suspicious Activity". The page content includes:

Banks must report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and other crimes that exceed the regulatory dollar thresholds. While banks are required to report suspicious activity, banks are not required to confirm the underlying crime. Investigation is the responsibility of law enforcement.

However, when evaluating suspicious activity and filing a SAR, it helps law enforcement when a bank identifies the specific characteristics of the suspicious activity that gave rise to the SAR filing. This is one reason that banks assign the responsibility to one person or division to make the decision. However, when evaluating suspicious activity and completing the SAR, banks are expected, to the best of their ability, to identify the characteristics of the suspicious activity.

Unusual activity identification can result from the following sources:

- Employee identification
- Law enforcement requests (including National Security Letters)
- Transaction monitoring
- Surveillance monitoring

At the bottom of the page, there is a navigation bar with "Page 18 of 53" and buttons for "< Back" and "Next >".

Identifying the Suspicious Activity

Banks must report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and other crimes that exceed the regulatory dollar thresholds. While banks are required to report suspicious activity, banks are not required to confirm the underlying crime. Investigation is the responsibility of law enforcement.

However, when evaluating suspicious activity and filing a SAR, it helps law enforcement when a bank identifies the specific characteristics of the suspicious activity that gave rise to the SAR filing. This is one reason that banks assign the responsibility to one person or division to make the decision. However, when evaluating suspicious activity and completing the SAR, banks are expected, to the best of their ability, to identify the characteristics of the suspicious activity.

Unusual activity identification can result from the following sources:

- Employee identification
- Law enforcement requests (including National Security Letters)
- Transaction monitoring
- Surveillance monitoring

Employee identification
Employee identification includes suspicious activities that are identified by employees during day-to-day operations. Therefore, employees need methods they can use to report suspicious activity to the appropriate personnel within the bank, such as a worksheet, email, or phone. Some banks ask employees to report to supervisory staff, while others provide a central point of contact.

It is hard to say what suspicious activity looks like. Suspicious activity will appear differently based on what role a particular employee holds at the bank and how employees interact with customers. For example, a teller might identify certain activity as being suspicious that a lender may never see, such as the structuring of deposits to avoid CTR reporting.

The opposite is also true since a lender will be able to identify suspicious activity that a teller would not see, such as fraudulent information on loan applications. This is one of the reasons that it is important not only for banks to know their customers, but also to ensure that all bank employees are trained to recognize suspicious activity when it occurs.

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 19 of 53 < Back Next >

Identifying the Suspicious Activity

Employee identification

Employee identification includes suspicious activities that are identified by employees during day-to-day operations. Therefore, employees need methods they can use to report suspicious activity to the appropriate personnel within the bank, such as a worksheet, email, or phone. Some banks ask employees to report to supervisory staff, while others provide a central point of contact.

It is hard to say what suspicious activity looks like. Suspicious activity will appear differently based on what role a particular employee holds at the bank and how employees interact with customers. For example, a teller might identify certain activity as being suspicious that a lender may never see, such as the structuring of deposits to avoid CTR reporting.

The opposite is also true since a lender will be able to identify suspicious activity that a teller would not see, such as fraudulent information on loan applications. This is one of the reasons that it is important not only for banks to know their customers, but also to ensure that all bank employees are trained to recognize suspicious activity when it occurs.

Employee identification—tellers and customer service representatives (CSRs)
 A typical example of a suspicious transaction for a teller would occur when a customer begins to conduct a currency transaction that exceeds \$10,000 but then reduces the amount of the transaction to below \$10,000 when told that the bank must complete a CTR for large cash transactions. Variations of this situation, referred to as *structuring*, are perhaps the most frequently cited examples of suspicious transactions that occur in banks.

» Click the image to see a list of examples of suspicious activity that may come to the attention of a teller or CSR.

» Click the image of Krystal Ballentine to see a suspicious activity scenario.

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 20 of 53 < Back Next >

Identifying the Suspicious Activity

Employee identification—tellers and customer service representatives (CSRs)

A typical example of a suspicious transaction for a teller would occur when a customer begins to conduct a currency transaction that exceeds \$10,000 but then reduces the amount of the transaction to below \$10,000 when told that the bank must complete a CTR for large cash transactions. Variations of this situation, referred to as *structuring*, are perhaps the most frequently cited examples of suspicious transactions that occur in banks.

» Click the image to see a list of examples of suspicious activity that may come to the attention of a teller or CSR.

Suspicious activity examples

- Corporate accounts where deposits or withdrawals are primarily in cash rather than checks
- Small businesses that frequently make cash deposits consisting of \$50 bills and/or \$100 bills
- Single-location businesses that make deposits at several branches of a bank
- Customers who frequently visit their safe deposit boxes before making cash deposits and then make cash deposits that are always less than the reportable dollar amount
- Deposits of sequentially numbered cashier's checks or money orders
- Large amounts of cash deposited that are wrapped with the currency straps from another bank
- Customers who insist on being added to the bank's CTR exemption list
- Customers who make numerous, separate deposits at ATMs below the reportable dollar amount
- Customers who are reluctant to provide personal information or information about their businesses
- Customers who have no record of past or present employment but make frequent large transactions
- Customers whose activity is inconsistent with their business
- Accounts receiving multiple ACH payroll deposits for individuals not on the account (may indicate human trafficking)

» Click the image of Krystal Ballentine to see a suspicious activity scenario.

Example

Krystal Ballentine, a customer of First National Bank, brought \$27,000 in cash to deposit to her checking account. When the teller told Krystal that the bank would need to complete a CTR, Krystal took back the money and left the bank. (Note that refusing to complete a transaction is suspicious and may be sufficient reason to file a SAR). The next day, there were three separate cash deposits into Krystal's checking account of \$9,000 each, apparently to avoid the CTR filing. Besides splitting the deposit into smaller amounts, a step known as structuring, Krystal's son and nephew made two of the deposits at different First National Bank branches.


In this example, the bank would still need to aggregate (add together) the transactions conducted in 1 business day and file a CTR, but the attempt to structure the transactions could also require the bank to file a SAR.

Glossary term:

Structuring transactions

A person structures a transaction if that person conducts or attempts to conduct one or more transactions in currency in any amount, at one or more banks, on 1 or more days, in any manner, for the purpose of evading the CTR filing requirements. "In any manner" includes, but is not limited to, breaking down a single currency sum exceeding \$10,000 into smaller amounts and conducting a series of transactions at or less than \$10,000. The transactions need not exceed the \$10,000 CTR filing threshold at any one bank on any single day in order to constitute structuring. The ABA Frontline Compliance course, *BSA/AML: Fundamentals*, covers structuring in greater detail.

Page 20



BSA/AML: SAR Filing

Identifying the Suspicious Activity

EXIT DC

Home Dictionary Resources Help

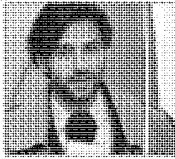
Employee identification—lenders

Suspicious activity detection and monitoring at banks should be an enterprise-wide process that considers the entire customer relationship. While a bank may have a sound process to identify and monitor potentially suspicious activities in deposit account products, formal processes may not exist for the bank's loan accounts. Monitoring a customer's entire relationship can give bankers greater perspective on the legitimacy and legality of a customer's business and transactions, especially when it comes to the lending function.

Bank employees involved in the lending function will encounter numerous suspicious situations.

Example

Larry Springer, the local TV weatherman and a customer of First National Bank, has applied for a loan. He has never married, preferring to devote himself entirely to predicting the weather. Mr. Springer tells the loan officer that he is in danger of being replaced at WJRK TV by Jerry Strum, a local celebrity tornado chaser, but Larry thinks if he can upgrade his education and become certified in weather forecasting, he can hold on to his job. Larry will use the funds to obtain a certification from the American Meteorological Society.



When the bank's loan officer reviews Larry's financials, it does not appear that Larry's income supports the amount he wants to borrow. Larry also exhibits a lavish lifestyle that is not supported by the income from his job. Larry has offered several recently purchased certificates of deposit (CDs) as collateral for the loan, but the source of the funds in those CDs is unclear and appears to have come from multiple negotiable instruments deposited to Larry's account by unknown persons.

© 2022 Copyright 2022 American Bankers Association. All rights reserved.

Page 21 of 53

< Back Next >

Identifying the Suspicious Activity

Employee identification—lenders


Suspicious activity detection and monitoring at banks should be an enterprise-wide process that considers the entire customer relationship. While a bank may have a sound process to identify and monitor potentially suspicious activities in deposit account products, formal processes may not exist for the bank's loan accounts. Monitoring a customer's entire relationship can give bankers greater perspective on the legitimacy and legality of a customer's business and transactions, especially when it comes to the lending function.

Bank employees involved in the lending function will encounter numerous suspicious situations.

Example

Larry Springer, the local TV weatherman and a customer of First National Bank, has applied for a loan. He has never married, preferring to devote himself entirely to predicting the weather. Mr. Springer tells the loan officer that he is in danger of being replaced at WJRK TV by Jerry Strum, a local celebrity tornado chaser, but Larry thinks if he can upgrade his education and become certified in weather forecasting, he can hold on to his job. According to the loan application, Larry will use the funds to obtain a certification from the American Meteorological Society.

When the bank's loan officer reviews Larry's financials, it does not appear that Larry's income supports the amount he wants to borrow. Larry also exhibits a lavish lifestyle that is not supported by the income from his job. Larry has offered several recently purchased certificates of deposit (CDs) as collateral for the loan, but the source of the funds in those CDs is unclear and appears to have come from multiple negotiable instruments deposited to Larry's account by unknown persons.



BSA/AML: SAR Filing

Identifying the Suspicious Activity

EXIT DC

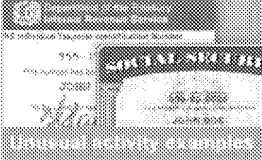
Home Dictionary Resources Help

Employee identification—lenders, continued

Due diligence is required during the loan application and underwriting process through customer identification program (CIP) and loan documentation requirements. However, the level of customer due diligence (CDD) performed for guarantors, signatories, principals, and other loan participants can vary, in part due to the fact that the bank may not require CIP compliance for some of these individuals.

One of the most important controls to address this aspect of compliance is the bank's BSA/AML training program. The bank's training program should provide for role-specific training and educate bank personnel on the types of activity that deemed loan processors might view as suspicious in their particular area of the bank.

The objective of CDD should be to help the bank predict, with relative certainty, the types of transactions that will be typical for a particular customer. These processes also should help the bank determine when transactions are potentially suspicious.



» Click the image to see examples of unusual activities lenders might see that may warrant follow-up consideration.

While banks typically consider loans secured by cash collateral and/or marketable securities as lower risk credit, criminals can easily use such collateral to hide illegal monies or obscure the purpose of funds. This is not the only way criminals use such loans to launder money, but this is one of the most common methods. The fact is, criminals can use any loan to launder money, but understanding the red flags and educating personnel on how to evaluate and monitor loan customers can help to identify possible suspicious activity.

© 7/2022 American Bankers Association. All rights reserved.

Page 22 of 53

< Back Next >

Identifying the Suspicious Activity

Employee identification—lenders, continued

Due diligence is required during the loan application and underwriting process through customer identification program (CIP) and loan documentation requirements. However, the level of customer due diligence (CDD) performed for guarantors, signatories, principals, and other loan participants can vary, in part due to the fact that the bank may not require CIP compliance for some of these individuals.

One of the most important controls to address this aspect of compliance is the bank's BSA/AML training program. The bank's training program should provide for role-specific training and educate bank personnel on the types of activity that deemed loan processors might view as suspicious in their particular area of the bank.


The objective of CDD should be to help the bank predict, with relative certainty, the types of transactions that will be typical for a particular customer. These processes also should help the bank determine when transactions are potentially suspicious.

» Click the image to see examples of unusual activities lenders might see that may warrant follow-up consideration.

Unusual activity examples

- A customer presents documents that cannot be readily identified or verified
- A customer provides both an Individual Taxpayer Identification Number (ITIN) and a Social Security number (SSN)
- A customer's home or business phone is disconnected for no apparent reason
- A customer is a trust, shell company, or private investment company that is reluctant to provide information on controlling parties or underlying beneficiaries
- A customer does business in high-risk locations
- A customer offers bribes to the loan officer for overlooking certain discrepancies
- A customer provides false or conflicting identification

While banks typically consider loans secured by cash collateral and/or marketable securities as lower risk credit, criminals can easily use such collateral to hide illegal monies or obscure the purpose of funds. This is not the only way criminals use such loans to launder money, but this is one of the most common methods. The fact is, criminals can use any loan to launder money, but understanding the red flags and educating personnel on how to evaluate and monitor loan customers can help to identify possible suspicious activity.



BSA/AML: SAR Filing

Identifying the Suspicious Activity

Exit DC


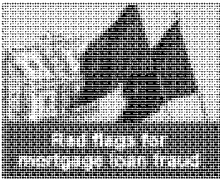
Home Dictionary Resources Help

Employee identification—mortgage lenders

Depository institutions have seen a large increase in mortgage loan fraud. According to the Federal Bureau of Investigation (FBI), mortgage fraud continues to be an escalating problem in the United States. The FBI also reports that many borrowers across the United States are still struggling with their mortgages, which creates an ideal climate for mortgage fraud perpetrators to employ a variety of schemes. Emerging and reemerging schemes include loan modification scams, foreclosure rescue, and identity theft exploiting home equity lines of credit.

In recent years, federal and state law enforcement and regulatory agencies have devoted considerable effort to the prevention, investigation, and prosecution of mortgage loan fraud. One of the ways law enforcement becomes aware of mortgage fraud is through the analysis of SARs filed by banks. These SARs provide valuable intelligence in mortgage fraud trends and can lead to the initiation of mortgage fraud cases as well as the enhancement of law enforcement investigations.

» **Click each image below to learn more about loan fraud.**

© 2022 American Bankers Association. All rights reserved.

Page 23 of 53

< Back Next >

Identifying the Suspicious Activity

Employee identification—mortgage lenders

Depository institutions have seen a large increase in mortgage loan fraud. According to the Federal Bureau of Investigation (FBI), mortgage fraud continues to be an escalating problem in the United States. The FBI also reports that many borrowers across the United States are still struggling with their mortgages, which creates an ideal climate for mortgage fraud perpetrators to employ a variety of schemes. Emerging and reemerging schemes include loan modification scams, foreclosure rescue, and identity theft exploiting home equity lines of credit.

In recent years, federal and state law enforcement and regulatory agencies have devoted considerable effort to the prevention, investigation, and prosecution of mortgage loan fraud. One of the ways law enforcement becomes aware of mortgage fraud is through the analysis of SARs filed by banks. These SARs provide valuable intelligence in mortgage fraud trends and can lead to the initiation of mortgage fraud cases as well as the enhancement of law enforcement investigations.

» **Click each image below to learn more about loan fraud.**

Common types of mortgage fraud

According to FinCEN, the following are common types of mortgage fraud:

Income fraud: Includes both overstating income to qualify for larger mortgages and understating income to qualify for hardship concessions and modifications

Appraisal fraud: Includes both overstating home value to obtain more money from a sale of property or cash-out refinancing and understating home value in connection with a plan to purchase a property at a discount


Liability fraud: Occurs when borrowers fail to list significant financial liabilities, such as other mortgages, car loans, or student loans, on mortgage loan applications. Without complete liability information, lenders cannot accurately assess borrowers' ability to repay debts

Foreclosure rescue scams: Target financially distressed homeowners with fraudulent offers of services or advice aimed at stopping or delaying the foreclosure process. Some of these scams require homeowners to transfer the title—or make monthly mortgage payments—to the purported "rescuer," rather than the real holder of the mortgage. Some foreclosure rescue scams require homeowners to pay fees before receiving "services" and are known as "advance fee" schemes

SSN fraud and other identify theft: Include the use of an SSN or other government identification card or number that belongs to someone other than the applicant in a loan application. Identity theft includes broader use of another's identity or identifiers (beyond an SSN) to obtain a mortgage or perpetrate a "fraud for profit" scheme

Red flags for mortgage loan fraud

- Inflated appraisals
- Bonuses to brokers or fee-based providers paid outside of closing or at closing
- Higher fees than customary for the local market
- Falsification of income, deposits, rents, etc.
- Falsification of identity documents—ITINs and SSNs for the same person
- Fake supporting documentation
- Requesting documents be signed in blank
- Purchase loans disguised as refinancing with cash-outs
- Investment opportunities and guarantees
- Terms too good to be true
- Employing high-pressure tactics
- Unexplained excessive fees/costs
- Requiring "prepayment" of certain disallowed fees



BSA/AML: SAR Filing

Identifying the Suspicious Activity

EXIT DC

Home | Glossary | Resources | Help

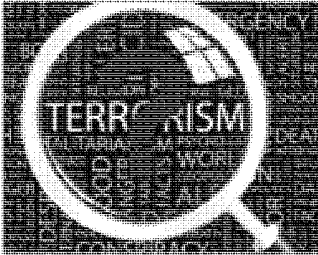
Identifying suspicious activity—all bank employees

The use of legitimate funding sources for terrorist objectives is a form of financial crime that often defies detection. One key difference between terrorists and traditional criminal organizations is that terrorist organizations often use funds from legitimate sources to support their objectives.

Ideological and political goals generally motivate terrorists, unlike other criminals who are motivated by profit. For the terrorist, money is a means to an end, while for other criminals, the money is an end in itself. Therefore, terrorists may use funds that come from legitimate sources, while money launderers have funds from illegitimate sources that they are trying to make appear legitimate.

In addition to using funds from legitimate sources, terrorists often engage in illegal activity, like kidnapping or human trafficking, to earn money to support their terrorist goals. Other funding sources for terrorists can include extortion, narcotics trafficking, smuggling, fraud, identity theft, and improper use of charitable donations.

However, the fact that terrorists often rely on legitimate funds can make it extremely difficult to distinguish a transaction that supports terrorist activities from normal bank transactions; for example, the 9/11 hijackers withdrew funds from ATMs that were no different from withdrawals by any other consumer.



© 2022 Copyright 2022 American Bankers Association. All rights reserved.
Page 24 of 53
< Back Next >

Identifying the Suspicious Activity

Identifying suspicious activity—all bank employees

The use of legitimate funding sources for terrorist objectives is a form of financial crime that often defies detection. One key difference between terrorists and traditional criminal organizations is that terrorist organizations often use funds from legitimate sources to support their objectives.

Ideological and political goals generally motivate terrorists, unlike other criminals who are motivated by profit. For the terrorist, money is a means to an end, while for other criminals, the money is an end in itself. Therefore, terrorists may use funds that come from legitimate sources, while money launderers have funds from illegitimate sources that they are trying to make appear legitimate.

In addition to using funds from legitimate sources, terrorists often engage in illegal activity, like kidnapping or human trafficking, to earn money to support their terrorist goals. Other funding sources for terrorists can include extortion, narcotics trafficking, smuggling, fraud, identity theft, and improper use of charitable donations.

However, the fact that terrorists often rely on legitimate funds can make it extremely difficult to distinguish a transaction that supports terrorist activities from normal bank transactions; for example, the 9/11 hijackers withdrew funds from ATMs that were no different from withdrawals by any other consumer.

Identifying suspicious activity—all bank employees, continued
Banks should develop practices and procedures to help detect transactions that may involve funds used in terrorist financing so that terrorists do not use the bank unknowingly to further the goal of terrorism. To do this, banks should be aware of possible red flags that could indicate terrorist financing.

The following categories of potentially suspicious or unusual activities demonstrate transactions that could necessitate additional scrutiny. These categories and examples are not exhaustive but should be used with other available information (including any lists issued by appropriate national authorities of suspected terrorists, terrorist groups, and associated individuals and entities), the nature of the transaction, and the parties involved in the transaction. While any one or more of the factors listed may warrant further investigation, none of these factors by itself means the transaction is suspicious or unusual.

» Roll over each category to see examples of potentially suspicious or unusual activities.

- Accounts
- Fund transfers
- Deposits and withdrawals
- Characteristics

© 7/2022 American Bankers Association. All rights reserved. Page 25 of 53 < Back Next >

Identifying the Suspicious Activity

Identifying suspicious activity—all bank employees, continued

Banks should develop practices and procedures to help detect transactions that may involve funds used in terrorist financing so that terrorists do not use the bank unknowingly to further the goal of terrorism. To do this, banks should be aware of possible red flags that could indicate terrorist financing.

The following categories of potentially suspicious or unusual activities demonstrate transactions that could necessitate additional scrutiny. These categories and examples are not exhaustive but should be used with other available information (including any lists issued by appropriate national authorities of suspected terrorists, terrorist groups, and associated individuals and entities), the nature of the transaction, and the parties involved in the transaction. While any one or more of the factors listed may warrant further investigation, none of these factors by itself means the transaction is suspicious or unusual.

» Roll over each category to see examples of potentially suspicious or unusual activities.

Accounts

- Accounts that receive periodic deposits but then stay dormant. These accounts can be used to create others that appear legitimate through which additional fraudulent activities may be carried out
- A dormant account with a minimal sum that suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the deposited sum has been removed
- When opening an account, a customer who refuses to provide information, attempts to reduce the level of information provided, or provides information that is misleading or difficult to verify
- An account for which several persons who are unrelated or have no apparent connection have signature authority
- An account opened for a legal entity or organization using the same address as other legal entities or organizations, where the same person or persons have signature authority, but there is no apparent economic or legal reason for such an arrangement
- An account opened in the name of a recently formed legal entity where a higher-than-expected level of deposits are made in comparison with the income of the founders of the entity

Funds transfers

- A large number of incoming or outgoing funds transfers through a business account without any logical business or other economic purpose for the transfers. This is especially true when the activity involves higher-risk locations
- Funds transfers that do not include information on the originator or the person on whose behalf the transaction is conducted when the inclusion of such information would be expected

- Foreign exchange transactions for a customer that are conducted by a third party followed by funds transfers to locations that either have no apparent business connection with the customer or that are higher-risk countries

Deposits and withdrawals

- Large cash withdrawals from a business account not normally associated with cash transactions
- Large cash deposits to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted by check
- Multiple transactions on the same day at the same branch of a bank with an apparent attempt to use different tellers
- Structuring of deposits through multiple branches of the same bank or by groups of individuals who enter a single branch at the same time
- Deposit or withdrawal of cash in amounts that fall consistently just below identification or reporting thresholds
- Deposit of multiple monetary instruments at amounts that fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered

Characteristics of the customer and/or the customer's business activity

- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.)
- Stated occupation of an account holder or transactor that is not consistent with the level or type of activity in the account or transaction—for example, a student or unemployed individual who receives or sends large numbers of wire transfers or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area
- Financial transactions by or for nonprofit or charitable organizations with no logical economic purpose or where there is no link between the stated activity of the organization and the parties in the transaction
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer does not appear to justify the use of a safe deposit box

The screenshot shows a web-based interface for "BSA/AML: SAR Filing" titled "Identifying the Suspicious Activity". It includes a navigation menu with "Home", "History", "Resources", and "Help". The main content area is titled "Exercise" and "Situation 1". Under "Background", it describes a teller named Betty A. Warren at the Last Bank of the South who notices unusual cash withdrawals from an account owned by Misty Smith, a contract law attorney. Betty decides to overlook reporting these transactions to management. The interface prompts the user to answer the question "What would you have done if you were Betty?" and provides a text input field and a "Suggested Results" button. The footer contains copyright information for the American Bankers Association (© 2022), page number 26 of 53, and navigation buttons for "Back" and "Next".

Identifying the Suspicious Activity

Exercise

Situation 1

Background

Betty A. Warren, a teller at the Last Bank of the South, notices an increase in cash withdrawal activity from an account owned by Misty Smith, a contract law attorney. These large cash withdrawals, just under the \$10,000 reporting threshold for CTR filing, appear to follow the deposit of sequentially numbered money orders and cashier's checks. This activity seems very unusual for a contract law attorney, and Misty has not transacted business in this way in the past.

Betty has a long line of customers waiting. Because Misty is an established customer, and because Betty is in such a hurry to get to the other customers, Betty makes the decision to overlook reporting Misty's transactions to management.

What would you have done if you were Betty?

» **Type your answers in the field. When finished, click the Suggested Results button to view possible responses.**

Suggested Results

Betty should not have ignored the activity. Betty could be missing a very important opportunity to protect the bank, and failure to report the activity could cause law enforcement to accuse Betty of "willful blindness." Willful blindness is a deliberate failure to make a reasonable inquiry of wrongdoing despite suspicion or an awareness of the high probability of its existence. Willful blindness involves conscious avoidance of the truth and gives rise to an inference of knowledge of the crime in question.

Although there may be a very logical and legal reason for the unusual activity, Betty is in no position to know that. Betty does not have to refuse to conduct Misty's transactions, nor close her line down and ignore other customers. However, Betty should report the activity to the bank's BSA officer or person responsible for filing SARs. If, after investigating the activity, the bank may decide not to file a SAR, but that is a decision that the appropriate person at the bank should make.

Exercise

Situation 2

Background
 Helen Wailing is a loan officer at the Third National Bank. Kathy Morgan applies for a loan to purchase a pickup truck. When Helen obtains Kathy's credit report, it contains an identity theft alert and an address discrepancy alert. Kathy says she placed the alert because someone hacked the database of the university she attended, and the faculty advisor recommended that all students place such an alert. She changed her address because she was being harassed by another student and had to move into an apartment, but the credit report still shows the house as her primary residence.

Things have been slow in the auto-lending department lately, and Helen has had a hard time meeting her goals. Helen feels that she can rely on her 40 years of experience as a loan officer and believes that the explanations that Kathy has provided for the alert and the address discrepancy all sound reasonable.

What would you do if you were Helen?

» Type your answers in the field. When finished, click the Suggested Results button to view possible responses.

Suggested Results

© Copyright 2022 American Bankers Association. All rights reserved. Page 27 of 53 < Back Next >

Identifying the Suspicious Activity

Exercise

Situation 2

Background

Helen Wailing is a loan officer at the Third National Bank. Kathy Morgan applies for a loan to purchase a pickup truck. When Helen obtains Kathy's credit report, it contains an identity theft alert and an address discrepancy alert. Kathy says she placed the alert because someone hacked the database of the university she attended, and the faculty advisor recommended that all students place such an alert. She changed her address because she was being harassed by another student and had to move into an apartment, but the credit report still shows the house as her primary residence.

Things have been slow in the auto-lending department lately, and Helen has had a hard time meeting her goals. Helen feels that she can rely on her 40 years of experience as a loan officer and believes that the explanations that Kathy has provided for the alert and the address discrepancy all sound reasonable.

What would you do if you were Helen?

» Type your answers in the field. When finished, click the Suggested Results button to view possible responses.

Suggested Results

Helen should not have ignored the obvious suspicious issues with this loan. Although Kathy may be telling the truth, Helen is in no position to make a loan knowing that the information given is potentially fraudulent or may have resulted from identity theft. Therefore, she needs to investigate further before a decision can be made.

BSA/AML: SAR Filing EXIT DC

Identifying the Suspicious Activity Home Glossary Resources Help

Self-Check Quiz

Bill Stodder is the owner of a delicatessen near the bank. He frequently makes large cash deposits to his general operating account at your bank. Which two options might lead you to believe this activity is suspicious?

» **Select the correct answers and click Submit.**

A) Bill always comes to the bank at 3 p.m.

B) Bill repeatedly makes deposits consisting of moldy-smelling \$50 and \$100 bills

C) Bill has begun making large cash deposits, which is unusual for a deli

D) Bill brings a platter of sandwiches for the tellers

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 28 of 53 < Back Next >

Identifying the Suspicious Activity

Self-Check Quiz

Bill Stodder is the owner of a delicatessen near the bank. He frequently makes large cash deposits to his general operating account at your bank. Which two options might lead you to believe this activity is suspicious?

» **Select the correct answers and click Submit.**

- A) Bill always comes to the bank at 3 p.m.
- B) Bill repeatedly makes deposits consisting of moldy-smelling \$50 and \$100 bills
- C) Bill has begun making large cash deposits, which is unusual for a deli
- D) Bill brings a platter of sandwiches for the tellers

B and C are correct.

A is incorrect because the fact that he comes to the bank in the afternoon could just indicate that he does his banking after the lunch rush. D is incorrect because a friendly gesture does not necessarily indicate suspicious activity.

Page 28

BSA/AML: SAR Filing
Identifying the Suspicious Activity

Self-Check Quiz

Which three customer situations could indicate suspicious activity?

» Select the correct answers and click Submit.

A) The customer presents unusual documents that cannot be readily identified or verified

B) The customer's home or business phone has been disconnected for no apparent reason

C) The customer provides both an ITIN and an SSN

D) The customer has a single location business that makes deposits at only one branch of your bank

Submit Try Again

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 29 of 53 < Back Next >

Identifying the Suspicious Activity

Self-Check Quiz

Which three customer situations could indicate suspicious activity?

» Select the correct answers and click Submit.

- A) The customer presents unusual documents that cannot be readily identified or verified
- B) The customer's home or business phone has been disconnected for no apparent reason
- C) The customer provides both an ITIN and an SSN
- D) The customer has a single location business that makes deposits at only one branch of your bank

A, B, and C are correct.

D is incorrect because individuals wishing to conduct illegal activity will take deposits to different branch locations, hoping the bank will not have the ability to aggregate all of the activity if it is done in different locations.

Page 29

Law enforcement inquiries and requests
The following examples of law enforcement requests are another way banks may be alerted to potential suspicious activity:

- Grand jury subpoenas
- National Security Letters (NSLs)
- 314(a) requests

Each bank should establish policies and procedures for the following tasks:

- Identifying the subject of the request
- Monitoring the subject's transaction activity, if appropriate
- Identifying potentially suspicious activity, and as appropriate, filing a SAR

It is important to understand that a grand jury subpoena, an NSL, or a 314(a) request alone does not mean that something is suspicious. Law enforcement or the grand jury may be seeking information for an investigation that is not directly related to the bank's own customer. However, it may be a reason to investigate further.

Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Instead, the SAR should reference only the facts and circumstances that supported the finding of suspicious activity.

© 7/2022 American Bankers Association. All rights reserved. Page 30 of 53 < Back Next >

Identifying the Suspicious Activity

Law enforcement inquiries and requests

The following examples of law enforcement requests are another way banks may be alerted to potential suspicious activity:

- Grand jury subpoenas
- National Security Letters (NSLs)
- 314(a) requests

Each bank should establish policies and procedures for the following tasks:

- Identifying the subject of the request
- Monitoring the subject's transaction activity, if appropriate
- Identifying potentially suspicious activity and, as appropriate, filing a SAR

It is important to understand that a grand jury subpoena, an NSL, or a 314(a) request alone does not mean that something is suspicious. Law enforcement or the grand jury may be seeking information for an investigation that is not directly related to the bank's own customer. However, it may be a reason to investigate further.

Note: Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Instead, the SAR should reference only the facts and circumstances that supported the finding of suspicious activity.

Glossary terms:

National Security Letters (NSLs)

NSLs are written investigative demands that may be issued by local FBI and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain records from financial institutions. These are highly confidential and must be handled following all appropriate procedures.

314(a) requests

A 314(a) request is an information-sharing procedure authorized by Section 314(a) of the USA PATRIOT Act. Section 314(a) authorizes a federal, state, local, or foreign law enforcement agency investigating terrorism or money laundering to request that FinCEN solicit, on its behalf, certain information from banks and other financial institutions about an individual, entity, or organization about which the law enforcement entity is seeking information.

Page 30

BSA/AML: SAR Filing Exit X

Identifying the Suspicious Activity New Gallery Resources Help

CONFIDENTIAL

NSLs are also highly confidential, so no bank or officer, employee, or agent of the institution can disclose to any person that a government agency has sought or obtained access to records through an NSL.

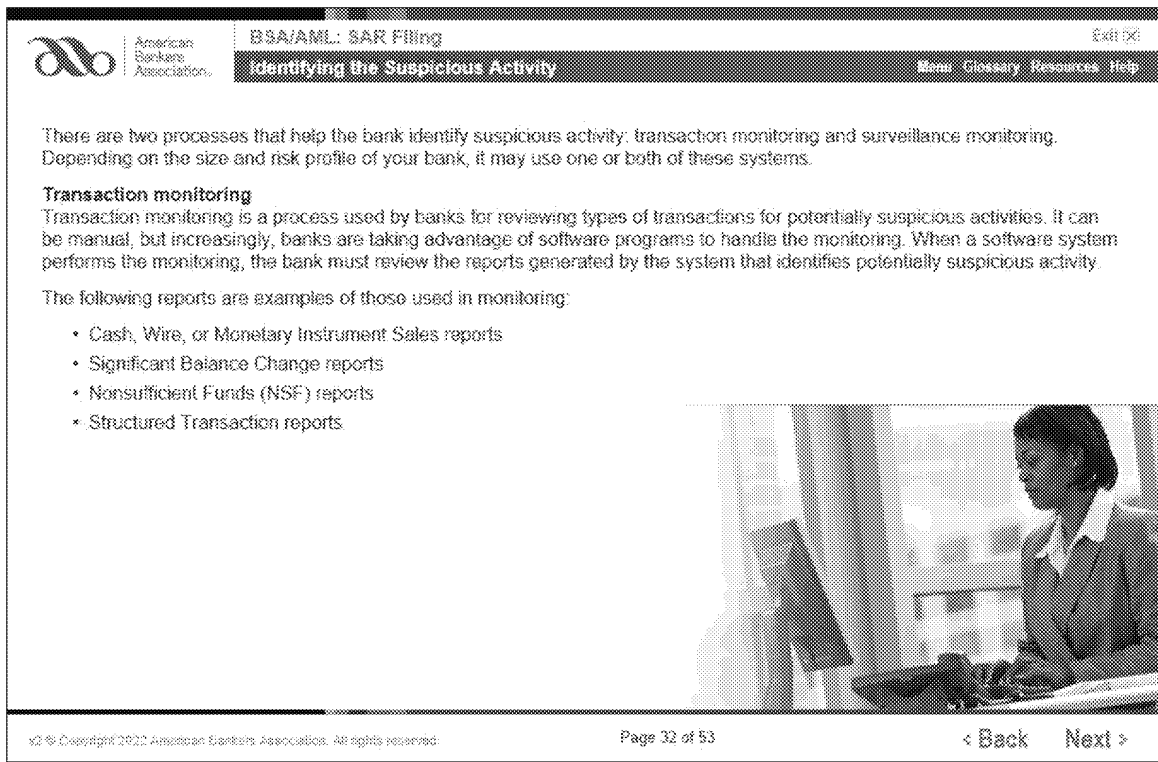
The BSA officer must respond appropriately to ensure confidentiality, and the bank should have written policies and procedures in place for processing and maintaining confidentiality. If the bank files a SAR, it should not contain any reference to receipt or existence of an NSL and should only reference the facts and activities that supported the decision to file a SAR.

© 7/2022 American Bankers Association. All rights reserved. Page 31 of 53 < Back Next >

Identifying the Suspicious Activity

NSLs are also highly confidential, so no bank or officer, employee, or agent of the institution can disclose to any person that a government agency has sought or obtained access to records through an NSL.

The BSA officer must respond appropriately to ensure confidentiality, and the bank should have written policies and procedures in place for processing and maintaining confidentiality. If the bank files a SAR, it should not contain any reference to receipt or existence of an NSL and should only reference the facts and activities that supported the decision to file a SAR.



There are two processes that help the bank identify suspicious activity: transaction monitoring and surveillance monitoring. Depending on the size and risk profile of your bank, it may use one or both of these systems.

Transaction monitoring
Transaction monitoring is a process used by banks for reviewing types of transactions for potentially suspicious activities. It can be manual, but increasingly, banks are taking advantage of software programs to handle the monitoring. When a software system performs the monitoring, the bank must review the reports generated by the system that identifies potentially suspicious activity.

The following reports are examples of those used in monitoring:

- Cash, Wire, or Monetary Instrument Sales reports
- Significant Balance Change reports
- Nonsufficient Funds (NSF) reports
- Structured Transaction reports

Page 32 of 53

Identifying the Suspicious Activity

There are two processes that help the bank identify suspicious activity: transaction monitoring and surveillance monitoring. Depending on the size and risk profile of your bank, it may use one or both of these systems.

Transaction monitoring

Transaction monitoring is a process used by banks for reviewing types of transactions for potentially suspicious activities. It can be manual, but increasingly, banks are taking advantage of software programs to handle the monitoring. When a software system performs the monitoring, the bank must review the reports generated by the system that identifies potentially suspicious activity.

The following reports are examples of those used in monitoring:

- Cash, Wire, or Monetary Instrument Sales reports
- Significant Balance Change reports
- Nonsufficient Funds (NSF) reports
- Structured Transaction reports

Identifying the Suspicious Activity

» Roll over the reports below to see some of the information generated by transaction monitoring reports.

Currency activity reports

Banks use currency activity reports to help ensure that CTRs are filed and to identify suspicious cash activity. These reports include the following information:

- Cash transactions, either deposits or withdrawals, aggregating \$10,000 or more and, therefore, requiring a CTR
- Cash transactions (either single or multiple transactions) that are below the \$10,000 reporting threshold (e.g., between \$7,000 and \$10,000)
- Cash involving multiple lower transactions (e.g., \$3,000) that over a period of time aggregate to a substantial sum
- Cash aggregated by a tax identification number, customer information file number, or other identifier such as an address or a telephone number

Funds transfer records

Wire transfer reviews can also help the bank identify patterns of unusual activity. The bank will determine the frequency of these reviews based on the bank's risk profile and the volume of activity. Reports may focus on identifying higher-risk geographic locations and larger dollar funds transfer transactions.

When creating these reports, whether manually or using software, filters are set to identify transactions for review. For example, the report may identify groups of noncustomer transactions or payable upon proper identification (PUPID) transactions. Banks should subject such activities to additional research to ensure the activity is consistent with the stated account purpose and expected activity. When the bank identifies inconsistencies, it may need to investigate further to determine if a SAR is warranted.

Monetary instrument records

Banks must maintain records of transactions in certain monetary instruments (this is covered in greater detail in the Frontline course, *BSA/AML: Recordkeeping*). These records can help identify possible cash structuring through purchases of cashier's checks, official bank checks, money orders, gift cards, or traveler's checks.

The review for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) to identify the following patterns:

- Common payees
- Common purchasers
- Consecutively numbered monetary instruments

Note: It is important to remember that a single unusual transaction alone may not be suspicious. It is important, though, that your BSA officer is aware of the transaction so he or she can take appropriate steps in compliance with the BSA and the bank's policies and procedures.

The screenshot shows a document page with the following elements:

- Header:** American Bankers Association logo on the left, and 'BSA/AML: SAR Filing' and 'Identifying the Suspicious Activity' in the center. Navigation links 'Home', 'Directory', 'Resources', and 'Help' are on the right.
- Image:** A black and white photograph of a man in a suit sitting at a desk, looking thoughtful.
- Text:**

Banks should base the level of review of any daily or monthly reports on risk and should cover the bank's higher-risk products, services, customers, entities, and geographic locations. The dollar threshold set for review is discretionary but should be set to allow the bank to detect unusual activity that is outside the norms set by the bank.

When the bank identifies unusual activity, the bank's BSA officer or risk officer will evaluate all relevant information to determine whether the activity is suspicious.

Management should periodically evaluate the appropriateness of filtering criteria and thresholds. Each bank should evaluate and identify filtering criteria most appropriate for their bank. In addition, independent reviewers should review and evaluate the programming of the bank's monitoring system for reasonable filtering criteria.
- Footer:** '© 2022 Copyright 2022 American Bankers Association. All rights reserved.', 'Page 34 of 53', and navigation buttons '< Back' and 'Next >'.

Identifying the Suspicious Activity

Banks should base the level of review of any daily or monthly reports on risk and should cover the bank's higher-risk products, services, customers, entities, and geographic locations. The dollar threshold set for review is discretionary but should be set to allow the bank to detect unusual activity that is outside the norms set by the bank.

When the bank identifies unusual activity, the bank's BSA officer or risk officer will evaluate all relevant information to determine whether the activity is suspicious.

Management should periodically evaluate the appropriateness of filtering criteria and thresholds. Each bank should evaluate and identify filtering criteria most appropriate for their bank. In addition, independent reviewers should review and evaluate the programming of the bank's monitoring system for reasonable filtering criteria.

The screenshot shows a document page with the following elements:

- Header:** American Bankers Association logo on the left, "BSA/AML: SAR Filing" in the center, and "Exit" on the right. Below the title is a navigation bar with "Home", "Contact", "Resources", and "Help".
- Image:** A black and white photograph of a person's silhouette looking out a window with multiple panes.
- Section Header:** **Surveillance monitoring**
- Text:**

Surveillance monitoring is an automated type of transaction monitoring that may combine multiple types of transactions and is likely to use various rules to identify individual transactions, patterns of activity, or deviations from expected activity.

The programs may be off-the-shelf or developed and customized in-house, but they are designed to capture a wide range of account activity, such as cash activity, funds transfers, automated clearing house (ACH) transfers, and ATM transactions and include rule-based and intelligent systems to detect unusual or higher-risk transactions.

Surveillance monitoring is generally more sophisticated than transaction monitoring since transaction monitoring is only based on a single rule (e.g., a transaction greater than \$10,000). Surveillance monitoring, though, applies multiple overlapping rules and filters or "alerts" that are more complex to identify potentially suspicious transactions.
- Footer:** "© Copyright 2022 American Bankers Association. All rights reserved." on the left, "Page 35 of 53" in the center, and "< Back Next >" on the right.

Identifying the Suspicious Activity

Surveillance monitoring

Surveillance monitoring is an automated type of transaction monitoring that may combine multiple types of transactions and is likely to use various rules to identify individual transactions, patterns of activity, or deviations from expected activity.

The programs may be off-the-shelf or developed and customized in-house, but they are designed to capture a wide range of account activity, such as cash activity, funds transfers, automated clearing house (ACH) transfers, and ATM transactions and include rule-based and intelligent systems to detect unusual or higher-risk transactions.

Surveillance monitoring is generally more sophisticated than transaction monitoring since transaction monitoring is only based on a single rule (e.g., a transaction greater than \$10,000). Surveillance monitoring, though, applies multiple overlapping rules and filters or "alerts" that are more complex to identify potentially suspicious transactions.

The parameters and filters used in such systems must be reasonable and tailored to activity that the bank is trying to identify or control. When installing such a system, bank management will review the system prior to implementation to identify any unaddressed gaps (common money laundering techniques or frauds).

Example
The bank may have set its filters for cash structuring to only be triggered by a daily cash transaction aggregation in excess of \$10,000 (CTR threshold). The bank may need to refine the filters to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions slightly under the CTR threshold or ones conducted over several days.

Note
When a bank uses an automated system, regulators will ask the bank to validate two elements. First, the bank must validate that the system itself is properly constructed and works in conjunction with the bank's risk profile. Second, the bank should periodically check the filter settings to make sure they are working properly and capture the appropriate transactions for review and investigation.

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 36 of 53 < Back Next >

Identifying the Suspicious Activity

The parameters and filters used in such systems must be reasonable and tailored to activity that the bank is trying to identify or control. When installing such a system, bank management will review the system prior to implementation to identify any unaddressed gaps (common money laundering techniques or frauds).

Example

The bank may have set its filters for cash structuring to only be triggered by a daily cash transaction aggregation in excess of \$10,000 (CTR threshold). The bank may need to refine the filters to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions slightly under the CTR threshold or ones conducted over several days.

Note: When a bank uses an automated system, regulators will ask the bank to validate two elements. First, the bank must validate that the system itself is properly constructed and works in conjunction with the bank's risk profile. Second, the bank should periodically check the filter settings to make sure they are working properly and capture the appropriate transactions for review and investigation.

BSA/AML: SAR Filing
American Bankers Association

Identifying the Suspicious Activity

Self-Check Quiz

Which type of transaction monitoring report can help identify possible cash structuring through purchases of cashier's checks, official bank checks, money orders, gift cards, or traveler's checks?

» Select the correct answer and click Submit.

A) Currency activity reports

B) Funds transfer records

C) Monetary instrument records

D) Overdraft reports

Submit Try Again

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 37 of 53 < Back Next >

Identifying the Suspicious Activity

Self-Check Quiz

Which type of transaction monitoring report can help identify possible cash structuring through purchases of cashier's checks, official bank checks, money orders, gift cards, or traveler's checks?

» Select the correct answer and click Submit.

- A) Currency activity reports
- B) Funds transfer records
- C) Monetary instrument records
- D) Overdraft reports

C is correct.

A is incorrect because these reports are used to help the bank file CTRs and identify suspicious cash activity. B is incorrect because these reports are used to help the bank identify patterns of unusual activity. D is incorrect because overdraft reports are not a type of transaction monitoring report.

Page 37

The screenshot shows a web interface for a quiz. At the top left is the American Bankers Association logo. The page title is 'BSA/AML: SAR Filing' and the specific topic is 'Identifying the Suspicious Activity'. A navigation menu includes 'Home', 'Glossary', 'Resources', and 'Help'. The main content area contains a question box with a question mark icon and the text: 'Which type of monitoring system is generally more sophisticated: surveillance monitoring or transaction monitoring?'. Below the question box is a text prompt: 'Click the Answer button to view the answer.' and an 'Answer' button. To the right of the question box is a photograph of a woman with her hand on her chin, appearing to be in deep thought. At the bottom of the page, there is a footer with the text: '© 2022 Copyright 2022 American Bankers Association. All rights reserved.', 'Page 38 of 53', and navigation buttons '< Back' and 'Next >'.

Identifying the Suspicious Activity

Question: Which type of monitoring system is generally more sophisticated: surveillance monitoring or transaction monitoring?

Answer: Surveillance monitoring is generally more sophisticated than transaction monitoring since transaction monitoring is only based on a single rule (e.g., a transaction greater than \$10,000). Surveillance monitoring, though, applies multiple, overlapping rules and filters or "alerts" that are more complex to identify potentially suspicious transactions.

Page 38

The screenshot shows a web page from the American Bankers Association. The page title is "BSA/AML: SAR Filing" and the sub-header is "Managing Alerts". The main content area contains the following text:

The second component in the process is a method for managing alerts so they do not become overwhelming. The bank must have systems in place to investigate alerts and be sure there are processes and staff assigned to evaluate any unusual activity, no matter how the bank identifies that activity.

Typically, in managing alerts, the bank will take the following steps:

- Have policies and procedures in place for referring unusual activity from all areas of the bank or business lines to the personnel responsible for evaluation and reporting
- Establish clear and defined escalation processes from the point of initial detection to the conclusion of the investigation
- Assign adequate staff to identify, evaluate, and report potentially suspicious activities

Below the text is a horizontal navigation bar with five numbered steps:

1. Identify unusual activity
2. Investigate alerts
3. Escalate activity
4. Complete all files
5. Report suspicious activity

The footer of the page includes the copyright notice "© 2022 Copyright 2022 American Bankers Association. All rights reserved.", the page number "Page 39 of 53", and navigation links "< Back" and "Next >".

Managing Alerts


The second component in the process is a method for managing alerts so they do not become overwhelming. The bank must have systems in place to investigate alerts and be sure there are processes and staff assigned to evaluate any unusual activity, no matter how the bank identifies that activity.

Typically, in managing alerts, the bank will take the following steps:

- Have policies and procedures in place for referring unusual activity from all areas of the bank or business lines to the personnel responsible for evaluation and reporting
- Establish clear and defined escalation processes from the point of initial detection to the conclusion of the investigation
- Assign adequate staff to identify, evaluate, and report potentially suspicious activities

BSA/AML: SAR Filing Exit DC

Managing Alerts Home Directory Resources Help



The bank should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the bank's overall risk profile and the volume of transactions.

Additionally, a bank should ensure that the assigned staff are experienced and provided with comprehensive and ongoing training to maintain their expertise. The bank should provide staff with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

After thorough research and analysis, investigators should document conclusions, including any recommendation regarding whether or not to file a SAR. When multiple departments are responsible for researching unusual activities (for example, when the bank's BSA department researches BSA-related activity and the bank's fraud department researches fraud-related activity), the lines of communication between the departments must remain open. This ensures that the bank identifies, evaluates, and reports all suspicious activity.

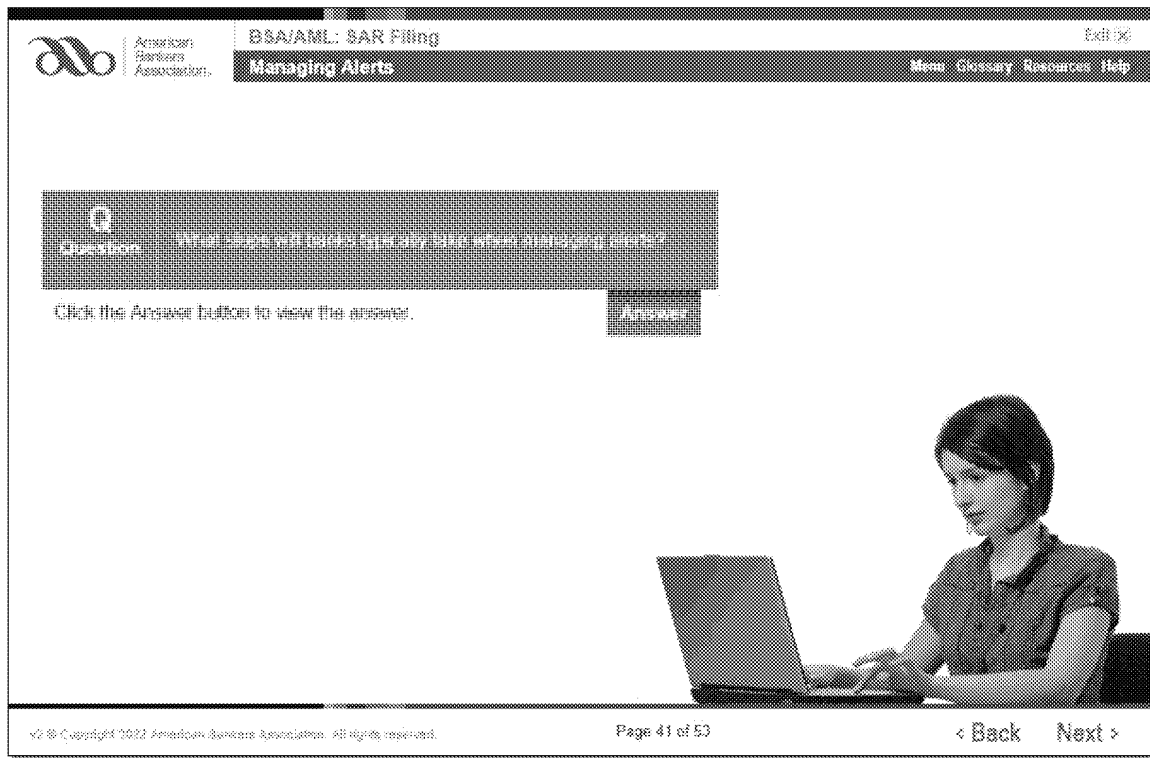
© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 40 of 53 < Back Next >

Managing Alerts

The bank should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the bank's overall risk profile and the volume of transactions.

Additionally, a bank should ensure that the assigned staff are experienced and provided with comprehensive and ongoing training to maintain their expertise. The bank should provide staff with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

After thorough research and analysis, investigators should document conclusions, including any recommendation regarding whether or not to file a SAR. When multiple departments are responsible for researching unusual activities (for example, when the bank's BSA department researches BSA-related activity and the bank's fraud department researches fraud-related activity), the lines of communication between the departments must remain open. This ensures that the bank identifies, evaluates, and reports all suspicious activity.



BSA/AML: SAR Filing
Managing Alerts

Home Glossary Resources Help

Question: What steps will banks typically take when managing alerts?

Click the Answer button to view the answer.

Answer

© Copyright 2022 American Bankers Association. All rights reserved. Page 41 of 53 < Back Next >

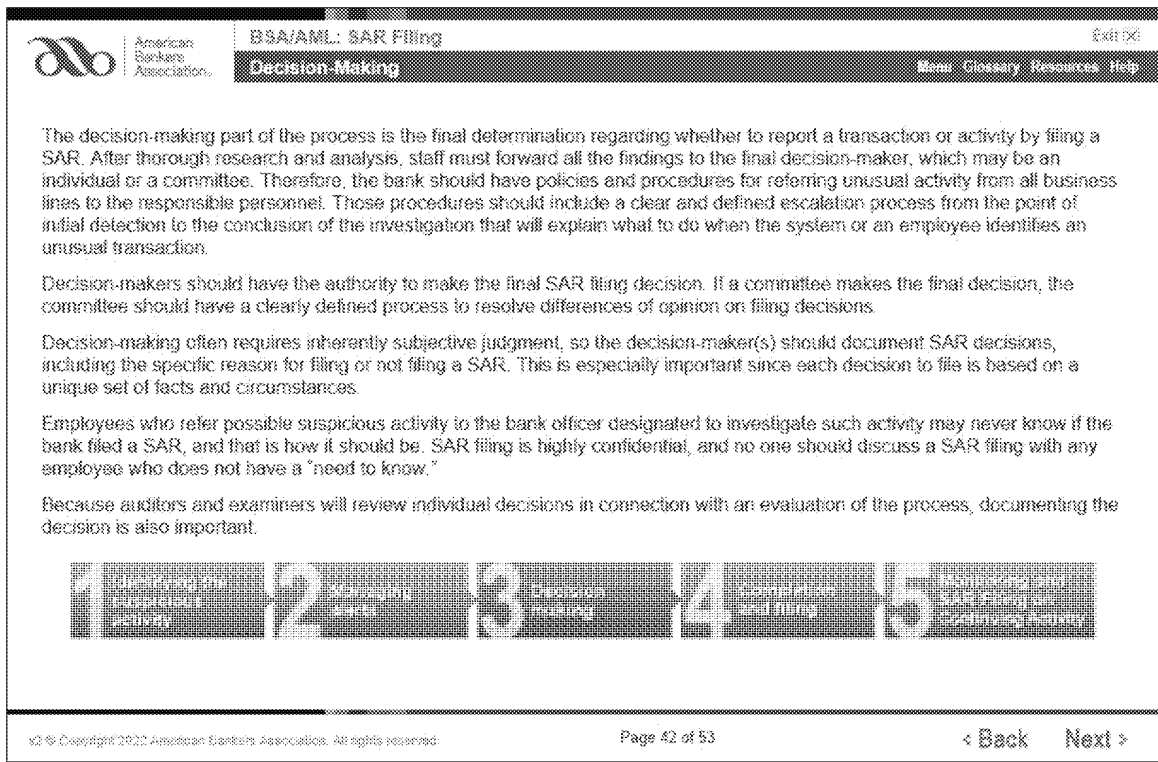
Managing Alerts

Question: What steps will banks typically take when managing alerts?

Answer:

- Have policies and procedures in place for referring unusual activity from all areas of the bank or business lines to the personnel responsible for evaluation and reporting
- Establish clear and defined escalation processes from the point of initial detection to the conclusion of the investigation
- Assign adequate staff to identify, evaluate, and report potentially suspicious activities

Page 41



The decision-making part of the process is the final determination regarding whether to report a transaction or activity by filing a SAR. After thorough research and analysis, staff must forward all the findings to the final decision-maker, which may be an individual or a committee. Therefore, the bank should have policies and procedures for referring unusual activity from all business lines to the responsible personnel. Those procedures should include a clear and defined escalation process from the point of initial detection to the conclusion of the investigation that will explain what to do when the system or an employee identifies an unusual transaction.

Decision-makers should have the authority to make the final SAR filing decision. If a committee makes the final decision, the committee should have a clearly defined process to resolve differences of opinion on filing decisions.

Decision-making often requires inherently subjective judgment, so the decision-maker(s) should document SAR decisions, including the specific reason for filing or not filing a SAR. This is especially important since each decision to file is based on a unique set of facts and circumstances.

Employees who refer possible suspicious activity to the bank officer designated to investigate such activity may never know if the bank filed a SAR, and that is how it should be. SAR filing is highly confidential, and no one should discuss a SAR filing with any employee who does not have a "need to know."

Because auditors and examiners will review individual decisions in connection with an evaluation of the process, documenting the decision is also important.

1. Identify suspicious activity
2. Escalate to the responsible personnel
3. Conduct investigation
4. Document findings
5. Document final decision and reporting history

© 2022 Copyright 2022 American Bankers Association. All rights reserved. Page 42 of 53 < Back Next >

Decision-Making

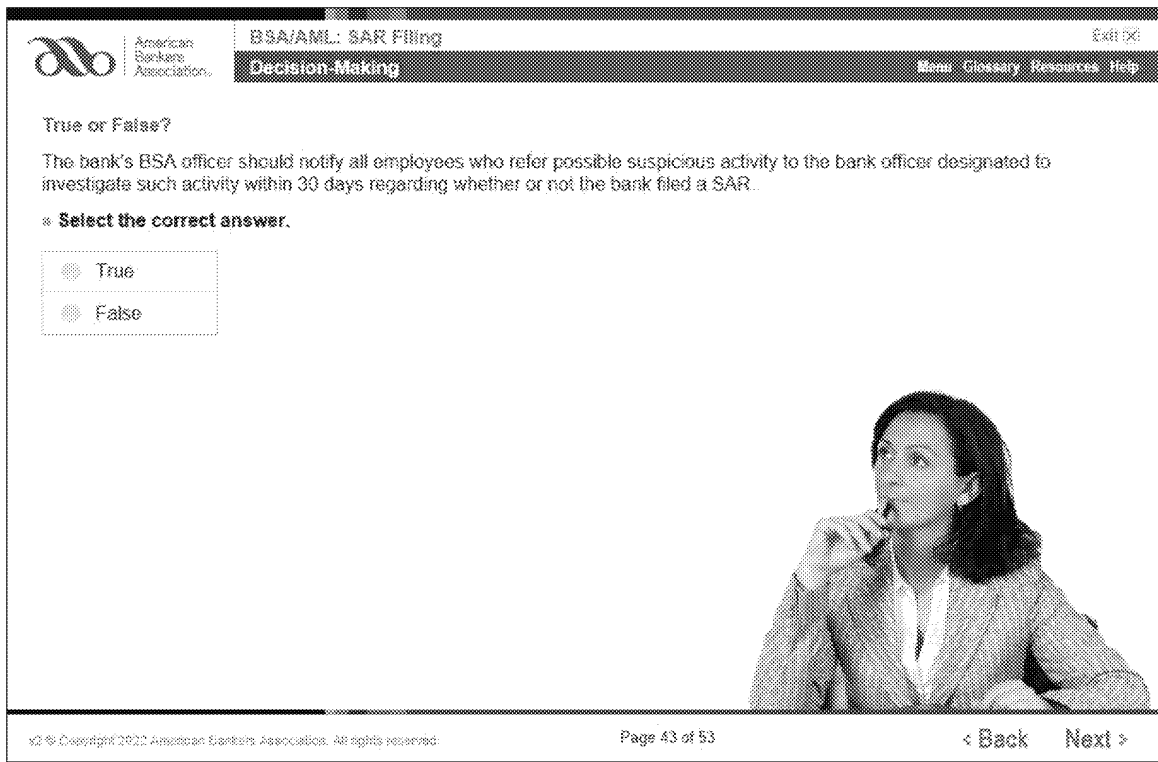
The decision-making part of the process is the final determination regarding whether to report a transaction or activity by filing a SAR. After thorough research and analysis, staff must forward all the findings to the final decision-maker, which may be an individual or a committee. Therefore, the bank should have policies and procedures for referring unusual activity from all business lines to the responsible personnel. Those procedures should include a clear and defined escalation process from the point of initial detection to the conclusion of the investigation that will explain what to do when the system or an employee identifies an unusual transaction.

Decision-makers should have the authority to make the final SAR filing decision. If a committee makes the final decision, the committee should have a clearly defined process to resolve differences of opinion on filing decisions.

Decision-making often requires inherently subjective judgment, so the decision-maker(s) should document SAR decisions, including the specific reason for filing or not filing a SAR. This is especially important since each decision to file is based on a unique set of facts and circumstances.

Employees who refer possible suspicious activity to the bank officer designated to investigate such activity may never know if the bank filed a SAR, and that is how it should be. SAR filing is highly confidential, and no one should discuss a SAR filing with any employee who does not have a "need to know."

Because auditors and examiners will review individual decisions in connection with an evaluation of the process, documenting the decision is also important.



BSA/AML: SAR Filing

Decision-Making

True or False?

The bank's BSA officer should notify all employees who refer possible suspicious activity to the bank officer designated to investigate such activity within 30 days regarding whether or not the bank filed a SAR.

» Select the correct answer.

True

False

< Back Next >

Page 43 of 53

© 2022 Copyright 2022 American Bankers Association. All rights reserved.

Decision-Making

True or False?

The bank's BSA officer should notify all employees who refer possible suspicious activity to the bank officer designated to investigate such activity within 30 days regarding whether or not the bank filed a SAR.

» Select the correct answer.

True

False

The statement is false. Employees who refer possible suspicious activity to the bank officer designated to investigate such activity may never know if the bank filed a SAR. SAR filing is highly confidential, and employees responsible for SAR decision-making should not discuss SAR filing with any employee who does not have a "need to know."

Page 43

Completing the SAR
Banks must electronically file all BSA-required reports, including SARs, with the FinCEN BSA E-Filing System. Banks should provide the most complete filing information available regardless of whether or not the individual fields are critical (required) for technical filing purposes.

Although the bank must complete the basic information fields on a SAR, the SAR contains an area known as the *SAR Narrative*. This part of the SAR tells the story so that law enforcement can understand what led the bank to believe the activity was suspicious. Law enforcement agencies rely on this information to assist in money laundering, terrorist financing, and financial crimes investigations. The SAR Narrative should include enough information to clearly explain who was involved, what took place, when and where the activity happened, and why the bank believes the transaction was suspicious.

Remember, when completing the SAR Narrative, the law enforcement representatives who read the SAR will not be familiar with bank-specific product names or banking buzzwords. When completing the SAR, or providing a written explanation of the activity, ensure that any novel or proprietary terms are described in detail so they are well-defined.

» Click the EZ Reference button to view or download a sample SAR.

[EZ Reference](#)

- 1 Introduction
- 2 SAR Narrative
- 3 SAR Reporting
- 4 Reporting Details
- 5 Reporting Activity

© 7/2022 American Bankers Association. All rights reserved. Page 44 of 53 < Back Next >

Completion and Filing

Completing the SAR

Banks must electronically file all BSA-required reports, including SARs, with the FinCEN BSA E-Filing System. Banks should provide the most complete filing information available regardless of whether or not the individual fields are critical (required) for technical filing purposes.

Although the bank must complete the basic information fields on a SAR, the SAR contains an area known as the *SAR Narrative*. This part of the SAR tells the story so that law enforcement can understand what led the bank to believe the activity was suspicious. Law enforcement agencies rely on this information to assist in money laundering, terrorist financing, and financial crimes investigations. The SAR Narrative should include enough information to clearly explain who was involved, what took place, when and where the activity happened, and why the bank believes the transaction was suspicious.

Remember, when completing the SAR Narrative, the law enforcement representatives who read the SAR will not be familiar with bank-specific product names or banking buzzwords. When completing the SAR, or providing a written explanation of the activity, ensure that any novel or proprietary terms are described in detail so they are well-defined.

» Click the EZ Reference button to view or download a sample SAR.

Sidebar:

SAR Narrative information

Filers may attach a small file and must describe the contents of that file in the SAR Narrative. Filers may not include any other supporting documentation with the FinCEN SAR. Instead, they should use the SAR Narrative to describe the other supporting documentation not included in the file. This supporting documentation, such as copies of instruments; receipts; sale, transaction, or clearing records; photographs; and surveillance (audio or video recordings) must be made available to appropriate authorities upon request.

Filers must retain all supporting documentation or a business record equivalent for 5 years from the date of the report. Banks may also submit an Excel spreadsheet with detailed information about specific transactions and funds transfers or other analytics. The new addition also states these Excel spreadsheets are considered part of the narrative but do not take the place of the narrative ("narratives should not simply state 'see attachment'"). Finally, as part of the SAR filing, banks should treat any supplemental material filed on an Excel spreadsheet with the SAR as confidential.

Page 44

Any failure to describe adequately the factors that make the activity suspicious undermines the very purpose of the SAR and lessens its usefulness to law enforcement. The goal is to tell law enforcement what happened and why the bank thinks there is something suspicious about what took place.

» Roll over each button to see examples of questions that each bank employee should consider when determining the necessary information for reporting possible suspicious activity to the appropriate person at the bank. This information provides the basis for the SAR Narrative.

Who? What? When? Where? Why? How?

WARNING

Consideration of the appropriate person to report suspicious activity is the responsibility of the bank employee. Failure to report suspicious activity to the appropriate person at the bank may result in disciplinary action. The bank employee should report suspicious activity to the appropriate person at the bank. If you are not the appropriate person, please contact your supervisor.

© 7/2022 American Bankers Association. All rights reserved. Page 45 of 53 < Back Next >

Completion and Filing

Any failure to describe adequately the factors that make the activity suspicious undermines the very purpose of the SAR and lessens its usefulness to law enforcement. The goal is to tell law enforcement what happened and why the bank thinks there is something suspicious about what took place.

» Roll over each button to see examples of questions that each bank employee should consider when determining the necessary information for reporting possible suspicious activity to the appropriate person at the bank. This information provides the basis for the SAR Narrative.

Who is conducting the activity? This includes names of businesses or individuals as well as other relevant facts about those individuals, which are all important pieces of the information provided on a SAR. These may include the following facts:

- Employer and occupation information
- Relationship between the suspect and the bank
- Length of the financial relationship between the subject and the bank

What instruments or mechanisms did the suspected criminal use in the suspicious transactions? Examples include the following:

- Fraudulent documents
- Cash deposits/withdrawals
- Wires or other electronic transactions
- Stocks, bonds, or notes
- Loans

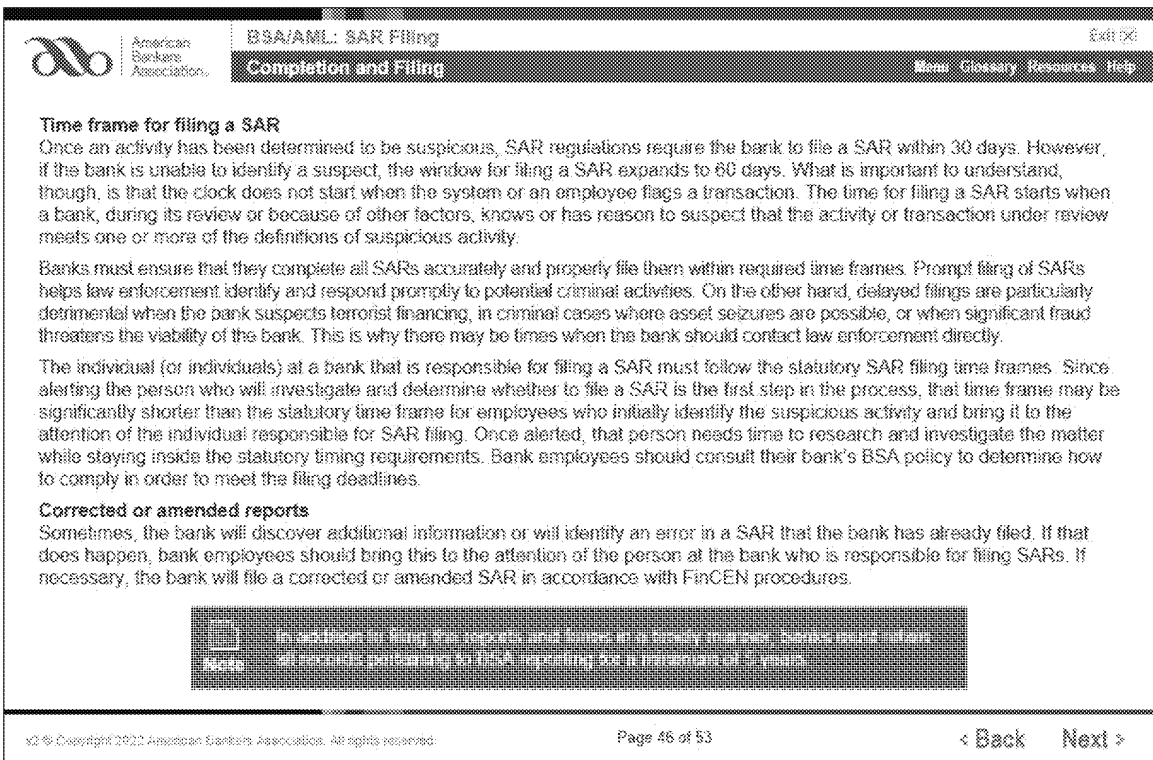
When did the suspicious activity take place? It helps to identify all accounts and transactions that were involved in chronological order by date and amount.

Where did the suspicious activity take place? Identify the branch, department, or other locations where the activity occurred by name and street address.

Why does the SAR filer think the activity is suspicious? Describe concisely, but fully, why the bank believes the transactions are suspicious.

How did the suspicious activity occur? Describe how the suspect transactions or patterns of transactions were completed. For account activity, provide as completely as possible an explanation of the cycle of funds, including the source of the funds and the application of those funds.

Warning: Sometimes, it is important to alert law enforcement about a transaction or activity immediately, before the bank files a SAR. If a bank thinks that may be necessary, bank procedures will explain who to alert and how. It may be an immediate supervisor, or it may be the bank's BSA officer, but the bank will have procedures in place on what steps to take.



The screenshot shows a web page with the following content:

Time frame for filing a SAR
 Once an activity has been determined to be suspicious, SAR regulations require the bank to file a SAR within 30 days. However, if the bank is unable to identify a suspect, the window for filing a SAR expands to 60 days. What is important to understand, though, is that the clock does not start when the system or an employee flags a transaction. The time for filing a SAR starts when a bank, during its review or because of other factors, knows or has reason to suspect that the activity or transaction under review meets one or more of the definitions of suspicious activity.

Banks must ensure that they complete all SARs accurately and properly file them within required time frames. Prompt filing of SARs helps law enforcement identify and respond promptly to potential criminal activities. On the other hand, delayed filings are particularly detrimental when the bank suspects terrorist financing, in criminal cases where asset seizures are possible, or when significant fraud threatens the viability of the bank. This is why there may be times when the bank should contact law enforcement directly.

The individual (or individuals) at a bank that is responsible for filing a SAR must follow the statutory SAR filing time frames. Since alerting the person who will investigate and determine whether to file a SAR is the first step in the process, that time frame may be significantly shorter than the statutory time frame for employees who initially identify the suspicious activity and bring it to the attention of the individual responsible for SAR filing. Once alerted, that person needs time to research and investigate the matter while staying inside the statutory timing requirements. Bank employees should consult their bank's BSA policy to determine how to comply in order to meet the filing deadlines.

Corrected or amended reports
 Sometimes, the bank will discover additional information or will identify an error in a SAR that the bank has already filed. If that does happen, bank employees should bring this to the attention of the person at the bank who is responsible for filing SARs. If necessary, the bank will file a corrected or amended SAR in accordance with FinCEN procedures.

Note: In addition to filing the reports and forms in a timely manner, banks must retain all records pertaining to BSA reporting for a minimum of 5 years.

Page 46 of 53

Completion and Filing

Time frame for filing a SAR

Once an activity has been determined to be suspicious, SAR regulations require the bank to file a SAR within 30 days. However, if the bank is unable to identify a suspect, the window for filing a SAR expands to 60 days. What is important to understand, though, is that the clock does not start when the system or an employee flags a transaction. The time for filing a SAR starts when a bank, during its review or because of other factors, knows or has reason to suspect that the activity or transaction under review meets one or more of the definitions of suspicious activity.

Banks must ensure that they complete all SARs accurately and properly file them within required time frames. Prompt filing of SARs helps law enforcement identify and respond promptly to potential criminal activities. On the other hand, delayed filings are particularly detrimental when the bank suspects terrorist financing, in criminal cases where asset seizures are possible, or when significant fraud threatens the viability of the bank. This is why there may be times when the bank should contact law enforcement directly.

The individual (or individuals) at a bank that is responsible for filing a SAR must follow the statutory SAR filing time frames. Since alerting the person who will investigate and determine whether to file a SAR is the first step in the process, that time frame may be significantly shorter than the statutory time frame for employees who initially identify the suspicious activity and bring it to the attention of the individual responsible for SAR filing. Once alerted, that person needs time to research and investigate the matter while staying inside the statutory timing requirements. Bank employees should consult their bank's BSA policy to determine how to comply in order to meet the filing deadlines.

Corrected or amended reports

Sometimes, the bank will discover additional information or will identify an error in a SAR that the bank has already filed. If that does happen, bank employees should bring this to the attention of the person at the bank who is responsible for filing SARs. If necessary, the bank will file a corrected or amended SAR in accordance with FinCEN procedures.

Note: In addition to filing the reports and forms in a timely manner, banks must retain all records pertaining to BSA reporting for a minimum of 5 years.

Requests by law enforcement to review documentation

There are times when law enforcement will want to review the documentation that forms the basis for filing the SAR, such as transaction records or account statements. A bank can provide SAR backup information and related information about the subject of the report to an authorized law enforcement official, but there are procedures that most banks will have to follow before helping the law enforcement representative with their inquiry.

If law enforcement approaches a bank employee requesting follow-up information about suspicious activity that the bank reported, employees should refer the matter to the bank's BSA officer for coordination. If a law enforcement agent asks for information, explain that the appropriate officer at the bank must handle the request since that individual has all the necessary information and can provide it in the right way.

It is also important to understand that law enforcement is entitled only to the records that are included in the backup documentation specific to the SAR. Any request for information that falls outside of the SAR may require the law enforcement agency to follow a state or federal legal process.


Completion and Filing

Requests by law enforcement to review documentation

There are times when law enforcement will want to review the documentation that forms the basis for filing the SAR, such as transaction records or account statements. A bank can provide SAR backup information and related information about the subject of the report to an authorized law enforcement official, but there are procedures that most banks will have to follow before helping the law enforcement representative with their inquiry.


If law enforcement approaches a bank employee requesting follow-up information about suspicious activity that the bank reported, employees should refer the matter to the bank's BSA officer for coordination. If a law enforcement agent asks for information, explain that the appropriate officer at the bank must handle the request since that individual has all the necessary information and can provide it in the right way.

It is also important to understand that law enforcement is entitled only to the records that are included in the backup documentation specific to the SAR. Any request for information that falls outside of the SAR may require the law enforcement agency to follow a state or federal legal process.



BSA/AML: SAR Filing

Completion and Filing

Exit 

Menu Gallery Resources Help

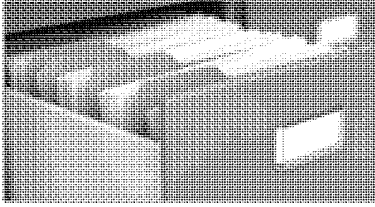
Closing an account

A bank may use its reasonable business judgment to decide whether to close an account after it has made a SAR filing. It would be prudent for a bank to implement additional monitoring of an account that is the subject of a SAR filing, particularly if numerous SAR filings are involved. The bank will make the ultimate decision to maintain or close an account in accordance with its own standards and guidelines.

There are times, however, when a bank has an account with suspicious or potential criminal activity and law enforcement requests that the bank keep the account open. Banks should ask for a written request from the law enforcement agency. A supervisory agent or an attorney should issue this request within a U.S. Attorney's Office or another office of the Department of Justice.

If the request comes from a state or local law enforcement agency, the request should be from a supervisor of the state or local law enforcement agency or from an attorney within a state or local prosecutor's office. The request should indicate that the agency requested that the bank maintain the account and the purpose of the request. The request should also indicate the duration of the request, not to exceed 6 months (law enforcement may issue a subsequent request for a longer duration).

Although the BSA does not have a recordkeeping requirement with respect to these requests, FinCEN advises banks to maintain the request for at least 5 years after it has expired.



© 2022 Copyright 2022 American Bankers Association. All rights reserved.

Page 48 of 53

< Back Next >

Completion and Filing

Closing an account

A bank may use its reasonable business judgment to decide whether to close an account after it has made a SAR filing. It would be prudent for a bank to implement additional monitoring of an account that is the subject of a SAR filing, particularly if numerous SAR filings are involved. The bank will make the ultimate decision to maintain or close an account in accordance with its own standards and guidelines.

There are times, however, when a bank has an account with suspicious or potential criminal activity and law enforcement requests that the bank keep the account open. Banks should ask for a written request from the law enforcement agency. A supervisory agent or an attorney should issue this request within a U.S. Attorney's Office or another office of the Department of Justice.

If the request comes from a state or local law enforcement agency, the request should be from a supervisor of the state or local law enforcement agency or from an attorney within a state or local prosecutor's office. The request should indicate that the agency requested that the bank maintain the account and the purpose of the request. The request should also indicate the duration of the request, not to exceed 6 months (law enforcement may issue a subsequent request for a longer duration).

Although the BSA does not have a recordkeeping requirement with respect to these requests, FinCEN advises banks to maintain the request for at least 5 years after it has expired.

BSA/AML: SAR Filing
Completion and Filing

Self-Check Quiz

In addition to filing the reports and forms in a timely manner, how long must banks retain records pertaining to BSA reporting?

» Select the correct answer and click Submit.

A) Minimum of 3 years

B) Minimum of 5 years

C) Minimum of 7 years

D) Minimum of 10 years

Submit Try Again

© 7/2022 American Bankers Association. All rights reserved. Page 49 of 53 < Back Next >

Completion and Filing

Self-Check Quiz

In addition to filing the reports and forms in a timely manner, how long must banks retain records pertaining to BSA reporting?

» Select the correct answer and click Submit.

- A) Minimum of 3 years
- B) Minimum of 5 years
- C) Minimum of 7 years
- D) Minimum of 10 years

B is correct.

A, C, and D are incorrect because banks must retain all records pertaining to BSA reporting for a minimum of 5 years.

Page 49

BSA/AML: SAR Filing Exit X

Monitoring and SAR Filing on Continuing Activity Home Contact Resources Help

SAR filing on continuing activity

There are times when an activity will continue after the bank has filed a SAR. If the activity continues, the bank must bring this to the attention of law enforcement. FinCEN guidelines suggest that banks should report activity on a regular basis, a process that also helps the bank monitor for potential problems. As a result, banks should have policies and procedures about when to escalate issues or problems identified as the result of repeat SAR filings on accounts.

These procedures should include the following elements:

- A review by senior management and legal staff (e.g., a BSA compliance officer or a SAR committee)
- Criteria for when an analysis of the overall customer relationship is necessary
- Criteria for whether to close the account and, if so, when
- Criteria for when to notify law enforcement

When filing SARs on continuing activity, the generally accepted threshold is to review an activity 90 days after the most recent SAR with a goal for filing the next SAR 120 days after the most recently filed SAR.

1. Introduction	2. Monitoring	3. Reporting	4. Compliance and Ethics	5. Monitoring and SAR Filing on Continuing Activity
-----------------	---------------	--------------	--------------------------	---

© Copyright 2022 American Bankers Association. All rights reserved. Page 50 of 53 < Back Next >

Monitoring and SAR Filing on Continuing Activity

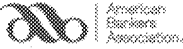
SAR filing on continuing activity

There are times when an activity will continue after the bank has filed a SAR. If the activity continues, the bank must bring this to the attention of law enforcement. FinCEN guidelines suggest that banks should report activity on a regular basis, a process that also helps the bank monitor for potential problems. As a result, banks should have policies and procedures about when to escalate issues or problems identified as the result of repeat SAR filings on accounts.

These procedures should include the following elements:

- A review by senior management and legal staff (e.g., a BSA compliance officer or a SAR committee)
- Criteria for when an analysis of the overall customer relationship is necessary
- Criteria for whether to close the account and, if so, when
- Criteria for when to notify law enforcement

When filing SARs on continuing activity, the generally accepted threshold is to review an activity 90 days after the most recent SAR with a goal for filing the next SAR 120 days after the most recently filed SAR.



BSA/AML: SAR Filing

Monitoring and SAR Filing on Continuing Activity

Exit X

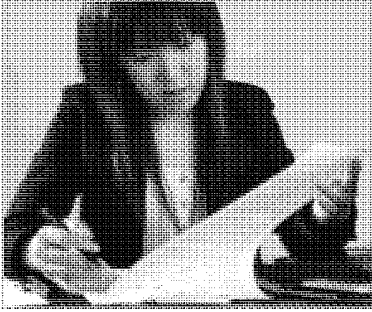
Menu Glossary Resources Help

SAR filing on continuing activity, continued

What is most helpful for law enforcement is to report the range of activity that the bank has reviewed. When a bank files an ongoing SAR, law enforcement would like two specific bits of information (that way they know what has been covered).

In Field 27 of the SAR, what they would like are the dates for the review for that particular SAR. In other words, the bank would enter the full 90-day range of activity that it has reviewed. Meanwhile, in the SAR, what law enforcement would also like to see is information about the full scope of the activity.

For example, a bank is filing a report on suspicious activity from March 22, 2022, through June 22, 2022. The bank would enter those dates on the SAR that it is filing. *However*, if the activity that prompted the original SAR occurred in December 2021, the bank should note that in the narrative, along with a reference number or something to connect this SAR with the prior SARs. That makes law enforcement's task easier.



v1 © CopyRight 2022 American Bankers Association. All rights reserved.

Page 51 of 53

< Back Next >

Monitoring and SAR Filing on Continuing Activity

SAR filing on continuing activity, continued

What is most helpful for law enforcement is to report the range of activity that the bank has reviewed. When a bank files an ongoing SAR, law enforcement would like two specific bits of information (that way they know what has been covered).

In Field 27 of the SAR, what they would like are the dates for the review for that particular SAR. In other words, the bank would enter the full 90-day range of activity that it has reviewed. Meanwhile, in the SAR, what law enforcement would also like to see is information about the full scope of the activity.

For example, a bank is filing a report on suspicious activity from March 22, 2022, through June 22, 2022. The bank would enter those dates on the SAR that it is filing. *However*, if the activity that prompted the original SAR occurred in December 2021, the bank should note that in the narrative, along with a reference number or something to connect this SAR with the prior SARs. That makes law enforcement's task easier.

The screenshot shows a web-based quiz interface. At the top left is the American Bankers Association logo. The page title is "BSA/AML: SAR Filing" and the subtitle is "Monitoring and SAR Filing on Continuing Activity". A navigation menu includes "Home", "Glossary", "Resources", and "Help". The main content area contains a question box with a question icon and the text: "When filing SARs on continuing activity, what is the threshold for reviewing the subject activity?". Below the question box is an "Answer" button and the instruction "Click the Answer button to view the answer:". On the left side of the page, there is a photograph of a man in a suit, looking thoughtful with his hand on his chin. At the bottom of the page, there is a footer with copyright information: "© 2022 Copyright 2022 American Bankers Association. All rights reserved.", the page number "Page 52 of 53", and navigation buttons "< Back" and "Next >".

Monitoring and SAR Filing on Continuing Activity

Question: When filing SARs on continuing activity, what is the threshold for reviewing the subject activity?

Answer: The generally accepted threshold is to review an activity 90 days after the most recent SAR with a goal for filing the next SAR 120 days after the most recently filed SAR.

Page 52

By completing *BSA/AML: SAR Filing*, you learned about the scope of activities appropriate for SAR filing and the importance of keeping SARs confidential. You also learned about indicators of suspicious activity and the five key components of SAR filing.

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Knowing the controls, due diligence techniques, and red flags is not necessarily enough to ensure that a bank is effectively monitoring for, and reporting on, suspicious activity. A control breakdown commonly noted by examiners is ineffective or inefficient reporting of suspicious activity by bank personnel. Therefore, all bank staff should be educated about what to look for and should be equally educated on how to report suspicious activity within the bank. This helps to ensure a seamless process that eventually results in documentation supporting why certain activities are not suspicious or why a SAR is filed.

» **Click Exit to close this course.**

Suspicious Activity Report
Form # SAR-1000-0000

Item # 1000000

1 2 3 4 5

Filing name:

© 7/2022 American Bankers Association. All rights reserved. Page 53 of 53 < Back Next >

Wrap-Up

By completing *BSA/AML: SAR Filing*, you learned about the scope of activities appropriate for SAR filing and the importance of keeping SARs confidential. You also learned about indicators of suspicious activity and the five key components of SAR filing.

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Knowing the controls, due diligence techniques, and red flags is not necessarily enough to ensure that a bank is effectively monitoring for, and reporting on, suspicious activity. A control breakdown commonly noted by examiners is ineffective or inefficient reporting of suspicious activity by bank personnel. Therefore, all bank staff should be educated about what to look for and should be equally educated on how to report suspicious activity within the bank. This helps to ensure a seamless process that eventually results in documentation supporting why certain activities are not suspicious or why a SAR is filed.

» **Click Exit to close this course.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

COMMITTEE ON THE JUDICIARY,
U.S. HOUSE OF REPRESENTATIVES,
WASHINGTON, D.C.

INTERVIEW OF: [REDACTED]

Tuesday, May 14, 2024

Los Angeles, CA

The interview in the above matter was held in Wilshire Federal Building, Suite 521,
commencing at 9:53 a.m. PST.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Appearances:

For the COMMITTEE ON THE JUDICIARY:

- [REDACTED] DIGITAL ASSISTANT
- [REDACTED] COUNSEL
- [REDACTED] SPECIAL COUNSEL
- [REDACTED] DEPUTY CHIEF COUNSEL FOR OVERSIGHT

For the SUBCOMMITTEE ON CRIME AND
FEDERAL GOVERNMENT SURVEILLANCE:

- [REDACTED] MINORITY DETAILEE

For the U.S. DEPARTMENT OF TREASURY:

- [REDACTED]
- [REDACTED]

1 [REDACTED] This is a transcribed interview of [REDACTED] Chairman Jordan has
2 requested this interview as part of the committee's oversight of the Department of
3 Treasury's Financial Crimes Enforcement Network.

4 Would the witness please state your name for the record?

5 [REDACTED] [REDACTED]

6 [REDACTED] Could agency counsel please state your name for the record?

7 [REDACTED] [REDACTED]

8 [REDACTED] [REDACTED]

9 [REDACTED] On behalf of the committee, I want to thank you for appearing here
10 today to answer our questions. The chairman also appreciates your willingness to
11 appear voluntarily.

12 My name is [REDACTED] I'm with Chairman Jordan's staff. I'll now have everyone
13 else from the committee who is here in the room introduce themselves as well.

14 [REDACTED] [REDACTED] with Chairman Jordan.

15 [REDACTED] [REDACTED] with Chairman Jordan.

16 [REDACTED] [REDACTED] Chairman Jordan.

17 [REDACTED] [REDACTED] with Ranking Member Nadler.

18 [REDACTED] I would like to now go over the ground rules and guidelines that will
19 be followed during today's interview.

20 Our questioning will proceed in rounds. The majority will ask questions first for 1
21 hour, and then the minority will have an opportunity to ask questions for an equal period
22 of time if they choose. We will alternate back and forth until there are no more
23 questions and the interview is over. Typically, we take a short break at the end of each
24 hour, but if you'd like to take a break apart from that, please just let us know.

25 As you can see, there is an official court reporter taking down everything we say to

1 make a written record, so we ask that you give verbal responses to all questions. Do you
2 understand?

3 [REDACTED] Yes.

4 [REDACTED] So the court reporter can take down a clear record, we will do our best
5 to limit the number of people directing questions at you during any given hour to just
6 those people on the staff whose turn it is. Please try and speak clearly so the court
7 reporter can understand and so the folks down at the end of the table can hear you.

8 It's important that we don't talk over one another or interrupt each other if we
9 can help it, and that goes to everybody present at today's interview.

10 We want you to answer our questions in the most complete and truthful manner
11 as possible, so we will take our time. If you have any questions or if you do not
12 understand one of our questions, please let us know.

13 Our questions will cover a wide range of topics, so if you need clarification at any
14 point, just say so. If you honestly don't know the answer to a question or do not
15 remember, it is best not to guess. Please give us your best recollection, and it's okay to
16 tell us if you learned information from someone else, just indicate how you came to know
17 the information. If there are things you don't know or can't remember, just say so, and
18 please inform us who, to the best of your knowledge, might be able to provide a more
19 complete answer to the question.

20 You should understand that although this interview is not under oath, that by law
21 you are required to answer questions from Congress truthfully. Do you understand
22 that?

23 [REDACTED] Yes.

24 [REDACTED] This also applies to questions posed by congressional staff in an
25 interview. Do you understand this?

1 [REDACTED] Yes.

2 [REDACTED] Witnesses that knowingly provide false testimony could be subject to
3 criminal prosecution for perjury or for making false statements under 18 U.S.C. Section
4 1001. Do you understand this?

5 [REDACTED] Yes.

6 [REDACTED] Is there any reason that you are unable to provide truthful answers to
7 today's questions?

8 [REDACTED] No.

9 [REDACTED] Finally, I'd like to make a note that the content of what we discuss
10 here today is confidential. We ask that you not speak about what we discuss in this
11 interview to any outside individuals to preserve the integrity of our investigation.

12 For the same reason, the marked exhibits that we will use today will remain with
13 the court reporter so that they can go in the official transcript. Any copies of those
14 exhibits will be returned to us when we wrap up.

15 That is the end of my reamble. Is there anything that my colleagues from the
16 minority would like to add?

17 [REDACTED] No, we'd just like to thank you for being here today.

18 [REDACTED] Counsel?

19 [REDACTED] Yes. Before we get started, I just wanted to put on the record
20 that some of the topics here today that I understand the committee is investigating touch
21 on the Bank Secrecy Act and potentially suspicious activity reports filed under the Bank
22 Secrecy Act.

23 The Bank Secrecy Act, which is 31 U.S.C. 5318(g), in particular, provides that
24 suspicious activity reports or anything that reveals the existence of a suspicious activity
25 report is confidential. Unauthorized disclosure of this material to the public is subject to

1 civil and criminal penalties. Unauthorized disclosure of this type of information is
2 also -- potentially can compromise the national security of the United States or active and
3 ongoing law enforcement investigations.

4 The Department of Treasury would respectfully ask that the committee, in
5 handling of the transcript of any matters discussed here today, to the extent they pertain
6 to specific SAR filings or anything that would disclose the existence of a particular SAR,
7 that that be redacted and not put in the public record.

8 We would also like to respectfully request -- as you all know, [REDACTED] is a
9 former Treasury employee. He's here voluntarily. We would really request that the
10 committee use all of its discretion in not releasing information about [REDACTED] not
11 releasing his name further into the public. He's no longer a government employee. He
12 was never an SES-level employee. So we would just like to respectfully make that
13 request on the record and again reiterate that he is here voluntarily to speak about
14 matters that are in the scope of his employment while at the Department of Treasury.

15 [REDACTED] Thank you.

16 [REDACTED] Thank you.

17 The clock now reads 9:58. We will start the first hour of questioning.

18 EXAMINATION

19 BY [REDACTED]

20 Q [REDACTED] what do you currently do for work?

21 A I'm an anti-money laundering compliance professional.

22 Q And how long have you been in that position?

23 A My current role or in that industry?

24 Q In your current role.

25 A About 6 months.

1 Q And with what company is that?

2 A Plaid.

3 Q And when did you join -- first join the Financial Crimes Enforcement
4 Network?

5 A I believe it was around November 2018.

6 Q And why did you join FinCEN?

7 A Oh, gosh. I had been in the private sector and worked with a lot of former
8 government and law enforcement officials and always found myself very motivated by
9 their service. So it was always something that I was interested in, you know, serving the
10 country in some way. And also, it was a great career opportunity, you know, getting
11 that government service in my industry.

12 Q And prior to joining FinCEN, what other positions did you hold?

13 A Sure. I was an AML compliance professional at a financial institution. And
14 then prior to that, I was an attorney in private practice.

15 Q And which financial institution was that?

16 A Standard Chartered Bank.

17 Q And what was your position in January of 2021?

18 A In January of 2021 -- let me think. November 18th through the beginning
19 of 2020. So in January 2021, I was the director of the Office of Stakeholder Integration
20 and Engagement for FinCEN.

21 Q And how long were you in that role?

22 A I was in that role about 2 years. Well, technically three. The third of
23 those 3 years I was acting deputy -- what do they call them -- deputy associate director of
24 the Strategic Operations Division. So, formally, same role but acting in a different
25 capacity.

1 Q And in those roles, can you describe what your responsibilities were in those
2 positions?

3 A Sure. I had two sections in that office. One was the data access and
4 management section, which oversees law enforcement and other, you know, intelligence,
5 other agencies that have access to the BSA data that FinCEN holds. So that section
6 oversaw the memoranda of understanding that we have in place with those
7 agencies -- we, being FinCEN, had in place with those agencies -- periodic audits of the
8 usage, et cetera, things of that nature.

9 And then my other section was called the domestic engagement section. That
10 section was responsible for liaising with external stakeholders of FinCEN, so law
11 enforcement, private sector, other regulators, things of that nature.

12 Q And can you describe -- to the extent that you already touched on that, can
13 you describe the organizational structure of those divisions within FinCEN?

14 A All or the strategic operations?

15 [REDACTED] It may help if he gives you his -- if he could just chronologically
16 give you his roles at FinCEN because he had a couple of different ones. So that may --

17 [REDACTED] Sure.

18 [REDACTED] -- answer your question a little more clearly.

19 [REDACTED] Yeah, I'll do that and sort of give you -- so FinCEN has seven -- well,
20 when I was there, FinCEN had seven divisions, plus counsel. One of the -- my first role at
21 FinCEN was with the Policy Division as the director of regulatory policy, and I did that for
22 about a year.

23 FinCEN has the front office, director, deputy director, et cetera. There is the
24 divisions. Each division has one or more offices, and then most or all -- most offices
25 have one or more sections, and then there is staff underneath all of those various

1 leadership and hierarchical roles.

2 So I started off as an office director in the Policy Division. Did that for a little over
3 a year, moved over to the role that I just mentioned, as the director of the Office of
4 Stakeholder Integration and Engagement. Did that for about 2 years.

5 My last year at FinCEN remained technically in that role but served as acting
6 deputy head of the Strategic Operations Division, which was the same division in which
7 my office was. And -- yeah, so --

8 [REDACTED] It may be helpful to just explain like what the Strategic
9 Operations Division did so you can explain your responsibilities in that office.

10 [REDACTED] Sure. The Strategic Operation Division did a lot of things. One of
11 its offices was in charge, for example, of foreign engagement. So our work with other
12 countries' financial intelligence units, some of our work at the FATF.

13 [REDACTED] Sorry. The what?

14 [REDACTED] Sorry, the Financial Action Task Force.

15 [REDACTED] Thank you.

16 [REDACTED] Yep.

17 [REDACTED] Don't quote me on that but close enough.

18 And so that was sort of the foreign engagement office.

19 I'm sure I'm going to miss things here, but -- and then other components -- a lot of
20 it really has to do with overall liaising with our external stakeholders. So you had the
21 office that handled the foreign, and then you had the office that handled, I guess, for lack
22 of a better way of saying it, customer support. So we have a phone -- FinCEN had a
23 phone help line and some filing, technical issues, things of that nature. So that was one
24 office.

25 And then there was the office that I oversaw, which had those two sections that I

1 described earlier.

2

BY [REDACTED]

3 Q So you mentioned the foreign division and you mentioned the customer
4 support division. Was there also a domestic division?

5 A Yeah. So those were offices within the Strategic Operations Division.
6 There were three offices, the office that oversaw the foreign engagement, the office that
7 oversaw the customer support, and then the office that I oversaw, which was called
8 Stakeholder Integration and Engagement. And then each of those offices had sections
9 underneath them. My office had the two sections I described earlier.

10 Q And so in the Office of Stakeholder Integration and Engagement, who was
11 your supervisor?

12 A I reported up to the head and deputy head of the Strategic Operations
13 Division. I believe they are called associate and deputy associate directors of FinCEN.

14 Q And who was that?

15 A At what point in time?

16 Q At all points in time while you were there.

17 A When I started in that office, which was I believe at the beginning of 2020,
18 the associate director that oversaw that division is AnnaLou Tirol. The deputy associate
19 director was Patrick O'Brien. I believe I formally reported to the deputy, who was
20 Patrick. So those were my -- that was my chain of command.

21 Q And so in your role as the director, how many people did you, roughly,
22 oversee?

23 A Gosh. Domestic engagement had, I don't know, five to seven. I'm
24 ballparking, but five, six, or seven. And data access had six to eight-ish.

25 Q Okay. And what was the mission of the Office of Stakeholder Integration

1 and Engagement?

2 A There is a formal mission. Can I defer to FinCEN on that? I mean, I sort of
3 described the offices and the roles as I know them, but I don't want to misstate. I think
4 FinCEN has an official mission for each division.

5 Q Sure. But in your words, how would you describe it?

6 A Best I can describe the division as a whole would be primarily the office that
7 oversaw external engagement generally, foreign, domestic, public, private, et cetera.

8 Q Did that mission change over time while you were there?

9 A Not terribly. That division did undergo some restructuring. I don't
10 remember when this change was made, but it was formerly called the liaison division. It
11 was the liaison division when I began at FinCEN at the end of 2018. At some point, it
12 was renamed Strategic Operations Division.

13 I don't recall the nature of the offices and sections changing significantly. I
14 believe the function and the mission, by and large, stayed the same, but there was some
15 restructuring.

16 Q And when did you leave FinCEN?

17 A I left FinCEN late summer of '22.

18 Q And why did you leave FinCEN?

19 A I would say a host of reasons. Primarily, though, I'm from Southern
20 California. I had been back East about 20 years and, you know, COVID changes people's
21 thinking and being shut inside, so I decided I wanted to move back home to L.A. and had
22 been looking for something.

23 Q And while you were at FinCEN, how often did you interact with FinCEN
24 leadership?

25 A What do you mean by FinCEN leadership?

1 Q The director of FinCEN.

2 A It depended a little bit on the director and what was going on. You know, a
3 month or two could go by without speaking to the director and then there could be a
4 6-week span where I spoke to the director every day. I certainly was at a level of
5 seniority where it would not be uncommon for me to be included in meetings or calls
6 with the director or speak with the director.

7 Q And so when you were speaking with the director, what was the nature of
8 those conversations? Were they generally on certain topics with your engagement in
9 the --

10 A It would -- well, I mean, listen, before COVID, you see somebody in the hall
11 and you're friendly. So certainly there was some informal, right. Generally, though,
12 given the pressing needs on the director's time, generally when you were speaking with
13 the director, it was on a specific topic or for a specific purpose.

14 Q And in general, what were those specific topics?

15 A I don't know that I can answer that question generally. It would have
16 depended on the topic. As an example, you know, one of the sections, as I mentioned,
17 oversaw, you know, FinCEN's access program to the BSA data. And there were multiple
18 times when various congressional hearings were going to cover that topic. So I would
19 sometimes be called upon to, you know, help inform the director or answer questions,
20 things of that nature.

21 That's an example. I mean, it could have been anything under my remit that
22 came up for whatever reason.

23 Q And did you interact with the Department of Justice while at FinCEN?

24 A Yes.

25 Q With whom at the Department of Justice?

1 A It would depend, and it would depend on the nature of the interaction. So,
2 certainly, DOJ components had access to the BSA data. So on my data access
3 management side, whether it was individual U.S. attorneys' offices or law enforcement
4 agencies like the FBI, you know, sometimes there would be issues on them accessing data
5 or they would need technical assistance or something of that nature.

6 And then on the domestic engagement side, one of the things that that section
7 oversaw was our public -- FinCEN's public-private partnership work. So, you know,
8 oftentimes we would provide assistance to law enforcement if they needed it on financial
9 access -- or access to financial data or some of the holdings that FinCEN had.

10 And so I would liaise, you know, either with Main Justice or U.S. attorneys or
11 assistant U.S. attorneys or, you know, law enforcement, FBI.

12 Q Were there certain persons within DOJ components that you liaised with the
13 most?

14 A Not that I recall. Certainly, I don't recall there being any particular person
15 that was so regular that the name sticks with me this many years later.

16 Q Okay.

17 ██████████ Any particular U.S. attorneys' offices that you interacted with more
18 frequently than others?

19 ██████████ Not that I recall.

20 ██████████ Did you ever interact with FBI field offices, or was it generally
21 out of DOJ, Main Justice?

22 ██████████ I'm not sure I ever knew at the time the distinction. I mean, I'm
23 not sure how they're structured. So FBI agent was FBI agent, and I'm not sure I
24 knew -- and, frankly, I struggled with that a little bit with DOJ as well. I never -- unless I
25 saw a title, I wouldn't necessarily know if they were out of a U.S. attorney's office or Main

1 or any of that. I'm not sure.

2

BY [REDACTED]

3

Q Shifting gears a little bit, what's your formal education?

4

A I have a bachelor's and a law degree, a JD.

5

Q Are you a licensed lawyer?

6

A Yes.

7

Q And when did you become licensed?

8

A I first took the New York bar and became licensed, it was either the very end

9

of '06 or the beginning of '07. And then I subsequently took the California bar and was

10

licensed at some point thereafter. I don't recall when.

11

Q And were you a lawyer, a licensed lawyer throughout your tenure at FinCEN?

12

A No. I actually never functioned as an attorney at FinCEN.

13

Q Were you a member of any bar while you were at FinCEN?

14

A I was an inactive member. So I am, to this day, a member of the New York

15

and California bars. I have been an inactive member of both, I believe, as best I can

16

recall, since I stopped formally practicing law in 2014.

17

Q And what's your formal training? I know you mentioned AML. Are there

18

any certifications or things along those lines?

19

A Sure. So I have a certification or at least I did at one point -- I'm not certain

20

I'm paying the dues anymore -- but of what's called ACAMS, which is the Association of

21

Certified Anti-Money Laundering Specialists. Also don't quote me on that one, but

22

which is sort of the industry credential for anti-money laundering financial crimes

23

professionals.

24

And then most of it, I would just say, on the job. You know, when I was in

25

private practice, I represented clients on compliance matters generally, including the BSA.

1 And then you, you know, you just learn on the job when I became an anti-money
2 laundering professional.

3 Q So moving back to your role when you were the director of the Office of
4 Stakeholder Integration and Engagement. So in that role, how did it relate to the
5 operations of FinCEN Exchange?

6 A So FinCEN Exchange was a public-private partnership program, and I would
7 say the logistics and the planning of those events were under the domestic engagement
8 section in my office. So my staff oversaw that event.

9 Q Can you describe the FinCEN Exchange briefly and then the events that you
10 mentioned?

11 A Sure. So, again, I'll do some of my own words, but FinCEN Exchange has an
12 official FinCEN description and whatnot, so I will defer to that. But, essentially, it was a
13 public-private partnership where it had a couple of components, and sometimes we
14 would focus on one, sometimes it would be everything. But it would, by and large,
15 either be where law enforcement was working on a case and needed access to financial
16 data, and so they would -- we would put together an event where law enforcement could
17 provide information to the private sector, banks usually, but didn't always have to be,
18 right -- there are numerous types of financial institutions under the BSA -- where they
19 would -- law enforcement could provide private sector members some information that
20 might help those institutions better identify suspicious activity, which is a requirement for
21 them to do under the BSA, so helping them sort of focus.

22 And then by the same token, there might be instances where financial institutions
23 are able to, within what authorities would allow, to share information with law
24 enforcement or each other, again, to better understand the nature of the conduct at issue
25 and, you know, try to catch bad guys.

1 Q And ordinarily, when Federal law enforcement is sharing information with
2 the private sector or vice versa, what mediums were used to facilitate that exchange?

3 A So particularly before COVID and then eventually, you know, there could be
4 in-person meetings, could be conference calls, could be email. So it would depend on,
5 you know, what type of communication and what the issue was.

6 Q You mentioned the different kinds of stakeholders and financial institutions.
7 Could you describe what kinds of financial institutions you were working with?

8 A Primarily banks. I believe in a few instances money services businesses,
9 MSBs.

10 Q For example?

11 A So I don't recall a specific MSB. Totally separate from your line of
12 questioning, an example of an MSB, for example, could be like Western Union as sort of
13 the classic example of a money transmitter. But I don't actually have a specific
14 recollection of a particular MSB participating in a FinCEN. I'm not saying they didn't; I
15 just don't recall.

16 Q And why was it important for FinCEN to reach out to the private sector?

17 A Not to be glib, when you say "important," like from whose -- I guess I'm not
18 really sure what you mean.

19 Q Well, I'll back up.

20 Why did you reach out to the private sector?

21 A So we would reach out to the private sector --

22 [REDACTED] You know, I guess -- I think he's testified about his job being to
23 reach out to the private sector on a variety of different topics, like everything from sort of
24 filing. Is your question now specific to FinCEN Exchange or like -- can you be more
25 specific about like -- what are you asking about specifically?

1 BY [REDACTED]

2 Q When you were liaising with the private sector, what sorts of information
3 were you looking for that the private sector had?

4 A Outside of FinCEN Exchange or specifically with -- just as a general matter?

5 Q As a general matter.

6 A Well, it could have been in the context of a FinCEN Exchange, which I just
7 described, or some of the other public-private partnership initiatives that FinCEN had. It
8 could be, you know, sometimes there's a miscommunication. Like, we'll have a law
9 enforcement agent reach out and say, hey, I'm trying to get X, Y, Z that I'm entitled to get
10 from such and such bank or such and such credit union, but they are not giving me what I
11 need. Can you -- you know, sometimes we'd literally just be a liaison.

12 I'm trying to think of other types of informal. You know, that's -- it could be any
13 number of reasons really.

14 Q Could you give an example of one of the public-private partnerships?

15 A So FinCEN Exchange is a big one. The other I would say major one is called
16 BSAAG, which is the BSA, the Bank Secrecy Act Advisory Group. Both are provided
17 foreign statute.

18 And the BSAAG was a bit more policy oriented, and it would also include, as an
19 example, other regulators, in addition to law enforcement and private sector members.
20 And it was a forum to discuss, like I said, a bit more on the policy realm. You know,
21 what's working, what's not, for FinCEN to receive feedback on its regulations, clarity or
22 lack thereof, things of that nature.

23 So certainly BSAAG and FinCEN Exchange were the two primary ones.

24 Q When you mention policy, was it discussing priorities for certain filings under
25 the Bank Secrecy Act or emerging suspicious activity, trends that you're seeing, things of

1 that nature?

2 A As best as I recall -- you're talking about BSAAG?

3 Q You're liaising with --

4 A So it would depend on the context, right. So BSAAG, which was a little
5 more policy oriented, dipped its toe into those areas but, by and large, was less tactical.
6 It was more, you know, hey, this regulation is not clear to us, so we're going in five
7 different directions. Or, you know, here's an example of guidance that the private
8 sector could use, you know. So FinCEN would take that feedback or, you know, FinCEN
9 would maybe pose questions to the private sector. Again, a little more on the policy
10 angle.

11 But what you just described would have taken place in the context of FinCEN
12 Exchange.

13 Q And before you were reaching out to the private sector, did you have to
14 receive approval before doing that?

15 A It would depend entirely on the reason I needed to reach out. For
16 example, the example I gave earlier, which definitely happened while I was there, where,
17 you know, a law enforcement agent was trying to get something from a financial
18 institution, that it was under statute and regulation. Law enforcement was entitled but
19 maybe the institution was just confused about what it was and was not allowed to share.
20 That would be something that, in the normal course of my duties at my level of seniority, I
21 would just go ahead and engage the institution.

22 But really, anything of greater import and certainly anything related to BSAAG or
23 FinCEN Exchange would generally require approval.

24 Q And who would that approval come from?

25 A I mean, I can only say that I would work with my chain of command. I

1 can't -- I couldn't speak to the extent to which they were informed by their leadership.
2 But I would go to my associate director and deputy associate director for those kinds of
3 approvals.

4 Q Which was Anna --

5 A AnnaLou and Patrick, at least at the beginning of '21.

6 [REDACTED] How long were they in those roles for?

7 [REDACTED] I don't recall.

8 [REDACTED] For each of them, who took on the next position when they left their
9 role?

10 [REDACTED] So at the beginning -- when I first started that office director job at
11 the beginning of 2020, it was AnnaLou Tirol was the associate director and Patrick O'Brien
12 was the deputy associate. At some point, I don't recall exactly when, AnnaLou -- our
13 director, the director of FinCEN left. I believe his deputy became acting director, and
14 AnnaLou became acting deputy director.

15 [REDACTED] Of FinCEN?

16 [REDACTED] Of FinCEN, yes.

17 I don't recall specifically what happened at the top of the division. I don't recall
18 whether Patrick was acting head at some point. And then there were various acting. It
19 was just a bit of a restructure while they figured out -- and I just don't recall people and
20 dates specifically.

21 [REDACTED] Is the restructuring complete by the time you had left?

22 [REDACTED] So I wouldn't call it a restructure as much as a sort of shuffling in
23 those roles. So I may have misspoke.

24 Well, so in mid to late '21, so at that time, the acting associate director was a guy
25 named Michael Dondarski, who was actually a member of our Enforcement Division but

1 he was acting as associate director, and his deputy was a guy named Andrew Winerman.

2 At some point, I don't recall when, Dondarski went back to enforcement.

3 Andrew became acting associate overseeing the Strategic Operations Division and asked
4 me to serve as the acting deputy associate. So at that point, and for my last nine or so
5 months at FinCEN, I was formally still the office director but I was serving as the acting
6 deputy of that division.

7

BY [REDACTED]

8 Q When you were engaging with the private sector, were there any topics or
9 issues that created points of tension?

10 A I'm not sure what you mean by points of tension, but not really, that I recall.

11 Q Disagreements. You mentioned earlier the example where a bank felt that
12 they couldn't share information or refused to share information. Were those kinds of
13 disagreements common?

14 A So I would say no. And I would also recharacterize -- that would be an
15 example where maybe like a very small institution doesn't necessarily have a level of
16 sophistication to know what they can and can't share. They are worried about BSA
17 confidentiality.

18 So when FinCEN would reach out and say, you know, hey, this is okay; you're
19 supposed to do this; you're required to do this; that would be sufficient for them to feel
20 comfortable that they're not violating law or reg and they would do so.

21 But I wouldn't -- I would call that more of a misunderstanding rather than a
22 disagreement. Certainly, generally no tension. An agent might be frustrated that he
23 was doing a dance, but I wouldn't call that tension. And I don't recall, again, at least at
24 that level of generality, I don't recall any points of tension, per se.

25 Q Do you recall there being confusion or misunderstanding about scope of the

1 Bank Secrecy Act?

2 [REDACTED] By whom? Can you be more specific?

3 [REDACTED] Yes, that's a broad question.

4 [REDACTED] Well, his example was a small institution that didn't understand
5 some of the confidentiality under the Bank Secrecy Act.

6 So were those misunderstandings -- did you routinely deal with some of those
7 misunderstandings about the breadth of the Bank Secrecy Act, what's confidential, what
8 they can provide, what they should be providing?

9 [REDACTED] I wouldn't say routinely, and I wouldn't -- you know, FinCEN wasn't
10 there necessarily to serve the private sector. Usually something like that would be to
11 assist law enforcement or something of that nature, if they were having trouble accessing
12 BSA data, whether that was with our -- within FinCEN's database, at a financial institution,
13 whatever it was.

14 So it's very hard for me to answer that question at that level of -- it's just a little
15 too general. I don't have recollections of disagreements or confusion, you know, writ
16 large.

17 [REDACTED] So would you view your role at FinCEN more of a partner of law
18 enforcement versus a partner of the financial institutions?

19 [REDACTED] All of the above. I'm not sure I would characterize any of our
20 relationships as above or below the other.

21 [REDACTED] Okay. When you say FinCEN was not there to assist the private
22 sector.

23 [REDACTED] We were certainly there to assist. I said we're not there to serve.
24 In other words, what I meant by that was, you know, it's not as if a bank could call FinCEN
25 and say jump and we would jump. Whereas, if the FBI said, hey, we're desperate; you

1 know, something major is happening; you know, we need you to jump, we would jump.

2 So it would depend on the nature of the relationship, but by the same token, we
3 had relationships with the private sector that maybe we didn't have with law. So it was
4 very specific to the relationship and to the topic what that relationship would have been.

5

BY [REDACTED]

6 Q Do you recall any examples -- we've talked a few times now about when
7 there was confusion or misunderstandings. When you're serving in a liaison position
8 between law enforcement and a private entity, do you recall any examples where there
9 wasn't confusion; there was a fundamental disagreement about how, you know, the Bank
10 Secrecy Act applied or a certain regulation?

11 A I don't specifically recall that, no.

12 Q Just to clarify the answer for the record. With the understanding you don't
13 have any specific recollections, generally, though, do you recall just that ever being an
14 issue or something that you or your office would be in a position to be aware of?

15 A Whether there was generally confusion or misunderstandings in the private
16 sector?

17 Q No, not regarding confusion or misunderstandings but where it's not an
18 issue of confusion, but there's a disagreement between how the Bank Secrecy Act applies
19 or what should be the --

20 A I see. Generally, that would not come to FinCEN. That's generally the
21 type of thing that would occur like with an examiner. So the functional regulators like
22 the Fed and the OCC, FDIC, et cetera. If there was like a dispute as to the BSA program
23 that an institution has in place, like that -- you know, FinCEN oversees the regulation, so
24 we would certainly be part of those conversations broadly.

25 And, again, you know, BSAAG, a lot of that conversation would come up about

1 policy, so not on a specific issue but, you know, broadly. But in terms of, like, specific
2 disagreements where FinCEN said X and some institution was saying Y, I don't recall that.

3 Q In the BSAAG group, do you recall any discussions about the scope of
4 disclosures or the scope of what should be kept confidential?

5 A I don't recall one way or the other.

6 [REDACTED] And just for the record, what was your involvement in BSAAG?
7 Because I just don't know how involved he actually was, so --

8 [REDACTED] Yeah, so BSAAG, like FinCEN Exchange, my staff would've sort of
9 coordinated the event. BSAAG has a mechanism for annual membership where we can
10 renew or replace members. So my staff would oversee the applications and all of that,
11 logistics, you know, getting a room or setting up conference calls, communications, things
12 of that nature. Not necessarily the substance of what's actually being discussed in any
13 of those forums.

14 BY [REDACTED]

15 Q And for BSAAG, was it generally like standing meetings or could they be
16 called on an ad hoc basis if there was an issue that had arisen?

17 A So there was a BSAAG plenary, all members, that was, I wouldn't say
18 standing as much as it was twice a year, but to be scheduled, right. It's not like -- it's not
19 like they have a calendar years out, right, but it's twice a year.

20 And then BSAAG -- within and under BSAAG, there were committees where
21 BSAAG members -- again, private sector, law enforcement, regulators -- would form sort
22 of working groups at the topical level. And so my staff would usually join and facilitate
23 those communications as well, but those were usually driven by the BSAAG members
24 themselves.

25 Q Do you recall like a couple examples of some of the topical choices for the

1 working group?

2 A Well, this is -- I should, but I don't recall specifically, no.

3

BY [REDACTED]

4 Q Does FinCEN have oversight responsibilities over financial institutions?

5 A Yes.

6 Q Can you describe those responsibilities?

7 A I can do the best I can. I mean, certainly they are set out in statute and reg.

8 So FinCEN owns the BSA, Title 31. So from a regulatory perspective, the
9 regulations that regulated financial institutions have to follow are drafted, revised.

10 Guidance is provided for by FinCEN. It's very complex because there are corollaries with
11 the functional regulators, which is Title 12 or title whatever it happens to be. And so
12 this is getting out of my sort of technical remit, but -- so certainly FinCEN has an
13 ownership role in the regulatory framework. And then FinCEN also has specific
14 statutory authority, such as FinCEN Exchange and BSAAG, with which they can engage the
15 private sector.

16 Q Which office was responsible for those oversight responsibilities?

17 A I would say most FinCEN divisions touch it at some point. So, for example,
18 there was the Policy Division, which oversaw regulatory guidance and interpretation,
19 regulatory drafting, technical advisories and bulletins, things of that nature. You had the
20 Enforcement Division, which would actually go out and examine and, if enforcement
21 activity was necessary, would handle that.

22 You know, there were other divisions that would analyze BSA data. The liaison
23 division, later Strategic Operations Division, that would liaise. So it really depended on
24 the nature of the interaction, but many divisions had a role to play.

25 Q And how did FinCEN enforce that oversight?

1 A I'm not quite sure I understand the question.

2 Q If you found that someone was out of compliance, how would that be
3 handled at FinCEN? Which office would lead that?

4 A Yeah, I mean, I was not involved in that. At a high level, it would generally
5 be the Enforcement Division, along with front office components, counsel, whoever
6 needed to participate, right. I mean, theoretically, it could be the folks in another
7 division that were looking at the data that led to the conclusion that they were out of,
8 you know, compliance. Like, it could be anybody.

9 But primarily, I would say the Enforcement Division, plus front office and counsel.
10 And they would do so -- you know, to your other part of your question, best I can answer
11 is that they would do so under the authorities and statute and reg, but it wasn't my
12 wheelhouse, so --

13 Q Were those enforcement actions involving violations of the Bank Secrecy
14 Act?

15 A Yes -- well, and I should say that my knowledge of that is limited to what's in
16 the public domain. So there may have been some activity that I just wasn't aware of
17 because it wasn't part of my job. So the enforcement actions that are publicly available
18 that were taken by FinCEN would have been, at least partially, due to Bank Secrecy Act
19 violations.

20 Q Could the failure to file a suspicious activity report according to material
21 shared or published by FinCEN result in an enforcement action?

22 [REDACTED] I'm sorry?

23 [REDACTED] In other words, FinCEN provides guidance, advisories, bulletins,
24 all the things that you mentioned.

25 [REDACTED] So I'm going to answer it this way.

1 [REDACTED] Was that something that was in your responsibility at all?

2 [REDACTED] No. The BSA requires that financial institutions have a risk-based
3 program. So you're taking a big step back. Generally, the way these institutions are
4 examined and assessed is, do you have policies, procedures, controls? Are they
5 appropriate? Were they being executed correctly?

6 If something falls through the cracks but your examiners or enforcement
7 personnel generally think that you were operating in a sound manner, something like that
8 may or may not actually result in enforcement action. It may. It, I believe, would
9 constitute a technical violation.

10 But, again, like, it's possible that they didn't know. A bank maybe didn't know
11 that something should have been filed because it was following its policies and
12 procedures and didn't identify -- you know, so it really is very hard to say, you know,
13 would X result in Y.

14 [REDACTED] And in your time at FinCEN, did you ever like, you know, do
15 your work in the Enforcement Division, or are you familiar with the standards of
16 willfulness that, like, the Enforcement Division would apply to an enforcement act?

17 [REDACTED] Not at all, no.

18 [REDACTED] So but in your role, you're responsible for sharing materials and
19 liaisoning with the private sector?

20 [REDACTED] Yeah, at a high level. Sure, yes.

21 [REDACTED] And so when you're sharing those materials and a bank receives
22 it -- a financial institution receives it, could a bank then be penalized for failing to file a
23 SAR according to the materials or guidance that is being shared with them? Would that
24 make it more risky to not file a SAR given that we've established the BSA is a risk-based
25 framework?

1 [REDACTED] Can you tell him what materials you're describing? Just
2 saying, like, material generally, I think that doesn't give him any information about
3 whether that would feed into the risk profile.

4 [REDACTED] Well, certainly he knows the materials that he shared.

5 [REDACTED] Well, I think we should establish that for the record.

6 [REDACTED] Yeah, I'm not sure I can recall. It might depend on what was being
7 shared.

8 [REDACTED] Okay. So could you give an example of what might distinguish
9 one from the other?

10 [REDACTED] Well, an example of materials that would be shared, and this,
11 actually, wouldn't have been shared by me, but, you know, FinCEN publishes advisories
12 on specific topics that contain some red flags.

13 [REDACTED] Yeah.

14 [REDACTED] I'm not sure I can really answer the question of, you know, if a bank
15 failed to take those red flags and do something with it and file a SAR and didn't file a SAR,
16 what would be more -- like, I'm not sure I can really speak to that at that level of
17 generality. And, again, it wasn't really my role at FinCEN.

18

BY [REDACTED]

19 Q Who would best be able to speak to that?

20 A Either people at FinCEN in enforcement, counsel, possibly front office. I
21 mean, I would defer to FinCEN as to, you know, who can best speak to that.

22 Q When the information is being shared -- previously there were questions
23 about, you know, specific information and maybe there is a failure to follow SAR. When
24 sharing information, was there an expectation that some of the information shared could
25 lead banks to or financial institutions to change what protocols they had in place?

1 A Whose expectation?

2 Q FinCEN's expectation.

3 A No. I don't believe that we had any expectation or criteria that that was
4 going to lead to. Really, it was -- FinCEN's purpose was to be helpful either to law
5 enforcement or to the private sector. If we had information that was available that we
6 felt we were legally allowed to share and it would be useful, we would do so, but it
7 didn't -- my recollection is it didn't come with any standards or expectations or
8 requirements.

9 Q Taking out expectations. This is a problem. Were there protocols put in
10 place based off the state of the world where protocols are implemented? FinCEN is
11 sharing new information that they think is helpful to the private sector partners. Were
12 there discussions about changing the protocols in light of what new information was
13 being shared?

14 A The banks' protocols?

15 Q Yes.

16 A I do not recall conversations like that, no.

17

BY [REDACTED]

18 Q Does FinCEN direct financial institutions to certain kinds of potential
19 suspicious activity?

20 A What do you mean by "direct"? Like, we'll share indicators, for example,
21 like in an advisory and provide them information that they may or may not have been
22 aware of.

23 Q Yeah, bring to their attention.

24 A Yes.

25 Q Okay.

1 [REDACTED] What types of indicators?

2 [REDACTED] It could be something like -- you know, depending on the topic,
3 right, but it could be something like, you know, those engaged in a certain type of fraud
4 tend -- you know, we've seen evidence that they move money in this manner, right.
5 Here's like a red flag, a typology that we have observed. It could be things like that.

6 [REDACTED] And kind of to turn back to a previous question, going off of this
7 hypothetical example, right. If you're identifying something new, was there ever a
8 discussion about whether protocols in place were adequately, you know, detecting that
9 sort of potential misconduct?

10 [REDACTED] Can we just sort of clarify the use of the word "protocols"?
11 Because I want to make sure you guys are using that -- I think what you mean is like a
12 bank's existing AML framework, right. What they're required to have under the BSA.
13 So I think for the record, like, can we just use that?

14 [REDACTED] Okay. Sure.

15 [REDACTED] Yeah, I mean, certainly I don't recall any discussions that an
16 institution would be expected to -- or that we would hope an institution would change its
17 policies, procedures, its program in place. You know, the focus would have been on the
18 information being shared and disseminating it. It's part of FinCEN's mission to analyze
19 the data we have and disseminate information where we can.

20 BY [REDACTED]

21 Q Were there any instances that you can recall where a financial institution
22 failed to file an SAR and there was a discussion about why that happened or why it was
23 missed?

24 A Not that I recall. I wouldn't have been involved in those conversations.

25 Q And who at FinCEN would have been?

1 A Likely enforcement personnel or front office or counsel.

2 Q We touched upon this earlier. Can you walk us through, again just very
3 briefly, during your time at FinCEN who was head of enforcement?

4 A Oh, boy. When I started, it was a guy named -- oh, I'm going to kick myself.
5 He was a nice guy. He retired. There was a longtime head of that division who retired
6 while I was at FinCEN. His name escapes me. I hope he doesn't see the video. Sorry.
7 And then when he retired, I don't actually recall who became associate director.

8 The gentleman I mentioned earlier, Mike Dondarski, was the deputy associate, but
9 I can't actually recall. It wasn't my division, and I actually didn't work a ton with those
10 folks. I mean, I was friendly in the hall, coworkers, but I just don't recall.

11 [REDACTED] Do FinCEN employees review the SARs that are filed?

12 [REDACTED] Certain FinCEN employees do, yes.

13 [REDACTED] What office would that fall within?

14 [REDACTED] It could be any. Certainly, our -- certainly, FinCEN's Intelligence
15 Division would review SARs. I know that there would be instances where enforcement
16 personnel would need to review SARs. There would be potential technical or filing
17 reasons for someone in strategic operations to review SARs, like customer support. You
18 know, oh, we double filed. What do we do? You know, that kind of stuff.

19 I mean, yes, the answer is -- I mean, I'm not really sure who else, but --

20 [REDACTED] Can I just make sure, because I think you asked did FinCEN
21 employees review SARs. To your knowledge, did FinCEN employees review all SARs that
22 are filed?

23 [REDACTED] To my knowledge, no, not one for one.

24 [REDACTED] That was going to be my next question.

25 [REDACTED] Sorry. I just wanted to make sure that was clear, because I

1 think that was a little messy.

2 [REDACTED] So, no, to the best of my knowledge, there isn't actually someone
3 putting eyeballs on every SAR. A lot of it would be based on, you know, keyword
4 queries and things of that nature.

5 [REDACTED] So how do you determine which SARs to review?

6 [REDACTED] It wasn't my job at FinCEN. I'm not sure I can answer that
7 question.

8 BY [REDACTED]

9 Q Whose job was it?

10 A For what purpose? To review SARs for what purpose?

11 Q Who at FinCEN would be in a position to decide which SARs are reviewed?

12 A It would depend on the purpose for which they're reviewing SARs.

13 Q What are some of the purposes of SARs review?

14 A I mean, I hate to speculate because it, by and large, was not my job. It
15 wasn't reviewing many SARs at all. You know, as an example, just to be helpful, like, if
16 Enforcement Division was looking at financial institution X, they would probably search
17 for a subset of that financial institution's SARs for whatever purpose.

18 If Intelligence Division was looking for, you know, healthcare fraud, they would
19 presumably search healthcare fraud.

20 I mean, but those are somewhat speculation just because it really was not part of
21 my job, by and large, to query the database and view SARs.

22 BY [REDACTED]

23 Q But you did manage the access to those databases?

24 A Yes.

25 Q And so then you would be maybe in a position to know what SARs are being

1 reviewed and for what purpose?

2 A My duties did not require or warrant a need to search the database, and I
3 generally did not. I don't actually recall ever. It may have happened once or twice, but
4 I'm not even sure I had a login. I don't recall searching SARs as part of my job.

5 Q Do you know if SARs were ever reviewed by using artificial intelligence or
6 machine learning?

7 A I do not know.

8 Q Do you know who would know?

9 A Current FinCEN personnel. I certainly know, while I was there, that there
10 were conversations both internal to FinCEN as well as feedback that we would get from
11 law enforcement or whomever about various ways that the ability to query the data
12 could be enhanced. But I don't recall where it stood at the time or where it's gone
13 since.

14 Q Enhanced using like machine learning or artificial intelligence?

15 A I don't recall. Improved, if you will, but not -- I don't have any specific
16 recollection of whether those mechanisms were being used or are currently being used.

17 Q Did you ever discuss with the private sector the use of artificial intelligence
18 or machine learning to identify suspicious activity?

19 A I don't have a specific recollection of that kind of conversation. Certainly,
20 regulated financial institutions use a variety of vendors and other technological
21 capabilities for their own purposes to execute their own program. You know, might that
22 have come up in some of the conversations I had in the course of my liaising, perhaps, but
23 I don't specifically recall.

24

BY [REDACTED]

25 Q What about internal discussions you mentioned when it comes to improving

1 the query? Who would those internal discussions have been with?

2 A Who would those discussions have been with if they had happened? I
3 mean, I don't recall the discussions is the issue, so I'm not really sure how to answer.

4 Q Sure. In a previous response, if I understood your testimony correctly, you
5 said that there were, you know, internal and external discussions about improving the
6 query, right, when searching --

7 A Yep.

8 Q -- keywords or whatever it might be. Maybe it's AI. Maybe it's not.
9 For the internal discussions, who would those have been with?

10 A So I recall -- and I apologize if I misspoke. I recall generally there being
11 conversations with some of the government-side agencies who have access to the
12 database about how to query, whether enhancements or improvements were in
13 discussions. I do not specifically recall whether those discussions covered AI or ML or
14 any of that.

15 I don't know internally -- I mean, those kinds of conversations internally would
16 have been with other Strategic Operations Division personnel, perhaps my leadership,
17 front office personnel, and the director's office. But that's also a bit of speculation, I
18 would say, because I'm not sure I really recall.

1 [10:52 a.m.]

2

BY [REDACTED]

3 Q And when we're accessing the BSA materials, how is that material accessed?

4 A Are you asking if you -- how does law enforcement access the database for

5 FinCEN or --

6 Q All of the above.

7 A So when I was there -- I can't speak for what it was now, but while I was at
8 FinCEN, there was a -- a portal. I don't recall whether it was hosted or cloud or a web or
9 how, but agencies with proper access would be able to access the data from their own
10 workstation. You know, they didn't have to come onsite or anything like that. So
11 there would be some logon and then they would have access to the portal where they
12 could query and access the data.

13 Q Was there a name of the portal?

14 A I don't recall. Yes, there was a name. I don't recall what it was.

15

BY [REDACTED]

16 Q And was the portal the same for all of those entities accessing it? So was
17 FinCEN hosting this portal?

18 A I'm not sure I recall that level of technical -- I definitely can't answer the did
19 FinCEN host. I don't really know where the data physically -- that's like our -- that's our
20 computer folks.

21 Yeah, sorry. Go ahead. I'm not sure I can --

22 Q I think -- this was a BSA database of SAR filings, what have you.

23 A Uh-huh.

24 Q When everyone was accessing, were they accessing the same database?

25 A I believe the answer is yes. I can't speak to whether there were other

1 sources that they may have had access to. I don't recall. But there certainly was sort
2 of one primary database.

3 I'm trying to remember -- I don't recall whether there were any restrictions for a
4 particular agency on data. I don't recall whether that existed or -- or was applied.
5 Certainly, that was a component of what my team would look for when they audited
6 access. You know, they would look, for example, for things like, you know, are they
7 pulling queries that are really broad, you know, maybe overbroad.

8 So there would be a component of assessing how an agency used data, but
9 whether there was like a block in place up front or whether this agency had access to A,
10 B, and C, and this agency only had access to A and B, I don't recall.

11

BY [REDACTED]

12 Q Who had access to the portal?

13 A FinCEN personnel. And then, best of my recollection, either statute and/or
14 reg provides for which agencies can have access. So I would kind of defer to that. But
15 it included law enforcement, Federal, State, local, whomever, intelligence community,
16 other regulators. Those were the primary stakeholders.

17 Q Do you know, roughly, how many individuals that is?

18 A No idea.

19 Q You also mentioned audit a moment ago. And can you describe what an
20 audit of those with access to the portal, what that looked like?

21 A Not in great detail. But as a general matter, FinCEN has a program whereby
22 there's a team that periodically will assess an agency's use of the data to make sure it's
23 appropriate, to make sure the proper security measures are in place, to make sure that
24 they're educated on how best to query. And that's a periodic process that FinCEN has to
25 ensure the integrity of the data and its use.

1 Q Did you ever find an example where an agency was not using it
2 appropriately?

3 A I don't recall. And I certainly don't recall inappropriate use. We
4 frequently saw examples where an agency could use better education on how to more
5 intelligently query the database just to yield better results. So, you know, a lot of what
6 this team did would be sort of, you know, provide, you know, assistance or -- or learning
7 to, you know, agency personnel on how best to query the data. But I don't have a
8 specific recollection of anybody, you know, uncovering inappropriate use.

9 Q When an audit was completed, how often were those audits performed, and
10 what happened with the results of those audits?

11 A The audits were periodic. I don't recall the frequency.

12 Q Once a year, twice a year?

13 A I -- fairly confident it was not twice a year. I don't recall if it was one once a
14 year or once every other year. It was that cadence, generally. Every year, two, or
15 something like that.

16 The FinCEN employee would engage with their counterparts at that agency, you
17 know, go through the steps of the audit, ask the questions, whatever they did, prepare a
18 report internally that would go up to the section chief for review and approval.

19 If there were -- I don't specifically recall this happening, but if there were issues or
20 something like that required escalation, it would come to me. The section chief
21 reported to me. That was the data access and management side of my office.

22 And then like any issue anywhere, depending on the nature of the issue, it could
23 go up, if needed. But I don't have a recollection of that happening.

24 [REDACTED] Can we go off the record, please?

25 [Recess.]

1 [REDACTED] Okay. We can go back on the record.

2 EXAMINATION

3 BY [REDACTED]

4 Q Thank you, [REDACTED]

5 You mentioned -- earlier, I believe you were asked what the mission of your unit at
6 FinCEN was, and you said you would defer to FinCEN. And I would just like to start by
7 saying that FinCEN's website describes the agency as a whole, FinCEN's mission as, "to
8 safeguard the financial system from illicit use, and combat money laundering and its
9 related crimes, including terrorism, and promote national security through the strategic
10 use of financial authorities and the collection, analysis, and dissemination of financial
11 intelligence."

12 Does that sound right to you?

13 A Yes.

14 Q And that's your understanding of the mission that you as a FinCEN
15 employee, the overall mission that you were working towards?

16 A Yes.

17 Q Thank you.

18 And so that's a very long way of saying FinCEN works to combat the use of
19 financial systems to finance terrorism and to launder money?

20 A Yes.

21 Q And FinCEN's work to combat the financing of terrorism includes the
22 financing of domestic terrorism, correct?

23 A Yes.

24 Q And just to back up, the -- the combating the financing of terrorism is
25 commonly referred to as CFT?

1 A Yes.

2 Q That's the acronym that is often -- often used?

3 A Yes.

4 Q And anti-money laundering is AML?

5 A Yes.

6 Q Okay. And you've had experience in those fields, the AML and CFT fields, in
7 both the private sector at a financial institution --

8 A Yes.

9 Q -- correct? And at FinCEN?

10 A Yes.

11 Q And so you've -- you've kind of got those two windows into that particular
12 activity?

13 A Yes. And on the legal side as well, representing clients who are compliant
14 with those laws and regs.

15 Q And was that before you went to work for the bank?

16 A Yes.

17 Q And FinCEN itself is not a law enforcement agency in the sense that it
18 doesn't go out and arrest people?

19 A Correct, in that sense. I'm not sure if there's a technical definition of law
20 enforcement of what FinCEN does and does not qualify for. But it certainly did not have
21 guns and badges and arrest power and things of that nature.

22 Q And when you used the term earlier of "law enforcement," and as I imagine
23 we'll all be using it today, you're referring more to agencies that do have those
24 authorities, like the FBI, DEA, local police agencies, that sort of thing?

25 A Yes.

- 1 Q Okay. Thank you.
- 2 Now, FinCEN is not a new agency, correct?
- 3 A Define "new". I mean, it's been around --
- 4 Q It was established in 1990.
- 5 A -- many, many years.
- 6 Q Does that sound right?
- 7 A '90? You know what, I'm not certain.
- 8 Q It wasn't something that just popped up in 2021?
- 9 A No.
- 10 Q And one of the -- one of the components of FinCEN's mission, as we just
- 11 discussed, was using financial authorities, financial statutes, but also the collection,
- 12 analysis, and dissemination of financial intelligence, correct?
- 13 A Yes.
- 14 Q What does the phrase "financial intelligence" mean to you, as best as you
- 15 can explain it?
- 16 A I mean, it can mean a lot of things. I think when I think of how FinCEN -- at
- 17 least my role at FinCEN went about doing that, it would be the BSA data that is filed with
- 18 FinCEN, analyzing that data, and deriving from it information about how nefarious actors
- 19 are -- are operating. We would call them red flags, typologies, indicators, things of that
- 20 nature.
- 21 Q And your work wasn't to actually do that analysis, correct?
- 22 A Correct.
- 23 Q That was a separate division of FinCEN?
- 24 A Correct.
- 25 Q Okay. Your work was more that of a liaison between the different

1 stakeholders who had access to BSA information?

2 A Correct.

3 Q And so it was part of your job to help communicate some of those typologies
4 and indicators that law enforcement had developed to the financial institutions, correct?

5 A Correct.

6 Q And financial institutions are not required to work with FinCEN in that
7 regard, correct?

8 A Correct.

9 Q It's their choice whether or not to participate in Exchange events, for
10 example?

11 A Correct.

12 Q And it's their choice whether or not to receive typologies from -- from you or
13 from law enforcement?

14 A Well, mostly correct. I mean, some of the -- we do issue typologies in the
15 public domain through, like, an advisory. So that's -- that's out there, right.
16 Nobody -- nobody can escape it. But in terms of, like, participation in engaging with
17 FinCEN on a particular item, certainly in the context of FinCEN Exchange, BSAAG, the
18 items -- or the initiatives I discussed earlier, that was totally voluntary.

19 Q Okay. Thank you.

20 Now, you mentioned several times that FinCEN's authority and some of its duties
21 and responsibilities are actually codified in statutes and regulations.

22 A Correct.

23 Q Now, I'm going to go through some of those a little bit and introduce some
24 of them into the record just so that we have a clear understanding. So I'll refer to this as
25 the potentially boring section of -- of this interview.

1 And I'm going to start -- and this will be exhibit 1. This is 31 U.S.C. Section 310.
2 Sorry. I hope I made enough copies. I did not expect quite as many people here today.
3 [REDACTED] Exhibit No. 1.
4 [REDACTED] was marked for identification.]

5 BY [REDACTED]

6 Q Okay. You can take a moment to look through it. I'm not going to ask you
7 anything from memory. I will point to you exactly what I would like to reference. So
8 you just let me know when you're ready.

9 A Yeah, go for it.

10 Q Okay. So first I want to start by noting that in this printout of the statute, it
11 says that the effective date is December 27, 2021. And I will just note for the record
12 that the only portion of the statute that went into effect on that date was the addition of
13 the phrase "other relevant private sector entities" on page 4 in subsection d(2). So
14 other than that, this was all in effect during your time at FinCEN.

15 So I want to turn your attention to page 1. And first of all, the title of this
16 subsection of the United States Code is called Financial Crimes Enforcement Network,
17 correct?

18 A Yes.

19 Q Okay. Now -- and subsection (a) states that the Financial Crimes
20 Enforcement Network -- I'm sorry.

21 "The Financial Crimes Enforcement Network established by order of the Secretary
22 of the Treasury on April 25th, 1990, shall be a bureau in the Department of the Treasury,"
23 correct?

24 A Yep.

25 Q Okay.

1 A Yes.

2 Q Now, if we look at subsection (b)(2), it refers to the duties and the powers of
3 the director of FinCEN. And, again, this is part of the record and this is publicly available,
4 so I'm not going to read the entire statute. But I think most relevant to -- to the issues
5 that we're going to be discussing here today, if you look at subsection (2)(B), the director
6 is required to "maintain a governmentwide data access service, with access, in
7 accordance with applicable legal requirements, to the following:"

8 And then it states, "Information collected by the Department of the Treasury,
9 including report information filed under subchapter II of chapter 53 of this title, such as
10 reports on cash transactions, foreign financial agency transactions and relationships,
11 foreign currency transactions, exporting and importing monetary instruments, and
12 suspicious activities."

13 Did I read that correctly?

14 A Yes.

15 Q Okay. And so the suspicious activities, that's a reference to the -- the SARs
16 that we were talking about earlier, correct?

17 A Yes.

18 Q And, again, so this is Congress telling the director of FinCEN that they're
19 required to maintain a governmentwide data access service with information including
20 SARs?

21 A Yes.

22 Q Now, if you turn the page to paragraph 2, subsection (C) requires the
23 director to "Analyze and disseminate the available data in accordance with applicable
24 legal requirements and policies and guidelines established by the Secretary of Treasury
25 and the Under Secretary of the Treasury for enforcement to -- identify possible criminal

1 activity to appropriate Federal, State, local, Tribal, and foreign law enforcement agencies;
2 and also to support ongoing criminal financial investigations and prosecutions and related
3 proceedings, including civil and criminal tax proceedings."

4 Did I read that correctly?

5 A Yes.

6 Q Okay. And that is consistent with the work that you were trying to carry
7 out at FinCEN?

8 A Yes.

9 Q And some of the other goals of the dissemination of that data include -- if
10 you look at subsection (v) -- "determining emerging trends and methods in money
11 laundering and other financial crimes," correct?

12 A Yes.

13 Q And the next subsection, subsection (vi), supporting -- and these are Roman
14 numerals -- "supporting the conduct of intelligence and counterintelligence activities,
15 including analysis, to protect against terrorism; and to support government initiatives
16 against money laundering," correct?

17 A Yes.

18 Q Okay. And FinCEN is also required, in subsection (D), to "Establish and
19 maintain a financial crimes communications center to furnish law enforcement
20 authorities with intelligence information relating to emerging or ongoing investigations
21 and undercover operations," correct?

22 A Yes.

23 Q And subsection (E) has a much longer description about how FinCEN is
24 required to furnish research, analytical and informational services to financial institutions,
25 and then it goes on a little longer.

1 But, essentially, this is all work that FinCEN is doing, at the end of that subsection,
2 "in the interest of the detection, prevention, and prosecution of terrorism, organized
3 crime, money laundering, and other financial crimes."

4 Did I read that correctly?

5 A I lost you on that last part.

6 Q I'm sorry. I'm -- I'm at subsection (E) on page 2.

7 A Oh, the bottom of that paragraph, yes. Interest -- yes.

8 Q And when you look at that subsection, that is essentially what you were
9 doing when you were passing along typologies and indicators to financial institutions,
10 correct?

11 A Yes.

12 Q And if you turn to page 3, subsection (K), FinCEN is required to
13 "Communicate regularly with financial institutions and Federal function regulators that
14 examine financial institutions for compliance with subsection II of chapter 53 and" -- I will
15 represent that that is the Bank Secrecy Act -- "promulgated under that subchapter and
16 law enforcement authorities to explain the United States Government's anti-money
17 laundering and countering the financing of terrorism priorities."

18 Did I read that correctly?

19 A Yes.

20 Q And, again, that was part of the mission that you were working towards,
21 correct?

22 A Yes.

23 Q And subsection (L) requires FinCEN to "Give and receive feedback to and
24 from financial institutions, State bank supervisors, State credit union supervisors, as those
25 terms are defined in section 6003 of the anti-money Laundering Act of 2020, regarding

1 the matters addressed in subchapter II of chapter 53 and regulations promulgated under
2 that subchapter," correct?

3 A Yes.

4 Q And, again, that's a reference to the Bank Secrecy Act, correct? It's okay
5 if --

6 A Yeah, you represent it as such. I don't remember, but yeah.

7 Q Okay. So stepping back, it's clear from this statute and from your
8 testimony that FinCEN's engagement with financial institutions, other members of the
9 private sector and their -- the work that you did liaising between those institutions and
10 law enforcement is something that is required by Congress, it is required by statutes that
11 Congress passed?

12 A Yes.

13 Q Okay. Thank you.

14 Now, I want to talk a little bit about the Bank Secrecy Act, because we -- it's come
15 up a lot already, but I don't think that we've -- we've talked about it at great detail.

16 So at a high level, is it fair to say that the Bank Secrecy Act provides for financial
17 institutions to report information for use in criminal and tax investigations, including
18 reports on suspicious transactions, relevant to a possible violation of law or regulation?

19 A Yes.

20 Q Does that sound right? Okay.

21 Now, I'm going to introduce as an exhibit a letter that was written to the chairman
22 of the Judiciary Committee by the acting assistant secretary of the Office of Legislative
23 Affairs at FinCEN, Mr. Corey Tellez -- or, I'm sorry, the Department of the Treasury. And
24 this will be exhibit 2.

25  Exhibit No. 2.

1 was marked for identification.]

2 [REDACTED] And I'm not sure if you've seen this, but whether you have or you
3 haven't, please feel free to take as much time as you need to review it.

4 Did I make enough?

5 [REDACTED] Great.

6

BY [REDACTED]

7 Q Okay. So I'm going to turn your attention on page 1 to the last paragraph,
8 and the second sentence says, "First, pursuant to the Bank Secrecy Act, FinCEN is
9 authorized to collect, analyze, and disseminate financial intelligence to law enforcement,
10 national security, and regulatory agencies for use in connections with criminal
11 investigations and related matters."

12 Did I read that correctly?

13 A Yes.

14 Q And, again, that's consistent with your understanding of FinCEN's authority?

15 A Yes.

16 Q And if you look at the footnote, that cites the statute that we just -- we just
17 reviewed --

18 A Yes.

19 Q -- 31 U.S.C. 310, correct?

20 Okay. Now, turning to page -- sorry, excuse me -- 2, in the section called BSA
21 Reporting, Assistant Secretary Tellez says that, "One of the key sources of information
22 that FinCEN uses to carry out its mission are suspicious activity reports, which are filed by
23 banks and other financial institutions that possess customer transactions."

24 Is that your understanding of suspicious activity reports?

25 A Yes.

1 Q And the -- then the letter then says, "The BSA requires that a bank or other
2 financial institution file a SAR whenever it identifies, quote, "a suspicious transaction
3 relevant to a possible violation of law or regulation," end quote.

4 Did I read that correctly?

5 A Yes.

6 Q And is that consistent with your understanding of the Bank Secrecy Act?

7 A Yes.

8 Q And, again, the footnote for that is for a different statute, a section of the
9 Bank Secrecy Act, 31 United States Code, section 5318, subsection (g)(1).

10 Did I read that correctly?

11 A Yes.

12 Q Okay. And the assistant secretary goes on to say that, "SARs constitute
13 critical tip-and-lead information that helps law enforcement identify, stop, and
14 apprehend criminal actors."

15 Did I read that correctly?

16 A Yes.

17 Q And is that your understanding of what SARs do?

18 A Yes.

19 Q Okay. Now, going back to banks' obligations under the BSA to file SARs,
20 banks -- the Bank Secrecy Act requires SARs to file -- I'm sorry -- requires banks to file
21 SARs for any transaction that might be relevant to a possible violation of criminal laws.

22 Is that your understanding?

23 A Is that a quote of particular language? Yeah, I think -- I think what's
24 tripping me up is the word "any," because it's not -- I don't want to imply that there's an
25 expectation that every single suspicious transaction get filed. It's -- it's only those that

1 the bank becomes aware of through the implementation of its AML program.

2 Q Okay. And I appreciate that clarification.

3 A Yeah.

4 Q Thank you.

5 And that -- well, we're going to talk about the AML programs in a minute. But,
6 essentially, banks are required to have programs to help them identify transactions that
7 must be reported under the Bank Secrecy Act?

8 A Yes.

9 Q Okay. Thank you.

10 And SARs are used across all -- different types of criminal investigations, correct?

11 A Yes.

12 Q Drug trafficking, for example?

13 A So I don't necessarily have firsthand knowledge because, you know, it wasn't
14 my job at FinCEN to really review or analyze SARs. But as a general matter, my
15 awareness in the industry, yes, for a wide variety of -- of potentially criminal conduct,
16 including drug trafficking.

17 Q And the primary mission of FinCEN, though, is to focus on money laundering
18 and financing of terrorism?

19 A Yes.

20 Q And when a financial institution files a SAR, they file it with FinCEN, correct?

21 A Yes.

22 Q And then it goes into FinCEN's database?

23 A Yes.

24 Q And then FinCEN makes SARs available to law enforcement agencies that
25 have access to those databases?

1 A Yes.

2 Q Okay. And SARs are subject to strict confidentiality provisions under the
3 law, correct?

4 A Yes.

5 Q And, in fact, as your counsel mentioned at the beginning, your -- FinCEN is
6 very sensitive about those provisions and about maintaining those confidentiality
7 provisions?

8 A Absolutely, yes.

9 Q And that was something that, I imagine, you received extensive training on
10 while you were at FinCEN.

11 A Yes.

12 Q And financial institutions file millions of SARs every year. Is that your
13 understanding?

14 A I believe so, yes.

15 Q And as you stated earlier, it is not your understanding that every single one
16 of those millions of SARs is actually viewed --

17 A Correct.

18 Q -- by a law enforcement agent or somebody working at FinCEN?

19 A Correct.

20 Q I imagine there are many that are filed and are never looked at.

21 A I believe so.

22 Q Now, based on your experience in the -- working at a financial institution and
23 working at FinCEN, you're aware that banks do not need a warrant or a subpoena in order
24 to file a SAR, correct?

25 A Correct.

1 Q And FinCEN does not need a warrant or a subpoena in order to receive a SAR
2 from a bank?

3 A Correct.

4 Q And that's because the legal process that authorizes the filing of a SAR is the
5 Bank Secrecy Act itself, correct?

6 A Correct.

7 Q And the Bank Secrecy Act does not require probable cause that a crime has
8 been committed. It's not the same standard as if you were applying for a warrant.

9 A Correct.

10 Q Now, I want to get back to what you mentioned earlier, which is the -- the
11 banks or the financial institutions' anti-money laundering program. So now I'm going to
12 be using the phrase -- or the word "bank" as a shorthand for financial institutions
13 generally just because it's a mouthful otherwise.

14 So it's the bank's responsibility to determine, consistent with the Bank Secrecy Act
15 and its implementing regulations, when it must file a SAR, correct?

16 A Correct.

17 Q And FinCEN can provide guidance or indicators but, ultimately, the
18 responsibility lies with the bank to determine whether or not a SAR is appropriate?

19 A Yes, correct. I mean, I would note that, to my knowledge, FinCEN wouldn't
20 or hasn't provided specific guidance at the SAR level. It would be at the sort of typology
21 red flag level.

22 Q Okay. Can you explain what you mean by that, what that -- what the
23 difference would be?

24 A Like, for example, FinCEN would never or, to my knowledge, has never told a
25 bank, if you see X, it's suspicious, or, you know, this person is a criminal, you must file a

1 SARs on them.

2 FinCEN wouldn't operate at that level of specificity. They would offer high-level
3 typology. You know, here's a description of how a drug trafficker might move money,
4 here's a description of how a fraudster places the money into the system, things -- things
5 that, you know, at that sort of typology level.

6 Q And it's the bank's responsibility to take that information or not and use it
7 to, again, make their own ultimate judgment about whether any particular transaction at
8 their institution merits the filing of a SAR?

9 A Correct. And just to link it back up to what we mentioned earlier, the
10 dissemination of that information, which, as you noted, is required by law for FinCEN to
11 do, does not come with any requirement or expectation as to how it is used or whether it
12 is used.

13 Q Okay. So when FinCEN sends along a typology, a bank can say, you know,
14 not helpful, sorry; we have our own program, and we're not going to use that?

15 A Correct.

16 Q I mean, they wouldn't necessarily say that to your face, but that's what they
17 could -- that's what they could say, you know?

18 A Yes.

19 Q That's how they could approach you?

20 A Sure.

21 Q Or they could say, this is helpful; we might use this?

22 A Correct.

23 Q But, ultimately, FinCEN has no authority over whether or not a bank files a
24 particular SAR?

25 A Correct.

1 Q And banks are actually required to maintain their own AML/CFT programs,
2 correct?

3 A Correct.

4 Q Okay. And those programs are designed, among other things, to ensure
5 their compliance with the BSA and that they are detecting and reporting suspicious
6 activity?

7 A Yes.

8 Q Okay. Now, I'm going to introduce another statute that might take me a
9 minute to find.

10 A While you're doing that, this is overly technical, but this is something I did at
11 FinCEN. I believe -- so the AML program is a specific reg. The requirement to file
12 suspicious activity is a separate reg. So I -- it might be technically incorrect to say an
13 AML program requires a filing of a SAR only because that's the way the -- the laws and the
14 statutes are written. The AML program must contain controls in place to identify and
15 detect, and it's all kind of cobbled together.

16 Q And I appreciate -- no, I appreciate that.

17 A Technical correction, but --

18 Q Thank you. And -- and it's a valuable one, because I think I did, in fact,
19 conflate two different statutes and regulations in that question.

20 So I'm going to go ahead and introduce, as exhibit 3, 31 U.S. Code Section 5318,
21 which is another long one. Again, I'm not going to take you through all of it.

22 [REDACTED] Exhibit No. 3.

23 [REDACTED] was marked for identification.]

24

BY [REDACTED]

25 Q I'm going to turn your attention to page 10 of this printout. It's a really long

1 statute, subsection (h). And subsection (h)(1) provides that, "In order to guard against
2 money laundering and the financing of terrorism through financial institutions, each
3 financial institution shall establish anti-money laundering and countering the financing of
4 terrorism programs."

5 Did I read that correctly?

6 A Yes.

7 Q And then it goes on to -- to list four different aspects that those programs
8 must have, correct?

9 A Correct.

10 Q Okay. So, again, this isn't just something that banks do because they want
11 to; it's something that they are required to do by law?

12 A Required. In fact, those four are referred to as pillars.

13 Q Okay. So --

14 A And they're required elements of the AML program.

15 Q Since they're pillars, we might as well read them into the record. They are
16 the development of internal policies, procedures, and controls; the designation of a
17 compliance officer; an ongoing employee training program; and an independent audit
18 function to test programs.

19 Did I read that correctly?

20 A Yes.

21 Q And those are the pillars you were referring to?

22 A Yes.

23 Q Thank you.

24 So financial institutions are required to have -- well, most of them have entire
25 units of employees where that's -- that's just their job, correct, is to work --

1 A It would depend on the size. I mean, there are some baby community
2 banks out there that have like one person sometimes wearing multiple hats, but then
3 there's a Wells Fargo, B of A of the world that will have many, many, many people doing
4 this work.

5 Q And that's the type of work that you did at I believe it was
6 Standard Chartered Bank?

7 A Yes.

8 Q Okay. Thank you.

9 And there are investigators in, particularly the banks that are large enough to have
10 multiple employees and entire compliance units, whose job it is to search and monitor
11 their customers' financial records for suspicious activity that must be reported?

12 A Yes.

13 Q And based on your experience both at a financial institution and at FinCEN,
14 that type of monitoring by a bank, by a financial institution of its own customers' data,
15 that's entirely legal, correct?

16 A Legal and required.

17 Q Legal and required?

18 A Yeah.

19 Q No subpoenas required, no -- no warrant is required?

20 A Correct.

21 Q And stepping back a bit, in addition to the statutes that we've just discussed,
22 part of the reason why banks are able to do that sort of monitoring, whatever monitoring
23 they determine necessary, of their own customers' transaction is because, many years
24 ago, the Supreme Court held that bank records -- customer bank records are the property
25 of the bank, not the individual customer and, therefore, the Fourth Amendment does not

1 apply to bank records.

2 Is that your understanding?

3 A I do not have an understanding one way or the other of that case.

4 Q Okay. But you are more familiar, as I think you just made clear, with all of
5 the statutes and the regulations --

6 A Correct.

7 Q -- that govern the banks and --

8 A And how they are generally understood, whether -- if that came from case
9 law, you know, I can't say one way or the other, but yes.

10 Q Now, in addition to being legally required to be in compliance with the Bank
11 Secrecy Act, banks also have a business interest in ensuring that their customers are not
12 using their products to finance terrorism or other illegal activities, correct?

13 A I mean, colloquially, I suppose I would agree with that. I don't really have
14 an opinion one way or the other on the commercials of it. That makes sense to me.

15 Q I mean, it would make sense to think that if word came out that a particular
16 institution was being used to finance a terrorist attack, that that could cause that
17 institution's stock to plummet --

18 A Absolutely.

19 Q -- or people to --

20 A Headline risk was a major -- yes. And, in fact, when I was in the private
21 sector before FinCEN and now, headline risk is something that compliance personnel
22 discuss.

23 Q And headline risk refers to?

24 A The risk that the company would be in headlines with -- that something
25 negative would be public, such as customers using the institution to facilitate money

1 laundering, terrorism, et cetera.

2 Q Okay. Thank you.

3 And banks can also be penalized for not having effective compliance programs or
4 having compliance programs that don't meet what's required by statute?

5 A Yes.

6 Q And they can incur civil penalties?

7 A Yes.

8 Q Give me just one moment.

9 Okay. We talked a little bit during the previous hour about FinCEN Exchanges,
10 and I want to talk about them a little bit more. And, again, we're just talking generally.
11 We're not going to talk about the particular Exchange right now.

12 So, again, I believe that we've established that while it's the bank's responsibility
13 to identify and report suspicious activity at their institutions, banks regularly engage with
14 both FinCEN and law enforcement agencies in order to understand how criminal actors
15 are operating.

16 Is that a fair statement?

17 A I -- what do you mean by engage? Like, actually communicate with them?

18 Q Communicate.

19 A I would say that the overwhelming majority of regulated financial
20 institutions do not regularly communicate with FinCEN. They, of course, file the
21 required reports with FinCEN. But in terms of actual communication or things of that
22 nature, I would say most do not. And I -- even the ones that do, there's -- there's only a
23 very small handful that I would say do it regularly.

24 Q So when you have a FinCEN Exchange event, is that typically with, like,
25 repeat players, the same --

1 A So, generally, what would happen, if -- if it was a FinCEN Exchange that was
2 tactical on a particular topic, is some combination of law enforcement and the
3 appropriate FinCEN personnel would try to identify, based on the SARs and the other BSA
4 data, which institutions would be most useful to participate and would extend an
5 invitation -- if there was no objection to a particular institution, would extend an
6 invitation to those institutions.

7 Because of the nature of specific banks and just the market share that they have,
8 there were definitely some repeat players just because so many of the financial
9 transactions in our ecosystem go through the same small handful. So those were the
10 ones that would definitely have communicated with FinCEN regularly.

11 Q Okay. And you mentioned invitations. So FinCEN would send out
12 invitations to the financial institutions that it wanted to participate in Exchange events?

13 A Yes.

14 Q And those institutions were free to decline that invitation if they chose?

15 A Yes.

16 Q And the purpose of those Exchanges, again, was for law enforcement to
17 share information, typologies, that sort of information that would help banks -- that
18 FinCEN thought would help banks better identify suspicious transactions on their --

19 A Law enforcement and FinCEN, yes.

20 Q Okay. And -- well, let me back up.

21 Law enforcement is providing, through FinCEN, through the Exchanges, guidance
22 to the banks in these Exchanges about particular terms or particular trends that they're
23 seeing or that they think they might be seeing for banks to keep an eye out for.

24 A Yes.

25 Q Is that a fair statement?

1 A Yes.

2 Q And, again, banks are free to do what they want with that information?

3 A Yes.

4 Q And FinCEN Exchanges were actually developed as a means to facilitate this
5 sort of information sharing between banks and law enforcement, correct?

6 A Yes.

7 Q And is it a two-way street? Do banks share information as well?

8 A Yes.

9 Q Okay. And so banks will sometimes alert other banks or law enforcement
10 to, these are some of the trends that we're seeing, or these are the search terms that we
11 use to help identify suspicious activities?

12 A Yes.

13 Q And as we just established, banks are -- this is something that banks are
14 doing on their own regularly because they're required by statute to identify suspicious
15 activity?

16 A Yes.

17 Q And also because they just don't want their institutions to be used to finance
18 terrorism or to be engaged in money laundering?

19 A Yes.

20 Q And while you were still at FinCEN, Congress actually codified the FinCEN
21 Exchange as part of the anti-money Laundering Act of 2020. Is that your understanding?

22 A Yes.

23 Q Okay. And so what that means is that, through legislation, Congress
24 actually formalized this mechanism for law enforcement to share information with
25 financial -- financial institutions?

1 A Correct.

2 Q For national security and to combat the financing of terrorism?

3 A I don't recall the specific language of the statute and what the purposes
4 were that were enumerated, but that's generally my understanding.

5 Q And I believe in the earlier hour you were asked about, again, the mission
6 statement of FinCEN Exchanges, and you said that you would defer to FinCEN on that
7 since you're no longer there.

8 And I just want to introduce into the record a FinCEN fact sheet -- FinCEN
9 Exchange fact sheet that FinCEN put out.

10 Are we on exhibit 4 now?

11 [REDACTED] Exhibit No. 4.

12 [REDACTED] was marked for identification.]

13 [REDACTED] Okay.

14 BY [REDACTED]

15 Q Okay. So if we look at just the very beginning of this fact sheet, it says that
16 on January 1st, 2021, Congress enacted the anti-money Laundering Act of 2020, and that
17 section 6103 of that Act establishes the FinCEN Exchange to facilitate a voluntary
18 public-private information-sharing partnership between law enforcement agencies,
19 national security agencies, financial institutions, and FinCEN to effectively combat money
20 laundering, terrorism financing, organized crime and other financial crimes; protect the
21 financial system from illicit use; and promote national security.

22 Did I read that correctly.

23 A Yes.

24 Q And is that your understanding with FinCEN's mission?

25 A Yes.

1 Q Okay. And, "The objective of FinCEN Exchange is to develop, deliver, and
2 sustain innovative public-private information sharing in order to enable the private sector
3 to better identify risks and provide FinCEN and law enforcement with critical information
4 to disrupt money laundering, terrorism financing, and other financial crimes."

5 Did I read that correctly?

6 A Yes.

7 Q And, again, is that consistent with your understanding of the FinCEN
8 Exchange?

9 A Yes.

10 Q And is that consistent with the work that you were doing in setting up
11 FinCEN Exchanges?

12 A Yes.

13 Q Now, I believe you said earlier, far more articulately than I ever could, that
14 FinCEN would never direct a bank, you must file a SAR if you see X, correct?

15 A Correct.

16 Q And so when FinCEN provides banks with typologies, it's not FinCEN's intent
17 to say that, if you see any one of the phrases in these typologies, file a SAR?

18 A Correct.

19 Q It's something that is just used as guidance for banks to consider in terms of
20 all of the other factors they consider when they're determining whether or not to file a
21 SAR?

22 A That's correct. I would add, a lot of times, it's to help them narrow the
23 scope of what they're looking at, right. So -- especially if you talk about the really large
24 institutions that have millions of customers, millions -- millions and millions of
25 transactions. They're running -- their program will run -- it's called the detection

1 scenario -- but run a pretty high-level algorithm to capture generic red flags. That's
2 what an investigator is looking at to try to figure out if they should file a SAR.

3 If FinCEN or law enforcement is able to provide a financial institution with higher
4 quality red flags, it helps narrow the focus of what they have to look for and makes it
5 more likely that they might be able to identify suspicious activity, but it in no way implies
6 that that makes something suspicious in and of itself. It's -- it's a -- it's an attempt to
7 improve their ability to search for suspicious activity.

8 Q Okay. And banks can take that information and then integrate it into the
9 other types of red flags or the other types of investigative techniques that they might
10 use?

11 A Correct.

12 Q So, for example, if FinCEN submits some typologies and a bank identifies a
13 customer whose transactions fit some of those typologies, bank investigators might then
14 choose to investigate that customer a little more closely, for example, by looking at their
15 social media, correct? Is that something that banks do?

16 A Yes, that is something that could be done, that sometimes a bank would do,
17 sure.

18 Q So banks are, in your experience on both sides of -- of this relationship, doing
19 more holistic investigations of their customers than just using FinCEN typologies?

20 A Correct.

21 Q But the typologies are there because, as you said, some of these banks have
22 millions and millions of customers, and you want to make sure that their searches are as
23 efficient and as effective as possible?

24 A Correct.

25 Q And you're doing that to, ultimately, protect the safety of Americans and of

1 our financial institutions, correct?

2 A Correct.

3 Q And, again, when FinCEN sends out this guidance and sends out these red
4 flags, it is ultimately the bank's responsibility to determine whether or not to use them
5 and whether or not to file any SARs if they do use them?

6 A Correct.

7 Q FinCEN does not ask banks to file SARs?

8 A Correct.

9 Q FinCEN does not instruct banks to file SARs?

10 A Not at any specific level of granularity. I mean, they're required to have a
11 program generally to file SARs.

12 Q Correct.

13 A But, no, not --

14 Q But not a particular SAR?

15 A Correct. Not at a topical or a specific level, correct.

16 Q You're simply there to help provide guidance to help the banks comply with
17 their responsibilities and help keep us all safe?

18 A Correct. And to do what we're required to do, right. One of the statutes
19 you submitted earlier requires us to analyze the data that's given to us and disseminate
20 those typologies. That's -- that's -- FinCEN views that as a requirement of the statute.

21 Q Thank you very much.

22 [REDACTED] And we can go off the record.

23 [Recess.]

24 [REDACTED] We can go back on the record.

25

BY [REDACTED]

1 Q I just want to run through a few questions, and then we can -- can move to
2 another topic.

3 Earlier you mentioned an example where a financial inst- -- the FBI was seeking
4 data from a financial institution, and the financial institution misunderstood the things
5 that it could share.

6 Do you recall that.

7 A Yes.

8 Q Was there ever an example where the FBI was seeking data from a financial
9 institution that it wasn't entitled to receive?

10 A So, yeah, let me -- let me clarify what the example was. The answer to
11 your question is no, not that I recall.

12 The SARs statute provides that law enforcement is able to obtain, under the BSA,
13 without additional process, supporting documentation that underlies the filing of a SAR.
14 So what happens, in practice, is a law enforcement agent will be querying the database,
15 they'll see a particular SAR. It might be relevant to their investigation, so they will reach
16 out to the filing institution and ask for that supporting documentation. Could be a file of
17 transactions, a screenshot of something that was, you know, a Google result -- I mean,
18 who knows? But that's what that mechanism is, and that's just provided for in the BSA.
19 And financial institutions are allowed and required to turn that over to law enforcement.

20 A less sophisticated institution sometimes might not fully appreciate that they're
21 allowed to do that without process, et cetera. So there's that -- a point of confusion
22 that sometimes would come to FinCEN that we would be able to clarify and help.

23 I'm not aware of an example of what I had described outside of what I just
24 described. Any other kind of data or that law enforcement was seeking outside of what
25 I just described, I'm not familiar with.

1 Q Moving back to the audits. Did you audit every agency that had access to
2 the BSA data?

3 A I'm going to answer that this way: Every agency that had access to data
4 was in scope of the audit program. I don't have, of course, any specific recollection
5 about which specific agencies were and were not audited while I was at FinCEN.

6 Q So some agencies may have not been audited?

7 A Correct. I just don't recall.

8 [REDACTED] Just during your time at FinCEN, but presumably at some point,
9 they are subject to audits if they have access to the data?

10 [REDACTED] Yes. I mean, they're always subject to the audit and, presumably,
11 at some point, unless their access is quite new, an audit would have been performed at
12 some point of a particular agency.

13 [REDACTED] What was the name of those results, those audit results? Like,
14 was it a kind of report, was it a memorandum?

15 [REDACTED] Yeah. It was a report -- not sure I recall if it was in the form of a
16 memo or whatnot, but some written documentation of the conclusions of the staffer that
17 performed the audit.

1 [12:11 p.m.]

2 [REDACTED] Into the agency being audited?

3 [REDACTED] Oh, no. That would be internal documentation. I don't recall
4 there being any actual -- unless something needed to be addressed, I don't recall that
5 there was any like results or report delivered to the agency being audited.

6 [REDACTED] Yeah. Okay. So internally what were those audit results
7 titled? How was that --

8 [REDACTED] Oh, I don't recall. It would have just been a written report. I use
9 "report" very generally to mean something written that documented to an extent the
10 conclusions of the auditor and the steps performed internal to FinCEN.

11 [REDACTED] I just want to make sure we're using "audit" like in the same
12 context, because this is not -- I think what you're talking about is not an audit by like the
13 Treasury OIG or the Treasury auditors. This is like an audit inspection by FinCEN
14 employees.

15 So I just want to make sure we're using the term "audit" in the same way. Is that
16 accurate?

17 [REDACTED] Yeah. No, no. Thank you.

18 Not at all OIG, GAO related. No private sector involvement. This is purely the
19 agencies that have access to the FinCEN database, FinCEN personnel examining that
20 access called an audit, and then documenting those conclusions internally.

21 BY [REDACTED]

22 Q Are you familiar with Agency Integrated Access?

23 A Agency Integrated Access?

24 I recall the term, so I might be able to -- I don't recall anything specific, but if there
25 is something that can jog my memory, I'm happy to take a look at it. But I recall the

1 term.

2 Q It may relate to the memorandums of understanding that certain agencies
3 have with FinCEN and accessing BSA data? And maybe we can just talk about those
4 memorandums of understanding.

5 A Sure, sure, sure. Yes.

6 Q Can you talk about in general what the function of the memorandums of
7 understanding served?

8 A Sure, to an extent. They were sort of jointly owned by my division and
9 counsel. They're, I guess, contracts, if you will.

10 But it basically provided for the legal authorities under which the access was being
11 provided. It would contain the manner of expected usage, limitations on usage, if any.

12 Just by way of example, the MOU for a traditional law enforcement agency might
13 look different than an -- will look different than an MOU for a regulator, which would look
14 different than an MOU for a member of the intelligence community, different authorities,
15 different functions.

16 And the MOU would provide for the parameters under which a particular agency
17 would be able to access and use the data.

18 Q How could a memorandum change -- a memorandum of understanding
19 change the parameters by which a law enforcement agency, for example, could access
20 that data?

21 A Well, it would set out the permissible parameters. And, generally, it would
22 be aligned with the mission of the law enforcement agency.

23 So, as you know, law enforcement agencies, members of the intelligence
24 community, regulators, they all operate under specific authorities that allow them to do
25 things and not do things.

1 So the MOU, by and large, would document that the user would only be able to
2 use the data in a manner consistent with their authorities and their mission.

3 Q And so --

4 A And FinCEN's mission and authorities as well.

5 Q And so they could take the data in the FinCEN database and then use it to
6 run their own analytics according to the terms of the memorandums of understanding?

7 A And I think you just reminded me on what Integrated Access meant.

8 So the overwhelming majority of agencies that accessed FinCEN data did so
9 through FinCEN Portal. There were a small -- there was a small handful of agencies that
10 had the ability to ingest the data into its own systems.

11 If I'm not mistaken, I believe that the term Integrated Access is a reference to that.

12 Q From our understanding that's also correct.

13 A Yeah. Okay. I think, just getting your question.

14 So I think that was the term that was created to reference those agencies that had
15 FinCEN data ingested into their own systems.

16 I don't have any specific recollection on how they queried their systems and what
17 capabilities those systems had. I don't recall.

18 Q Do you recall which agencies used Agency Integrated Access?

19 A I don't specifically, no.

20 Q Are there any restrictions on how individuals can access or use the FinCEN
21 Portal?

22 ██████████ Well, I think you just described the MOUs that set out those
23 restrictions.

24 But are you asking --

25 BY ██████████

1 Q Well, the FinCEN Portal is different than AIA, right?

2 A Well, all of it would have an MOU, though.

3 Q Okay.

4 A Every agency that had access of any manner had an MOU in place. The
5 MOU would provide for the type of access. So if an agency had that form of access, it
6 would have been addressed in the MOU.

7 Q Okay.

8 A And so, yeah. So to your question, like, primarily, I would defer to the
9 MOU in terms of the restrictions.

10 Of course, we're talking about sensitive agencies. We're talking about law
11 enforcement agencies, regulators. So they had controls on their side in terms of who
12 has access to their systems or who was granted access to FinCEN's system.

13 The janitor and the tech guy probably didn't have the login credentials to do it.
14 But that sort of -- I'm not sure if that answers your question.

15 Q I'll switch gears.

16 How does FinCEN use advisories and typologies, other key terms, as part of the
17 Bank Secrecy Act regime? You touched on this a little bit earlier. I just want to put a
18 finer point on it.

19 A Well, a lot of ways.

20 So FinCEN's analysis of the data can help us derive those typologies to begin with.
21 FinCEN itself and our law enforcement partners would use those typologies to inform
22 their own analysis to either find suspicious activity or derive new typologies or more
23 refined typologies.

24 You mentioned advisories. You know, we -- FinCEN would disseminate those
25 typologies. We had multiple mechanisms to do so, but certainly an advisory was a

1 major one where FinCEN would publicly publish something, usually topical, and would go
2 through those typologies and red flags on that topic.

3 Q Which office at FinCEN is responsible for analyzing the BSA data?

4 A Depends on the purpose for which it's being analyzed. If you're talking
5 about from a typology perspective, I would say primarily it would be the Intelligence
6 Division, which is not a member of the IC. It's not to be confused with the intelligence
7 community.

8 Q Are SARs ever deleted from the FinCEN Portal?

9 A For the most part, I would say I'm not the right person to ask.

10 The only thing I can recall, there was -- so sometimes you have like duplicate
11 filings or other technical errors that we would sort of de-dupe. I'm not sure if things
12 were deleted. The word I recall is "suppression."

13 So there may be -- there was a mechanism, I think, to ensure that those things
14 weren't popping up on the searches in a redundant manner.

15 I don't have any recollection one way or the other of whether there were any
16 substantive deletions or suppressions or anything of that nature.

17 [REDACTED] Is FinCEN notified when a SAR is reviewed, when one of these
18 divisions runs a query?

19 [REDACTED] FinCEN has access to that information. I don't recall
20 the mechanism. When you say notified, I don't know if there's a ping or something like
21 that.

22 But, yes, FinCEN personnel have the ability to see who is searching and what
23 they're searching.

24 [REDACTED] So each query that is run there is a record of that somewhere?

25 [REDACTED] To the best of my recollection, I believe that's correct.

1 [REDACTED] And I want to make sure we're distinguishing between a
2 record.

3 Are you aware of anyone at FinCEN affirmatively getting notice any time someone
4 conducts a review in the BSA database?

5 [REDACTED] I don't believe --

6 [REDACTED] Anyone in your division.

7 [REDACTED] I don't recall. I don't recall that one way or the other.

8 [REDACTED] We talked about earlier, in the earlier hour, the private sector
9 sharing materials with your office.

10 Verbal response, please.

11 [REDACTED] Oh, sorry.

12 [REDACTED] Was that a question?

13 [REDACTED] Yes, we talked about that earlier?

14 BY [REDACTED]

15 Q Yes.

16 A Oh, okay.

17 Q And what kinds of materials do the private sector often share? Or did it
18 depend?

19 A Yeah, I mean, it would depend. So they would, of course, file all the
20 required reports, SARs, CTRs, whatever was required, and that would go in the database.
21 I don't know if that's what you meant by sharing, but that would be a form of it.

22 You know, there are of course limitations to what they can share. They can't
23 share PII or anything of that nature outside of what allows them to do so, such as a SAR or
24 if it's a subpoena for law enforcement or something like that.

25 If you're talking about like the red flag typology level, it would depend on the

1 context. It could be a FinCEN Exchange where we're talking about a particular topic and
2 a financial institution in attendance might offer some high level, "Here's the trend that
3 we're seeing," or, "Here's a search that we found helpful to find X," things of that nature.

4 Q So when you received those materials, what did you do next with them?

5 [REDACTED] So I guess can we first establish like would you personally have
6 received those materials?

7 [REDACTED] Well, so it's -- not to go all Bill Clinton. It depends on what you
8 mean by "receive."

9 So a lot of this might be like a verbal conversation where -- I'm not sure there was
10 an official receipt. I mean, there may have been someone taking notes. Really it was a
11 collaborative discussion. So there may not have been anything physically received.

12 To the extent that that constitutes receipt, I would have been in the room. So I
13 would have been someone who heard the info, but it certainly wasn't my role to do
14 anything with the substance.

15 I and my staff, we didn't analyze SARs. We didn't engage in typologies and red
16 flags. You know, when it came to those kinds of collaborative efforts, we were more
17 logistics and planning the event and other components. Law enforcement attendees
18 would be sort of engaged in the substance.

19 BY [REDACTED]

20 Q Did the private sector ever flag or make you aware of particular SARs that
21 had been filed with FinCEN?

22 A So I can confidently say never in the context of a FinCEN Exchange because it
23 would have been a violation of confidentiality for them to discuss specific SARs in the
24 presence of other members of the private sector.

25 I don't have specific -- I do have a general recollection that there were times a

1 financial institution flagged for FinCEN a particular filing, like, "You should take a look at
2 this."

3 In fact, FinCEN also maintains a hotline for like emergency -- if somebody sees
4 something, was like, "Oh, crap, I need to pick up the phone and call somebody," FinCEN
5 actually has a hotline for that.

6 So I do have a general recollection that that occurred.

7 Q Did other liaison offices share information with the private sector, or would
8 that have always went through the Office of Stakeholder Engagement and Integration?

9 A No. I mean, it's such a broad question. There were certainly reasons why
10 multiple of FinCEN's components would have reason to exchange information with
11 stakeholders.

12

BY [REDACTED]

13 Q Just a clarifying question. The hotline two responses ago you mentioned,
14 that's separate from the customer support?

15 A I'm not even sure if it's -- I think it's a different phone number.

16 Q Okay.

17 A I'm not sure if that's your question. But it's a separate mechanism, yes.
18 It's a different team.

19 Q And who is on the receiving -- yeah, which team is on the receiving end of
20 that?

21 A Oh, gosh. I don't know what division they're in. That's a good question.
22 I don't know.

23 Q It's not your division?

24 A I don't -- it wasn't my office.

25 Q Okay.

1 A I don't believe -- I was deputy at a division for a minute. So I'm trying to
2 remember.

3 I don't recall who sits on the other side of that, of the substantive hotline. The
4 customer support was a different office within SOD.

5 Q Do you remember the internal name of what the substantive hotline was
6 called, like if we needed to reference it?

7 A I think it's literally called FinCEN Hotline. It's on the website somewhere.
8 Actually, I think it might even be in the regulation. I don't -- I want to say I believe it was
9 FinCEN Hotline, but I don't specifically recall.

10 Q And understanding you're going off a general recollection, you don't have a
11 specific recollection of an example, do you have a sense of how many times this hotline
12 would be used?

13 A No. No idea. And I don't even have a ballpark. I wasn't engaged in that,
14 not at all.

15 BY ██████████

16 Q When you would share materials in a FinCEN Exchange event or typologies,
17 what sort of approval process did you go through, if any, before sending those materials
18 out?

19 A Yeah. So let me take a bit of a step back.

20 "You," meaning ██████████ or FinCEN, right?

21 So I would not have been involved in the creation or analysis of any of that
22 information. So I can't speak to the extent to which -- I can't speak to what the approval
23 process was for that information to be finalized within FinCEN.

24 If at some point it came to me or my staff for dissemination, that -- I mean, at a
25 minimum, I would make sure that my direct leadership was -- approved of that.

1 At times -- again, from a dissemination perspective, which is all I can speak to -- at
2 times that may also include consulting FinCEN counsel and consulting FinCEN front office.

3 But, again, I can only speak to the dissemination. The actual content of what I
4 was disseminating, I can't speak to at all.

5 Q So when you received those -- the content that you were disseminating, who
6 did that ordinarily come from?

7 A Usually it would come from the Intelligence Division. It could come from
8 the front office if there was like a member of the director's staff that was working with
9 other FinCEN components or harmonizing. But to the best of my recollection, it
10 probably usually would have been the Intelligence Division.

11 Q And what are the ways you could share that information or disseminate it?

12 A I mean, assuming I got approval to disseminate it, it could be email. I'm
13 trying to remember if there was any kind of like secure portal, whatever. You know,
14 obviously, the private sector doesn't have access to the FinCEN database.

15 So my recollection is it was primarily email or presentation at an event. So there
16 were some times where something was spoken about verbally in an exchange or BSAAG
17 or something that wasn't physically disseminated.

18 Q Did your office coordinate with other Federal agencies, like the IRS?

19 A Yes.

20 Q Can you describe the -- that nature of that coordination?

21 A Yeah. Our relationship with the IRS would primarily have been one of two
22 components, either IRS CI in its capacity as a Federal law enforcement agency, or IRS
23 SBSE, which I think stands for Small Business and Self-Employed, which IRS is a functional
24 regulator as well.

25 So I was -- we're not usually talking with the tax folks as we think of IRS normally.

1 So it was the IRS as a law enforcement agency or the IRS as a regulator.

2 Q And did you disseminate the kinds of materials that were also disseminated
3 to the private sector to the IRS?

4 A Well, the IRS would have had access to the FinCEN database.

5 To the extent that the IRS had a reason to be on the dissemination, if you will, so
6 like, for example, if IRS CI was the law enforcement stakeholder for FinCEN Exchange,
7 then presumably they would have been in the room when these things were discussed.
8 I don't have a specific recollection, but I may have disseminated something to them in
9 that context.

10 Q What about the Department of Homeland Security? Did you work with
11 them?

12 A Yes. I would say, again, in their capacity as a law enforcement agency.

13 Q Did you work with any intelligence agencies?

14 A Yes.

15 Q Which ones?

16 A Well, most, if not all, would have access to the database. So I would work
17 with them in that context from a data access perspective, MOU perspective.

18 There were one or two projects at the Top Secret level that I can't speak about
19 that I had some touch points to with the IC. But, again, as someone who was not
20 engaged in substantive analysis, I had very little engagement with IC.

21 BY [REDACTED]

22 Q For the IRS, for the law enforcement wing, would you have similar
23 interactions to what you had with Federal law enforcement where --

24 A Yeah, I mean, they're one of the big five. So IRS CI would have been like
25 DEA, FBI to me. It was just a big Federal law enforcement agency.

1 Q You had mentioned when disseminating information there might be
2 occasions where it called on elevating up to the front office. What types of information
3 would you feel would be appropriate to elevate to the front office's attention?

4 A So I'm not sure it's a matter of elevating. If I was being asked to
5 disseminate something, then I would need approval to feel comfortable disseminating it.
6 It's possible that the person who gave it to me was of sufficient. It could have been the
7 senior adviser for the director or the head of ID, Intelligence. I mean, it could have been
8 somebody where I didn't feel the need to get somebody else's approval. It could have
9 been somebody where I would go to my leadership.

10 It sounds like you're more asking about like what kind of issue might I have seen
11 that would cause me to escalate something. Like, I guess I'm not really clear on what
12 you mean.

13 Q In an earlier response, you gave a pretty clear bottom line in your head as far
14 as creation and assessment versus dissemination. And then so just focus on that latter
15 category.

16 A Uh-huh.

17 Q Either specific recollections or a hypothetical based off your experience and
18 your job, what types of information where you had received an instruction that this can
19 be disseminated would you look at and say, "This is something I should at least flag," or --

20 A Oh, I see what you mean.

21 I'm not sure that it was a specific type of information that would cause me to feel
22 compelled to get approval one way or the other. As a general matter, I would get
23 approval.

24 I mean, we weren't regularly in the business of just sending stuff to financial
25 institutions. It would have been in context, an advisory that is published, a FinCEN

1 Exchange that we are hosting, a BSAAG working group that we are facilitating.

2 It is not the case that somebody would come to me and say, "Hey, here's a
3 PowerPoint. Can you send this to X, Y, Z bank?" That's really not something that
4 happened.

5 So that's why I'm sort of struggling to answer the question, because the
6 information I was being asked to disseminate would have been in the context of a
7 particular reason to disseminate.

8 And so I would either have prior knowledge that I was able to disseminate, and I
9 was expecting to receive something, and once I did and the appropriate people made me
10 feel comfortable that it was what I could disseminate, I would do it, or I would ask my
11 boss.

12 But it wasn't like I read something and said, "Ooh, this is about X. I'd better ask
13 somebody first." It wasn't really a substantive assessment, if that makes sense.

14 Q Was there any part in the process that you played where you were
15 conducting any sort of substantive assessment?

16 A Not that I can recall. I've been telling you guys on the phone for 6 months
17 you've got the wrong guy. But I don't recall. I don't think I ever did that at FinCEN.

18 Q For the Intelligence Division, who was the head of that when you were at
19 FinCEN?

20 A For most of the time I was there, it was a guy named Jimmy Kirby.

21 Q Kirby?

22 A Yeah, K-i-r-b-y. I believe he's still at FinCEN, or at least he was as of a
23 couple months ago.

24 [REDACTED] He is.

25 BY [REDACTED]

1 Q Who is the right guy?

2 A The right guy of?

3 Q Well, you said we don't have the right guy.

4 A Oh, it depends what your question is.

5 I mean, if you want to talk about the substance of what we were exchanging at
6 FinCEN Exchange, it would be law enforcement or maybe Jimmy.

7 Q Did you coordinate with any offices from the FBI?

8 A For what?

9 Q Did you coordinate with any offices from the FBI?

10 A Coordinate what?

11 Q Did you communicate with offices from the FBI?

12 A Yes.

13 Q Do you remember which offices?

14 [REDACTED] I think he's already testified about this. Like, I mean, he
15 testified about this at the very beginning of your questioning. So is there a specific topic
16 you want to ask him about?

17 [REDACTED] Did you work with the Strategic Partner Engagement Section?

18 [REDACTED] Not that I -- yeah, I mean, I would reiterate what I said earlier, which
19 is I'm not sure I ever knew or identified or distinguished where they came from. So I
20 couldn't really tell you one way or the other what office they were from.

21 [REDACTED] Did you interact with Peter Sullivan?

22 [REDACTED] I recall the name. I don't have any specific recollection of any
23 particular engagement with him.

24 [REDACTED] With the understanding you don't have any specific recollection, at a
25 general level, do you recall what types of issues or what might occasion interacting with

1 Mr. Sullivan?

2 [REDACTED] No. Like zero. I just vaguely recall the name.

3 [REDACTED] As part of your vague recollection, do you recall ever meeting him in
4 person or at those meetings? Any additional context?

5 [REDACTED] No.

6 [REDACTED] Are you aware of FinCEN sending SARs directly to the FBI or any
7 other law enforcement agency?

8 [REDACTED] I would ask there what you mean by "sending," just because
9 FinCEN makes them available pretty much immediately to all law enforcement agents
10 that have an MOU. So what do you mean by "send"?

11 BY [REDACTED]

12 Q Aside from access via the Portal, was a SAR ever directed to the FBI?

13 A I generally recall there were times where we would flag specific filing ID
14 numbers to them with which they could use to query the database and get the
15 information through the standard mechanism. And that was actually a control that
16 FinCEN had in place.

17 We tried to minimize as much as possible access to BSA data outside of the
18 normal channels because, just from a governance and tracking perspective, we wanted it
19 to be through the normal channels.

20 So I don't recall physically sending SARs or that happening one way or the other.
21 I don't recall.

22 I do, again, generally recall that there were times when we would say here's a list
23 of five ID numbers to look up.

24 Q Have you ever heard of executives at financial institutions sending SARs via a
25 secure email portal directly to the FBI once the SAR is published on the FinCEN Portal?

1 Q Yes.

2 A Right.

3 So as part of our advisory program -- so when FinCEN would publish an advisory,
4 they would usually include a specific term.

5 I mean, it would be -- it wouldn't have any meaning necessarily. It would just be
6 a term with a request that institutions filing SARs related to this topic include that term
7 for ease of searchability for law enforcement and FinCEN -- tracking, metrics, what's the
8 value of our advisory, et cetera, et cetera.

9 So I believe that -- my recollection is there was an effort to do that here so when
10 SARs were filed related to this topic we would be able to retrieve them quickly and easily.

11 Q That topic being the Capitol riots?

12 A Yes.

13 Q And are you aware whether this reference was also shared with other
14 Federal agencies? Would they be aware of it?

15 A I don't recall. I would not have been the one to have those conversations
16 with Federal agencies, so I don't know.

17 Q Who would have had those conversations?

18 A Intelligence Division possibly, front office personnel possibly, my chain of
19 command, AnnaLou, possibly.

20 [REDACTED] And just so it's clear for the record, if somebody from, say, the
21 FBI was looking at a filing that had this in the BSA portal, would they be able to see it?
22 Would they be able to see that filing code if a SAR had used that filing code?

23 [REDACTED] Yeah, it's usually thrown into what they call the narrative. The SAR
24 form has mostly fixed fields and then there's like a narrative field where you actually
25 describe the conduct. So generally it was just a reference that was thrown into the

1 narrative in the free form field.

2 But if a law enforcement or anybody with access to the data -- database -- knew to
3 search for the code, they could retrieve the SARs that had that code.

4

BY [REDACTED]

5 Q The email also thanks the invitees for their time earlier today. Was there a
6 call or Zoom before this email was sent, to your recollection?

7 A I don't specifically recall. That's certainly what it sounds like.

8 Q Do you know if there were any other Federal agencies besides FinCEN on the
9 call?

10 A I do have a general recollection that some of the calls that we had with this
11 group around this time also included law enforcement. I don't know what specific
12 conversation this is referring to and who was on it.

13 Q Do you know what law enforcement would have been on related calls?

14 A I actually don't have a specific recollection. I know we're talking about the
15 FBI. I don't have a specific recollection other than I know it was some DOJ components.
16 I do recall some AUSAs -- or I don't remember if it was Main Justice or AUSAs -- but I do
17 recall some of the lawyers.

18 And I have since gathered, just based on the reports you all have filed and
19 whatnot, it was the FBI, but I don't actually specifically recall.

20 Q The email also notes there will be daily Zoom invites. What purpose did
21 those further conversations have? And that's in the last bullet.

22 A So my recollection in the aftermath of January 6th is that there were ongoing
23 concerns not just about those who had participated in those events but ongoing concerns
24 about the possibility of future events.

25 I don't remember the date of the inauguration, but, obviously, the inauguration

1 was very shortly after the 6th, and there were concerns about that.

2 So I do know that when we stood up this group at some point we went to a
3 cadence where we spoke daily, more than once a week, I don't remember the specific
4 cadence -- obviously, at some point daily was contemplated -- to touch base on this topic.

5 Q The email also notes the "standard e-file process." Could you describe
6 that?

7 A That would have just been a reference to how the financial institutions filed
8 SARs in the normal course of business. And just to get ahead of you, and I know you
9 actually -- this jogs my memory of a question you asked a few minutes ago.

10 So FinCEN maintained this system called SISS, Secure Information Sharing System,
11 which the system serves multiple purposes, but it has the ability for financial institutions
12 with access to the system to submit files to FinCEN.

13 So not to get too technical, and I'm not the right person anyway, when a financial
14 institution files a form with FinCEN, whether it's a SAR or some other form, there is like a
15 day or two of a lag in its process -- like, it's got to process and do computer stuff that I
16 can't tell you about.

17 And so there was a conversation in this context about asking the group to upload
18 their SARs into SISS so we had access to them immediately rather than waiting until
19 they've completed the sort of technological process.

20 So we were asking them to file as you normally would, but please also put this
21 code in and please also upload it to SISS.

22 BY [REDACTED]

23 Q Had you ever made that request before?

24 A I don't recall.

25 Q Had there been other occasions during your time at FinCEN that warranted

1 either having or considering daily Zooms or daily meetings?

2 A I don't recall.

3 Q Your answer about your general recollection about calls around this time
4 and not the one referenced in this email, about members from DOJ writ large, do you
5 recall any titles or names of DOJ personnel that you recognized on the calls?

6 A I do believe there was at least one AUSA.

7 Q Do you recall from which office or his or her name?

8 A No, I'm afraid not. I don't. I'm sorry.

9 Q Was it an AUSA that you had worked with previously?

10 A I don't recall.

11 Do you mind if I ask -- and, obviously, you're not going to tell me what's
12 redacted -- but is this law enforcement contact info that's redacted? Because it looks
13 like a handful of -- or are these just the name of people at these institutions that are
14 redacted?

15 [REDACTED] Yes.

16 [REDACTED] Okay.

17 [REDACTED] And it's my understanding that these are the institutions that you
18 sent the invite to.

19 [REDACTED] Got it. Okay. Understood. Thanks.

20 [REDACTED] Were there -- sorry. One more.

21 There is reference to daily Zooms. During this time, obviously, January 2021, the
22 pandemic is still going on, were there any in-person meetings that occurred?

23 [REDACTED] Not that I recall.

24

BY [REDACTED]

25 Q And why did you ask, "For all SARs filed related to this topic, please alert us

1 of the filing"? Was it normal for FinCEN employees to be alerted?

2 A Which bullet is that?

3 Q It's the fifth bullet.

4 A "For all SARs filed related to this topic, please alert us."

5 So what was your question?

6 Q Why did you ask to be alerted to all SARs filed related to this topic?

7 A I believe just because we wanted to know -- we wanted the knowledge as
8 soon as it was sent to us. You know, we didn't want to have to -- we didn't want there
9 to be a lag between when the information was submitted and when we queried it or
10 whatnot. We just asked for a heads-up that it was there.

11 Q And so once you were alerted to a SAR, what happened next?

12 A I don't recall, and I wouldn't have been involved.

13

BY [REDACTED]

14 Q Who would have been involved?

15 A If somebody was looking at the SAR or reading the SAR. I don't recall ever
16 even reviewing any of the SARs we received because that would have been substantive
17 analysis that was outside of my remit.

18 Q As it related to the events on January 6th and the days and weeks following,
19 which teams within FinCEN were taking the lead on that?

20 A To the best of my recollection, it would have been the Intelligence Division.

21 Q Do you have any sense of which offices within the division?

22 A No.

23 Q In advance of like the daily Zoom calls or calls during this period, would there
24 typically be internal FinCEN-only pre-meetings?

25 A I can safely say that that happened. We certainly had pre-meets, and we

1 absolutely would not have gone into this cold at the outset. I can't say whether there
2 was a pre-meet, for example, before each call or each further discussion. I would
3 suspect not. But I don't recall.

4 Q Which personnel from FinCEN would most commonly attend any
5 pre-meetings during this time period?

6 A Listen, ultimately my answer is I don't recall. A little bit of it would depend
7 on the nature of the pre-meet.

8 If it was a bit of a logistical pre-meet, like who's going to say what, when, and how
9 are we going to administer the discussion, that might just be, for example, my staff and I
10 and my leadership.

11 Maybe counsel would have joined, maybe front office would have joined, maybe
12 Intelligence Division would have joined, but if that was just logistics, maybe not.

13 If it was actually a discussion of substance, it would have included Intelligence
14 Division. And I can say that confidently because that's what would have happened.
15 But I don't actually have a specific recollection of any of the particular meetings.

16 Q Which personnel from the Intelligence Division would have likely
17 participated in any substantive pre-meetings?

18 A I don't specifically recall which members of that division were involved in any
19 particular topic. I would refer you -- the head of the division was Jimmy. The deputy
20 head, who is listed on here, was Kim Donovan. Those are the two.

21 That's not to say that they would have been on the calls at their level. I don't
22 recall one way or the other. But those are the only two names I recall from the
23 Intelligence Division definitely being involved generally.

24 Q For these types of calls around this timeframe -- daily Zooms, but not quite
25 daily -- what was FinCEN's protocol for taking any notes, recording minutes?

1 A I don't recall.

2 Q Outside of this context, just generally, was there a practice or a protocol as
3 far as how notes or if notes should be taken?

4 A As a general matter for the FinCEN Exchange program, I do recall there
5 would be someone at FinCEN to take notes. I don't recall whether that included -- I
6 don't recall whether those notes would have covered the whole discussion.

7 In other words, when -- if it was in the context -- like, if there were actual tactical
8 discussions of typologies, things like that, I don't recall whether or not there were notes
9 maintained on that. I just don't recall.

10 [REDACTED] Do you recall whether 2 weeks after the AML Act codifying
11 FinCEN Exchange became effective that policy of taking notes at FinCEN exchanges would
12 have been in effect?

13 [REDACTED] I don't recall.

14 [REDACTED] Not policy, whether that would have been your practice.

15 [REDACTED] Yeah, I don't -- I just don't recall.

16 BY [REDACTED]

17 Q Whenever the practice began and for whatever parts of the meeting notes
18 are being taken for, what did the final work product or final iteration look like? Was it
19 email, I'm assuming?

20 A Yeah, I don't recall. I really don't. I don't recall that FinCEN would ever
21 publish a summary -- well, actually, I take it back.

22 They would often -- FinCEN would publish a summary of an event, but I'm not sure
23 how much detail it would include in terms of the actual discussion, whether that would
24 be derived from notes that were taken or not. I just don't recall.

25 Q Again, just general recollection, not necessarily specific to this time period,

1 who would most likely within FinCEN have the responsibility for taking notes?

2 A So because I don't recall whether there was like a formal note-taking policy
3 or whether that was done, it's hard for me to answer that question.

4 If there were substantive conversations that took place and FinCEN wanted to
5 take the information back for our own purposes, that would likely have been Intelligence
6 Division, because they were one of the primary components of FinCEN that analyzed SARs
7 for that purpose.

8 But outside of that, like if there was some formal note-taking, which I don't recall
9 one way or the other, I, therefore, also don't recall who would have been responsible for
10 that. It's possible it was my own staff from a logistics standpoint. I just don't recall.

11 Q To your recollection, it wasn't you?

12 A To the best of my recollection, it definitely was not me. I really hate taking
13 notes, and I'm pretty sure I feel like I'd remember if I had to do it for these long events.
14 But I just don't recall.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

BY [REDACTED]

Q How long did these events normally last?

A Oh, gosh. It would depend on the event. So I'm talking about FinCEN Exchange generally, not any particular topic.

You know, pre-COVID, sometimes institutions would actually put people on a plane to meet in person. So we tried to make it like a full-day event, sometimes 2 days, maybe even incorporating educational elements, and we really tried to make it a substantive program.

Certainly, after COVID -- bearing in mind, I was only at FinCEN for about a year and change before COVID hit, most of which was policy. So for the majority -- maybe not at the very beginning of me taking over this office, but the majority of time that I was in this seat, I was in my apartment on a screen.

The events naturally got shorter. I think -- I recall early, middle pandemic we tried like a full day or like a 2-day either of BSAAG or FinCEN Exchange and it was just a disaster. I mean, people were dropping off. You just can't hold people's attention on a computer for that long.

So I do recall we made them shorter and to the point just when they were remote.

Q Were there other instances or investigations that you recall personally asking to be alerted to SARs filed on the topic?

A I mean, I don't specifically recall. Most of those events and advisories contain one of those reference codes. I guess that's not necessarily affirmative. But outside of that, I don't recall.

Q The email also asks that the financial institutions send you, quote, "the FBI's points of contact you are working with in relation to this subject matter."

Do you recall any of those FBI points of contact?

1 A No.

2 Q Why were financial institutions directly working with the FBI?

3 A Well, as a general matter, the FBI had access to SARs, and they had the
4 authority to reach out to the filing institution to get supporting documentation and to
5 discuss that particular SAR. So that happened frequently throughout the whole
6 ecosystem.

7 There are also certain institutions that if they see conduct that's of particular
8 concern, if it's, God forbid, something that's imminent or something like that, a lot of
9 times they would file a SAR and then pick up the phone and call various law enforcement
10 contacts.

11 So those are general manners in which that kind of communication could have
12 taken place.

13 FinCEN frequently saw multiple different players, sometimes multiple agencies
14 looking at the same conduct, and we would try to deconflict and make things a little more
15 efficient. So I think that's what we were trying to do here.

16 Q We have already covered this, I believe, but who is AnnaLou Tirol?

17 A So she -- I don't remember the specific dates -- around this time was the
18 associate director in charge -- oh, yeah, she was the ADA of my division.

19 Q Did you report to her?

20 A Dotted line. I think I technically reported to her deputy.

21 Q And what was your professional relationship to Kim Donovan?

22 A Just a colleague. She was a FinCEN employee in a different division.

23 Q And with Tony Harris?

24 A Tony was my employee. He was the section chief of one of my two
25 sections. So that section, the Domestic Engagement Section, that was one of two

1 sections in my office. Tony was the chief of that section. And that's the section that
2 oversaw FinCEN Exchange.

3 [REDACTED] Besides Kim Donovan, do you recall others from the Intelligence
4 Division that were participating in calls around this time?

5 [REDACTED] Jimmy and Kim are the only ones I can recall specifically being
6 involved in this.

7 [REDACTED] And Jimmy was the director of the Intelligence Division at that
8 time?

9 [REDACTED] Yeah. They called him associate director of FinCEN. But the ADs
10 were the heads of divisions. So Jimmy was the head of ID. Kim was his deputy.

11 [REDACTED] During the protests and riots in the summer of 2020,
12 beforehand, was there anything similar to this that took place with FinCEN and these
13 exchanges?

14 [REDACTED] I don't recall.

15 [REDACTED] Turning back to January 2021, for the calls when the FBI or members
16 of DOJ were on it, do you recall just broadly how many personnel from DOJ and FBI would
17 be on?

18 [REDACTED] I don't. More than one. But I don't -- more than one, less than
19 10. It could have been way less than 10. I don't specifically recall.

20

BY [REDACTED]

21 Q Who made the determination of which banks to include, which financial
22 institutions?

23 A I don't know.

24 Q Were there others included that are not listed here, or was it limited to
25 these?

1 A So I can say that everyone who was, quote, "included" on this date is on
2 here.

3 I have a general recollection that one or a few institutions might have been added
4 along the way as our analysis progressed or there was a reason for that, and I don't recall
5 whether that had already taken place or whether that was after this particular email.

6 Q Do you know how it was determined what banks to include?

7 A I don't.

8 [REDACTED] Was this part of a FinCEN Exchange event?

9 [REDACTED] So my recollection is that these discussions were stood up under a
10 handful of authorities. I don't recall -- I'm not sure I'm the right person to speak to what
11 specifically that was, but I have a specific recollection of FinCEN making sure that
12 conversations were taking place properly, under specific authorities that authorized these
13 kinds of discussions, but I don't specifically remember what that entailed.

14 [REDACTED] Who decides whether to create a reference number like the one
15 here?

16 [REDACTED] Who decides? That's a good question.

17 I don't know. I don't know. I mean, I don't think it's the type of thing where it's
18 like a decision panel, should we or shouldn't we? I think if there is a component of
19 FinCEN that feels the need to, they would raise that.

20 So I know generally the Intelligence Division or Policy Division, which is where the
21 advisories are released out of. So, again, these would commonly be found in an
22 advisory.

23 But that was more FinCEN practice. So maybe it was just Policy Division just
24 doing what the agency said. But I don't actually have a specific recollection.

25 [REDACTED] We can go off the record.

1 [Recess.]

1 [1:44 p.m.]

2 [REDACTED] We are back on the record.

3 BY [REDACTED]

4 Q So, [REDACTED] I want to ask you a little bit about January 6th.

5 I believe you said in the earlier hour that in the aftermath of January 6th there
6 were ongoing concerns not just about those who participated in the riots at the Capitol,
7 but also about violence at future events, particularly the upcoming inauguration, correct?

8 A Yes.

9 Q And so FinCEN was working with law enforcement and the banks to help
10 identify first who was involved in the January 6th attacks on the Capitol, correct?

11 A Yes.

12 Q And also to identify folks who might be at risk of committing future acts of
13 violence, particularly at the Presidential inauguration?

14 A Yes.

15 Q And you were asked a series of questions about whether the frequency of
16 the Zoom calls that were set up or the requests to be notified if a SAR was filed, if that
17 was something that had ever been done before.

18 Were the actions that you took, for example, in having daily phone calls, was that
19 in relation to the urgency of FinCEN's efforts to try to help all the relevant parties prevent
20 violence at the inauguration and other events?

21 A Yes.

22 Q And was that also the same with request -- with respect to your request to
23 have -- to be notified of any SARs that were filed in relation to January 6th?

24 A I don't recall.

25 Q Now, you were also asked if this was something that you had seen before at

1 your time at FinCEN.

2 While you were at FinCEN, was there any other violent attempt to interfere with
3 the peaceful transfer of power in this country?

4 A Not that I'm aware of, no.

5 Q Okay. And there wasn't an event of mass domestic violence and extremism
6 that we saw on January 6th while you were at FinCEN?

7 A I mean, I don't know I'm in a position to compare events. It certainly was
8 a -- yeah. I mean, versus, like, the marathon bombing or any other -- I'm not really in a
9 position to compare events.

10 Q Were you at FinCEN during the -- for the marathon bombing?

11 A I don't think so. When was the marathon bombing?

12 [REDACTED] I could not tell you, but --

13 [REDACTED] I don't recall.

14 [REDACTED] I believe it was well before you.

15 [REDACTED] I believe so. I don't recall. Yeah.

16 BY [REDACTED]

17 Q And, I mean, if you had worked on it specifically, you certainly don't
18 remember that?

19 A Correct.

20 Q Okay. So it's fair to say, based on your testimony, that FinCEN's work,
21 along with law enforcement and the banks, in the aftermath of January 6th was both
22 reactive, in terms of trying to figure out who was involved in January 6th, and proactive,
23 in terms of preventing future events, correct?

24 A Yes, absolutely.

25 Q And that's typical for FinCEN. FinCEN engages in both reactive and

1 proactive investigations. I don't mean about necessarily a specific event, but that --

2 A Yeah.

3 Q -- both fall within FinCEN's authority.

4 A Certainly, yes.

5 Q And like any other FinCEN Exchange or any other communication event, the
6 banks who participated in these exchanges after January 6th, their participation was
7 voluntary, correct?

8 A Correct.

9 Q They could have chosen not to communicate with FinCEN at all?

10 A Correct.

11 Q Other than filing SARs that they were required to under the law?

12 A Correct.

13 Q And the banks that did or financial institutions that did choose to participate,
14 any information that was shared with them, they were free to disregard if they so chose?

15 A I would certainly say that there was no specific requirement as to what they
16 were supposed to do with the information.

17 The extent to which they should have taken the information into account would
18 really have depended on the institution itself and their own assessment of their risk and
19 the relevancy of the information, et cetera, certainly not anything directed by FinCEN.

20 Q So it was up to the institution to determine to what extent --

21 A Entirely.

22 Q -- the information would be valuable?

23 A Yes.

24 Q And that's based on their own knowledge of their own customer base and
25 the scope of their presence nationwide, that sort of thing.

1 A Yes.

2 Q Okay.

3 A Among other things, yeah.

4 Q And you were asked some questions about the codes that were used. It's
5 fair to say -- and I believe this is how you explained it -- that the code is simply a shortcut
6 to help identify relevant SARs so that, rather than just going through the millions
7 individually, if law enforcement wants to identify SARs related to a specific event, perhaps
8 a specific type of crime, they can just type in the code, correct?

9 A Yes.

10 Q Okay. And you talked about the FinCEN Portal that had been set up and
11 the SISS system. Are those two different things?

12 A Yes, they are different things.

13 Q Okay. Can you explain the difference to me?

14 A So not in a very technical level, but the --

15 Q Fair enough. And that wasn't my question. Just more generally.

16 A Yeah. The FinCEN Portal is what I'm saying is a reference to -- when we say
17 the database of the BSA information that is filed with FinCEN, it's in the portal. I mean,
18 I'm sure there might be multiple systems at a technical level of how we ingest and get the
19 data into the portal and searchable. I don't really know any of the guts of the system.

20 But when I say FinCEN Portal, we're talking about the traditional database of BSA
21 data that's filed with FinCEN and then made accessible to those agencies that are entitled
22 to have it.

23 SISS is a secure information-sharing system separate from the portal, and it's a
24 mechanism -- so FinCEN uses it -- I don't want to take us on a tangent, but there are some
25 information-sharing mechanisms provided for in the USA PATRIOT Act, section 314(a) in

1 particular. SISS is -- and section 314(b). SISS facilitates those mechanisms.

2 FinCEN also has other information-collection authorities that they will sometimes
3 use SISS to collect the information. So it's more of an ad hoc manner of information
4 collection than the formal e-filing and portal process.

5 Q But it's an information-sharing system that is set up pursuant to the
6 authorities that permit FinCEN --

7 A Absolutely.

8 Q -- to share information.

9 A Correct.

10 Q Now, you mentioned section 314 of the PATRIOT Act, so I just want to
11 discuss that very briefly. And I'm actually going to introduce it. I will not be
12 introducing the entire PATRIOT Act, thankfully, just section 314.

13 So this will be exhibit 6.

14 [REDACTED] Exhibit No. 6.

15 was marked for identification.]

16 BY [REDACTED]

17 Q So if you look on the second page, section 314(a) -- well, section 314 itself is
18 entitled "Cooperative Efforts to Deter Money Laundering," correct?

19 A Yes.

20 Q And section 314(a) is entitled "Cooperation Among Financial Institutions,
21 Regulatory Authorities, and Law Enforcement Authorities," correct?

22 A Yes.

23 Q And it states as follows: "The Secretary shall, within 120 days after the
24 date of enactment of this Act, adopt regulations to encourage further cooperation among
25 financial institutions, their regulatory authorities, and law enforcement authorities with a

1 specific purpose of encouraging regulatory authorities and law enforcement authorities
2 to share with financial institutions information regarding individuals, entities, and
3 organizations engaged in or reasonably suspected, based on credible evidence, of
4 engaging in terrorist acts or money laundering activities."

5 Did I read that correctly?

6 A Yes.

7 Q Okay. And then section 2 talks about the cooperation and
8 information-sharing procedures, correct?

9 A Yes.

10 Q Okay. Now, this type of information sharing that's described in section
11 314(a), that's part of what FinCEN was doing in the weeks after January 6th, correct?

12 A It was one of the several authorities that were being leveraged during that
13 period of time for the information sharing. In particular, it was the authority we would
14 use.

15 If we needed -- if FinCEN needed to disseminate specific indicators, for example,
16 like at the PII level, we would often use 314(a) as the mechanism to disseminate it.
17 That's not something we would just get on a Zoom and start talking about [REDACTED]
18 But we might do that via 314(a).

19 Q And so when you say specific information at the PII level, does that mean
20 that it's come to FinCEN's attention or a law enforcement agency's attention, they have a
21 particular individual in mind that's a suspect, and they want to ask financial institutions to
22 look for transactions that that person engaged in, they would use section 314(a)?

23 A Correct.

24 Q Okay. And can you explain a little bit more about how that process works?

25 A So there's a standard distribution -- I believe it's every two weeks -- where

1 FinCEN -- so FinCEN has a process to receive requests from law enforcement for the use
2 of this mechanism, and then every two weeks FinCEN will cobble together those multiple
3 requests into one distribution, and it goes out.

4 The standard distribution goes out to regulated financial institutions, mostly
5 banks. FinCEN has the authority to roll it out to other types of financial institutions, but
6 at least as of when I was there, it was primarily banks and a couple of MSBs, I think.

7 And the 314(a) request, exactly as you said, would ask those institutions to
8 respond, not with the underlying information, because 314(a) doesn't actually authorize
9 that, but to respond as to whether or not their institution has information related to
10 those individuals and entities. And, if so, it's a way for law enforcement to know the
11 location of the financial data.

12 Q And then law enforcement then determines whether or not to serve a
13 subpoena or whatever --

14 A Exactly.

15 Q -- it deems necessary --

16 A Correct.

17 Q -- with respect to that particular suspect.

18 A And they would need to use appropriate legal process to do so, correct.

19 Q Now, going back to the -- to SISS and the -- well, to make sure I understand
20 the difference, the portal is just access to the BSA data. So it's kind of like Westlaw for
21 looking at case law, correct?

22 A Yes, sure.

23 Q That's my only frame of reference.

24 And then SISS is more of a messaging platform to be able to share -- I mean, it's
25 not like a --

1 A Yeah, I wouldn't --

2 Q It's not Slack, but it's --

3 A I wouldn't say that, because it's also -- FinCEN would post documents that
4 those with access to SISS could download, the 314(a) distributions, for example.

5 There would be, like, drop-downs where they could input their responses for each
6 query -- yes, no.

7 It also maintains a repository of other documents, like the 314(b), which we'll get
8 to in a minute, participant list.

9 It's also a portal where, on an ad hoc basis, institutions can upload files in a secure
10 manner.

11 So it has a host of utilities, but it is not -- it does not possess BSA filings. Nobody
12 can go into SISS and search it or access any kind of SARs or CTRs or any of that; totally
13 different, separate mechanism and separate data holdings.

14 Q So it's information sharing that is separate from the actual SARs itself --

15 A Yes.

16 Q -- and separate from the BSA data itself.

17 A Correct.

18 Q Okay. And it is set up pursuant to statutory and regulatory authority.

19 A The information that is shared to and from are being shared pursuant to
20 those authorities. But physically setting up the system, I don't know one way or the
21 other. But yeah, it's --

22 Q Fair enough.

23 A Yes, to facilitate information sharing provided for by statute.

24 Q Okay. So the majority has stated in a report that it's published about what
25 it entitled "Financial Surveillance in America" that FinCEN and law enforcement would

1 communicate with the banks through secret back channel methods.

2 What is your response to that?

3 A Well, it certainly has a negative connotation. There's confidential -- there's
4 confidentiality that attaches to the sharing of protected information.

5 So there is information sharing that is occurring that is not known to those who
6 are not entitled to know about it.

7 Is it -- it would be inaccurate to say that that's being done in any manner that's not
8 otherwise clearly provided for by law. So that's what the implication sounds like, and I
9 would not agree with that characterization.

10 Q And the laws that provide for this type of information sharing, those are
11 publicly available. It's certainly a matter of public record that FinCEN is not only
12 authorized but required to set up information-sharing protocols and methodologies
13 between financial institutions, law enforcement, and FinCEN.

14 A Correct.

15 Q Okay. And since you touched on it, let's just briefly look at section 314(b),
16 which I believe is on the third page -- or not. No, it's on the --

17 A Third page. Well, title page --

18 Q Yeah, yeah.

19 A -- first page, second page.

20 Q Thank you.

21 And section 314(b) permits financial institutions to share information with one
22 another --

23 A Correct.

24 Q -- regarding individuals, entities, organizations, and countries suspected of
25 possible terrorist or money-laundering activities.

1 A Correct.

2 Q So there is some 314(b) information sharing that FinCEN is not a party to.

3 A Correct. Yeah. And just for clarification, the way that works, so it's
4 sharing between institutions, FinCEN doesn't need to be involved at all. But in order to
5 share information under 314(b), you have to have registered with FinCEN to do so.

6 So FinCEN maintains a participant list that's available on SISS. 314(b) participants
7 have access to SISS. So they know what institutions with which they can share.

8 Q So if I'm registered with FinCEN under a 314(b) and I want to know who else
9 the information I'm sharing goes to, that's available to me on SISS.

10 A So it's not -- so it's not as if -- no. Maybe I misunderstood. It's not as if
11 the information is, like, broadly shared and you look at the list to see who it goes to.

12 You're ABC Bank, you want to ask a question of XYZ Bank, or you want to send
13 something to XYZ Bank because you think they need to know about it. You would go to
14 the list to see if XYZ Bank is also a participant. And if they are, then you may validly,
15 under these parameters, share that information with XYZ Bank.

16 Q Okay. Thank you. That's very helpful.

17 [REDACTED] And with that, we can go off the record for now.

18 [Discussion off the record.]

19 [REDACTED] We can go back on the record.

1

BY [REDACTED]

2

Q So I'd just like to clarify something that was just discussed, and correct me if

3

I'm wrong, but you mentioned that the SISS does not include BSA filings, and it's separate

4

from the SAR process.

5

A Correct.

6

Q If we could look back at exhibit -- I believe it was exhibit 5, the email that you

7

had sent to financial institutions.

8

The third bullet from the top asks, "In addition to your standard e-file process,

9

please also upload the SAR to the SISS."

10

A Uh-huh.

11

Q So in this case, SARs were filed directly to the SISS and would be on.

12

A So, I guess, it comes down to what "would be on" means. It's a secure

13

information-sharing system. It's not accessible to anybody but FinCEN. So it's not

14

searchable even to us.

15

It would literally be us going into the system and downloading a file that was

16

uploaded, and that's that. And we still required, in this instance, the institutions to

17

follow the standard e-filing process, which would go into the portal, the database.

18

Q Is this the only situation that SARs were uploaded directly to the SISS?

19

A My general recollection is no, that I do recall there being other instances, but

20

I don't recall the circumstances.

21

Q And the participants who were part of the participant list who have access to

22

the information here, would they also be able to download the SARs from the SISS?

23

A No.

24

[REDACTED] Just to clarify, how are typologies that FinCEN creates used?

25

[REDACTED] By whom?

1 [REDACTED] The financial institutions who receive them.

2 [REDACTED] I think you just said that FinCEN creates.

3 BY [REDACTED]

4 Q Doesn't FinCEN create the typologies?

5 A Well, law enforcement -- well, the bad guys create the typologies, to be
6 technical.

7 Anyone analyzing BSA data could derive that by observing the conduct of those
8 actors. So it could be law enforcement, it could be FinCEN, it could be IC, could be
9 regulators, whomever is analyzing BSA data.

10 Q Can the typologies that FinCEN shares with financial institutions be used as
11 the basis for filing SARs?

12 A That's a -- I'm trying to answer that honestly.

13 The typologies can be used by financial institutions to inform their assessment of
14 whether specific conduct is or is not suspicious. If they determine something is
15 suspicious, they'll file a SAR. If they determine something is not suspicious, they won't.

16 Those red flags and typologies can be used to inform that assessment.

17 Q Have you ever seen SARs filed along the lines of typologies that FinCEN
18 shares?

19 A You know, I didn't really read or analyze many SARs in my time at FinCEN.
20 It wasn't really part of my job. So that's not really a question I can answer.

21 Q Would that have been the Intelligence Division?

22 A Primarily, from a substantive assessment. Again, different divisions might
23 have had different needs to look at SARs. But, yes.

24 Q And you may have already touched on this as well, but the Intelligence
25 Division is the one who creates SARs within FinCEN -- or creates typologies within FinCEN?

1 A I think it would be fair to say that the Intelligence Division is the primary
2 component of FinCEN that would analyze BSA data and derive typologies.

3 Q Okay.

4 [REDACTED] I want to enter an email from Anthony Harris dated January 15th,
5 2021, and the attachments -- "Jan 15 2021 compiled typologies" and "KeyBank Query
6 Logic for Active Shooters" -- with the subject line "Compiled typologies in advance of 4:30
7 call" into the record as exhibit --

8 [REDACTED] 7.

9 [REDACTED] -- 7.

10 [REDACTED] Exhibit No. 7.

11 [REDACTED] was marked for identification.]

12 [REDACTED] I'm just flagging -- I don't care at all -- but there's a redaction here.
13 If you want to add that to the official exhibit, Mark's name.

14 Okay.

15 BY [REDACTED]

16 Q Do you remember this email?

17 A Vaguely. Somewhat, yes.

18 Q And what do you remember about it?

19 A Not to be obnoxious, but that I sent it -- or that Tony sent it. That it was
20 sent.

21 Q Okay.

22 A I mean, I just recall seeing it and, you know.

23 Q And Anthony, I think you stated earlier, was the section chief within your
24 division. Is that right?

25 A Yeah. So my -- division office section. So Tony reported directly to me.

1 He was the chief in charge of one of my two sections in my office.

2 Q And it looks like there are 11 different financial institutions on this email.

3 A Okay.

4 Q Do you know how it was decided that these materials went to these financial
5 institutions and not others?

6 A I do not.

7 Q Do you know who would?

8 A I do not.

9 Q Do you remember if you had to get approval before sharing these materials
10 or if Anthony had to seek approval from you first?

11 A Yes. And to be clear, I don't specifically -- I said this earlier -- I don't
12 specifically recall whether approval was sought for this specific or if there was an
13 understanding that this was coming and that we were authorized and approved to send
14 it.

15 But, yes, this is not something that Tony or I sent on our own.

16 [REDACTED] If it was the latter where there was, like, an understanding that you
17 might be receiving this material and it could be sent, how would you have gained that
18 understanding?

19 [REDACTED] Well, it would have -- so my recollection is that there were times
20 when, for example, if one of the conversations, if one of the banks said, "Oh, we can
21 share X, we'll send it to you," someone on the -- an example of this, for example, if
22 someone on the call with authority to authorize me to send it said, "Great, we'll send it
23 out when we receive it," I may have interpreted that to mean I was approved. Or I may
24 have gone to that person to confirm, "Hey, I'm going to send this out. Are we good?"
25 Something like that I recall happening during that period of time.

1 And then others would have been more specific, like, "Hey, I got this. Are we
2 okay sending it out?"

3 ██████████ During that period of time, is your memory specific enough to refer to
4 January 2021, that some of the materials sent then came from --

5 ██████████ I was probably speaking about January to February, January to
6 March generally, my recollection. I'm not sure about this specific week, if you will.

7

BY ██████████

8 Q The subject line -- or, excuse me -- the body of the email also states, "in
9 advance of the 4:30 call."

10 Do you remember that call?

11 A No.

12 Q Do you remember if there were any pre-meetings within FinCEN to talk
13 about what would be discussed on that call?

14 A No.

15

BY ██████████

16 Q Do you remember any pre-meetings generally around this time, whether it
17 was discussion of typologies, key words, things like that?

18 A I think I answered that earlier. I have a general recollection that there were
19 some pre-meets and that there were not pre-meets before every conversation, but I'm
20 not sure I remember any details beyond that.

21 Q Any pre-meets -- again, with the understanding of not having a specific
22 recollection at this pre-meet this was discussed -- do you recall generally any of the
23 pre-meets where there was discussion of some of the terms on page Bates number 6
24 here?

25 A No. Although I will note on its face that this came from one of the financial

1 institutions, not FinCEN. So you're talking about an internal FinCEN pre-meet?

2 Q Yes.

3 A Got it. I don't recall.

4 BY [REDACTED]

5 Q Do you remember what the purpose of this call was?

6 A No.

7 Q Do you remember if there were any other Federal representatives other
8 than FinCEN on the call?

9 A No.

10 [REDACTED] Was this part of the, as we discussed earlier, kind of the daily
11 Zoom calls that you were having with financial institutions?

12 [REDACTED] I don't recall. I mean, I'm noting that I have two emails in front of
13 me that appear to refer to separate calls on the same day. So I have no idea of whether
14 they were part of a particular cadence or not. I don't recall.

15 [REDACTED] As part of those daily Zoom calls, were representatives from the
16 FBI and DOJ on those calls?

17 [REDACTED] I recall -- the answer is yes to some. I don't recall whether they
18 were on all.

19 BY [REDACTED]

20 Q Are you aware of how soon following January 6th FinCEN began coordinating
21 with the FBI?

22 A No.

23 Q How about with financial institutions?

24 A I don't recall. All I can say was I don't remember the date of the
25 inauguration, but I do know it was at some point before that.

1 Q Can you describe how FinCEN viewed its role in the investigation into
2 January 6th?

3 A Probably only with reference to the mission statements. I mean, I think we
4 were using FinCEN Exchange in a manner consistent with how we always used FinCEN
5 Exchange. That's how we viewed it.

6 Q And so would you view FinCEN as the lead or FBI as the lead?

7 A I'm not sure I would make that distinction.

8 Q Okay. Do you recall if certain thresholds or fact-based patterns for
9 reviewing data was discussed on the call or any of these calls?

10 A Repeat that for me. Sorry.

11 Q Sure. Were certain thresholds or fact-based patterns discussed on the calls
12 that you had with financial institutions?

13 A I'm not sure what you mean by thresholds. Like, financial thresholds or
14 thresholds to file a SAR or -- I'm not sure what you mean by threshold.

15 Q Were either of those discussed?

16 A Not to my recollection. I don't recall.

17 Q Did fact-based -- were fact-based patterns surrounding the events of January
18 6th discussed, to your recollection?

19 A And, again, not knowing what is meant specifically by fact-based patterns,
20 we had a -- I do recall at a general level discussions on red flags, typologies, indicators.

21 Q During a transcribed interview with the committee, Mr. Peter Sullivan with
22 the FBI stated that certain fact-based patterns were discussed with FinCEN and financial
23 institutions on at least one of these calls. Does that --

24 A Did he define fact-based pattern in that conversation?

25 Q In terms of certain transactions that were made related to travel,

1 weapons-related transactions.

2 [REDACTED] Do you guys have the transcript or some context you can give
3 him for that?

4 [REDACTED] I'm just -- not at the moment, no.

5 [REDACTED] Yeah. I don't recall any of that.

6

BY [REDACTED]

7 Q Okay. Have you heard of FinCEN creating fact-based patterns before or --

8 A I'm still not really --

9 Q -- you're not sure?

10 A I'm still not sure what you mean by fact-based patterns.

11 Q The answer may be no. I'm just --

12 A No. Yeah, I mean, I'm sure the answer is going to be I don't recall, because
13 I don't really remember this level of specificity. But, like, I don't -- I'm struggling with
14 what that means, if it's different than, for example, what I'm referring to as a red flag or a
15 typology.

16 Q Are you aware of the Bank of America SAR that has been the subject
17 of -- part of -- one of the subjects of the committee's investigation that was filed following
18 January 6th?

19 A I don't have a specific recollection of it.

20 Q Have you seen these typologies before?

21 A Which ones are we talking about?

22 Q Any of them.

23 [REDACTED] Any of what?

24 [REDACTED] Bates stamp 6, Bates stamp 7.

25

BY [REDACTED]

1 Q Does this look familiar?

2 A So on Bates stamp 6, what's characterized as number 1, my recollection is
3 that came from one of the bank participants. So this is the first time -- when I
4 received -- or whomever at FinCEN received this would have been the first time I saw it.

5 Number 2, I believe, is a reference to a previously published FinCEN advisory. I
6 might be wrong about that. I feel like we may have published one subsequent to this,
7 too. I don't recall. But I was generally aware of this type of analysis that's reflected in
8 number 2 that's attributed to FinCEN.

9 And then same thing on the whole KeyBank deck would have all been new to me
10 upon receiving it from KeyBank.

11 Q And did you receive the bank submission?

12 A I don't recall if I was the specific person or not. I mean, I may have been on
13 the email or I may have been the recipient directly. I don't recall.

14 Q And do you remember which bank submitted this?

15 A The deck?

16 Q The first number says, "1) Bank submission."

17 A Oh, I do not remember -- I do not recall which bank that is.

18 Q With respect to the lone actor, homegrown violent extremism indicators
19 developed from a prior FinCEN analysis, would that have been the Intelligence Division
20 that produced these?

21 A I would say primarily. They worked closely with an office in our Policy
22 Division, which at least when I was at FinCEN was technically the office that was
23 responsible for our advisories.

24 So I imagine most of the analysis was Intelligence Division, potentially in
25 conjunction with some of the folks in the Strategic Policy Office.

1 Q Do you recall whether these materials were shared with any other Federal
2 agencies?

3 A I don't recall.

4 Q What's the purpose of sharing these kinds of materials with financial
5 institutions?

6 A I don't want to mischaracterize it. I mean, I view the purpose of that as
7 that consistent with FinCEN's mission and the statutory authorities that we were using, all
8 of which have, like, mission and purpose statements.

9 Q Was there an expectation with how banks might use this information?

10 A Not to my recollection, no.

11 Q Are you aware of other typologies concerning domestic activity that were
12 shared with financial institutions following January 6th?

13 A I mean, I am generally aware that this was not the only communication that
14 was sent or received in relation to this period of time. Any level of specificity beyond
15 that, I don't recall.

16 Q Moving to that first number, the bank submission, it states, "Terms used for
17 searching Zelle payment messages for indicators of involvement in the riots or potential
18 violence." It then included search terms like MAGA and Trump and America First.

19 Have you seen search terms like this before?

20 A No. And I wouldn't have been the one analyzing that data anyway.

21 BY [REDACTED]

22 Q Who would have been analyzing that data?

23 A Some combination of law enforcement, FinCEN Intelligence Division, the
24 folks whose job it was to do that, I guess.

25 Q To your understanding, were there any internal discussions at FinCEN about

1 whether sharing these typologies implicated any First Amendment concerns?

2 A I don't recall.

3 Q Independent of this specific exhibit and independent of January 2021, at a
4 high level during your time at FinCEN were you ever aware of any conversations regarding
5 whether certain typologies would potentially implicate the First Amendment?

6 A Not that I recall.

7 Q During any of your time at FinCEN, were there ever instances where certain
8 terms, typologies would refer specifically to political leaders?

9 A I'm sorry. Can you restate the question?

10 Q Sure. So just in the list, there's Trump, Kamala, Biden. Are there other
11 instances during your time at FinCEN where some of the terms would be referring to
12 American political leaders?

13 A Oh. Not that I recall. I don't recall.

14 Q Do you recall one way or the other whether it stood out? Was there
15 anything unique about the typologies that you received from the banks during this time
16 period?

17 A Well, they felt unique to the topic as distinct from human trafficking or drugs
18 or something like that. So, I mean, unique from that perspective.

19 But in terms of the general category of indicators and red flags that might be used,
20 no, I don't recall thinking that anything was unique.

21 Q In an earlier answer you referenced, when asked why you send this
22 information to the other banks, you invoked the mission statement and the purpose of
23 the agency.

24 But just at a more -- again, just based on your understanding, not quoting the
25 mission statement or whatever it might be -- what's the benefit of sending these terms to

1 the banks?

2 A So take a big step back. I mean, if you talk -- especially some of the
3 institutions that were receiving this, B of A and Citi, millions and millions of customers,
4 billions of transactions -- their transaction monitoring program that they analyze to
5 determine whether SARs are filed probably has pretty generic typologies. So they're
6 looking for a needle in a whole big pile of haystacks.

7 So one of the purposes of disseminating typologies is to narrow the scope of a
8 search. So, for example, if you're looking for somebody located in California, it doesn't
9 make sense to look for people in New Mexico. You know you're looking for a
10 Californian.

11 So if you have that info and you can restrict your search and eliminate the other
12 49 and every other country, you have now greatly increased the chances that you're
13 going to find something relevant.

14 I say that at a high level because it's possible that a Zelle message that
15 says -- that's sent in March for NCAA tournament dues is not where you're looking -- I
16 mean, could be a clever way to cover something up.

17 I'm not suggesting you don't want to look at it, but that's less likely to be relevant
18 to the conduct you're looking for than perhaps terms that you might otherwise expect to
19 be more relevant to certain types of communications you're looking.

20 So a lot of it was to help them -- to provide them with more information that
21 might be helpful for them to generate higher quality results for analysis, I suppose.

22 Q Was there any internal discussion about whether the typologies included in
23 this list, yes, might narrow the scope, but also might disproportionately target
24 transactions that are completely fine and aren't the concern?

25 A I don't recall one way or the other specific discussions about that.

1 Q If there were to be discussions about that within FinCEN, whose team would
2 take the lead on assessing those types of concerns?

3 A I'm not sure I can answer that question. I mean, I don't know if it -- if it
4 involved legal issues maybe -- I'm not sure I can offer much there.

5

BY [REDACTED]

6 Q How would a financial institution search Zelle payment messages?

7 A I don't know. I suppose it would depend on their internal system. I mean,
8 the financial institution would have a record of the transactions that moved through its
9 institution and would have some sort of system that it could use to query that info, I
10 suppose.

11 Q And query that info using some of the terms here as we've discussed to
12 narrow the universe of potentially suspicious activity?

13 A I mean, I don't have firsthand knowledge. I can't even sit here and
14 guarantee you that every institution has that technological capability. I don't know.

15 Q Do you know if anyone communicated with Zelle that you would be
16 searching their payment messages?

17 A I don't know. Is Zelle even a company, or is it just a service that the
18 banks -- I don't know. Not to my knowledge.

19 Q Are you aware of whether FinCEN is searching Zelle payment messages?

20 A So FinCEN doesn't have access to transactional data unless it is filed as part
21 of a valid report, CTR or SAR or whatever. If it is in the BSA data in a manner that is
22 queryable, then the answer would be yes.

23 Did that answer the question?

24 Q So within that system, are you aware of searches for Zelle payment
25 messages?

1 A I'm not aware one way or the other of what people at FinCEN were doing to
2 analyze the BSA data. That's not what I did at FinCEN.

3 [REDACTED] And just to clarify, are you clear one way or another about
4 whether Zelle payment messages would have been reported as part of BSA filings?

5 [REDACTED] It is quite possible. Any type of financial transaction that goes
6 through a regulated institution is expected to be monitored for purposes of suspicious
7 activity reporting. So that would include Zelle, wires, whatever.

8 [REDACTED] At this time, did any of the financial institutions have questions
9 on what was expected of them when this was sent?

10 So did the financial institutions think that they needed to run a search using all of
11 these terms, and any time one of those search terms yielded a hit, they would have to file
12 something with FinCEN?

13 [REDACTED] I'm very confident that, especially this group, which is a pretty
14 sophisticated group of large institutions that had engaged with FinCEN with some
15 regularity, I'm confident that none of them believed that there was an expectation that
16 the mere existence of these terms made something suspicious.

17 [REDACTED] Did anyone ask questions about it?

18 [REDACTED] Not that I recall.

19 BY [REDACTED]

20 Q Just as a general practice, not specific to this email, if FinCEN is on the
21 receiving end of the listed typologies and then is considering sharing that with a broader
22 group of banks, is that -- does that process ever loop in legal counsel?

23 A I generally would not have been involved in that process, so I'm not sure.

24 Q Who generally is involved in that process?

25 A I'm not certain. I don't know.

1 Again, I know that Intelligence Division would do some of the actual analysis.
2 But in terms of how it goes from that early stage to here's something we're ready to
3 publish, I wasn't really involved. I'm not sure.

4 Q To your understanding, was this list modified in any way based on filings
5 received by FinCEN?

6 A I don't recall.

7

BY [REDACTED]

8 Q And so it was your office that ultimately made the decision to share these
9 typologies.

10 A No. It would not have been my office's decision. My office would have
11 been the one that physically shared it. But I likely and my staff wouldn't have had the
12 direct -- I shouldn't say authority. There's no specific thing written down that says who
13 can do what necessarily.

14 But, no, neither me nor my staff would have made an independent decision on
15 whether or not to share this.

16 Q So who would make that decision?

17 A I don't know.

18 Q You don't know who made that decision in this instance?

19 A Correct, I don't. I don't recall.

20

BY [REDACTED]

21 Q On these daily Zoom calls, whether they occurred daily or near daily around
22 this time, who is the most senior person at FinCEN to attend those meetings?

23 A I know for a fact that AnnaLou was on most of them. She was one of seven
24 division heads, plus chief counsel, eight, that reported up to the director and deputy
25 director.

1 I do have a recollection that the director popped in at least once or twice, sort of
2 with a preamble or whatnot, but I don't recall him being a regular participant.

3 AnnaLou and one or two other associate director or deputy associate director
4 level personnel, such as Jimmy and Kim, would have been involved.

5 And those are -- the ADs were SES's. FinCEN only had about 10, 11, 12 SES's.
6 Most of them were division heads, chief counsel, director, deputy director, Ken, if he's
7 still there, CTO.

8 Sorry. I started whispering on you guys. Sorry.

9 Q How frequently would the director attend calls with representatives from
10 the banks, on calls like [inaudible] from January 2021?

11 A Sorry. You're asking in connection with this --

12 Q No. Independent of this. Just to get a sense of --

13 A Just as a general matter? I mean, gosh, it --

14 [REDACTED] To the extent you know what Director Blanco would have been
15 involved in.

16 [REDACTED] Yeah. I wouldn't even know -- I would only know a fraction of
17 what he did. You know, he would usually be at BSAAG twice a year, not the working
18 groups. But I really couldn't speak much to that.

19 BY [REDACTED]

20 Q Have you seen indicators like the ones listed here before?

21 A I'm not sure what you mean by "like the ones." I mean, these specific
22 indicators do appear relatively specific to this topic.

23 Q And what office at FinCEN has the responsibility for creating extremism
24 indicators?

25 A So those could come from anywhere, again. I mean, a lot of times they

1 came from law enforcement, financial institutions sharing things. From an analysis of
2 BSA data at FinCEN, it would, to my knowledge, primarily be the Intelligence Division.

3 Q And are you aware of whether they created these indicators?

4 A In number 1?

5 Q Number 2.

6 A Oh, number 2. I don't have any specific knowledge of where these came
7 from. But as a general matter, based on my knowledge of FinCEN, most of this analysis
8 would likely have come out of the Intelligence Division.

9 Q When a financial institution receives indicators like this, how can they use
10 them in their system? In other words, how do you translate these indicators into
11 queryable, actionable items?

12 A I'm not sure I can really speak to what individual banks would be able to do,
13 to the extent they did anything at all. I really don't know.

14 Q Are you able to speak in general how they might?

15 A As a general matter, I suppose they could do manual searches. They could
16 develop an algorithm that includes some of this info. I mean, there's any number of
17 things. It depends on what their program looks like, what their tech stack looks like.

18 Q You mentioned earlier that this was a sophisticated group of banks. So do
19 you have any idea how their systems might be able to use this?

20 A I don't. And, anecdotally, even though they were sophisticated banks, I
21 wouldn't assume that their tech followed suit.

22 A lot of -- having been inside a big bank, a lot of times these banks get big by
23 acquiring other companies. And so you end up with about 20 systems with duct tape
24 and trying to -- it can be pretty messy.

25 So I couldn't tell you one way or the other.

1 Q One of the extremism indicators includes, "Transportation charges, such as
2 bus tickets, rental cars, or plane tickets, for travel to areas with no apparent purpose or
3 not commensurate with the previous travel history of the customer, for example, travel
4 to high-risk areas or indirect flightpaths for no apparent legitimate reason."

5 A Uh-huh.

6 Q Do financial institutions monitor and report these transactions?

7 A I don't know one way or the other.

8 Q Does FinCEN monitor Americans' transportation-related transactions?

9 A I don't know one way or the other.

10 Q Would they not have to in order to produce an analysis concluding this as an
11 indicator?

12 A I just wasn't involved in that work. Couldn't tell you.

13 Q How would FinCEN or a financial institution be able to determine whether
14 travel was for a legitimate reason or had no apparent purpose?

15 A I don't know.

16 [REDACTED] What type -- which personnel within FinCEN would be better able to
17 speak to conducting that type of assessment?

18 [REDACTED] I mean, I would defer to FinCEN. But my best guess would be
19 Intelligence Division personnel.

20 [REDACTED] Did you have a primary point of contact with the Intelligence Division?
21 Who did you --

22 [REDACTED] I'm not sure I would say I had a primary -- they're colleagues. It
23 depends on the -- you know, I would -- at my level, it most frequently would have been
24 Jimmy or Kim or their office directors. But I don't have any specific recollection beyond
25 Jimmy or Kim.

1 BY [REDACTED]

2 Q Another one of the extremist indicators includes, "The purchase of books
3 (including religious texts) and subscriptions to other media containing extremist views."

4 A Uh-huh.

5 Q Do you know how FinCEN may have concluded this as an indicator?

6 A I do not.

7 Q Did you review these indicators before they were sent out?

8 A I'm sure I read them. I didn't review them for any purpose. My job was
9 to send them. So I didn't review, evaluate, modify, revise any of that.

10 Q Do you know who sent these indicators to you?

11 A I don't recall. Again, likely would have been someone in ID.

12 Q Are there certain religious texts that FinCEN considers an indicator of
13 extremism?

14 A Not to my knowledge.

15 Q Are you aware of whether FinCEN monitors Americans' media subscriptions?

16 A Not to my knowledge.

17 Q Do you know whether FinCEN has a list of books or media that it believes
18 contains extremist views?

19 A Not to my knowledge.

20 Q To your knowledge, are financial institutions monitoring Americans'
21 purchases of books or media subscriptions?

22 A I don't have knowledge.

23 What I would say is that financial institutions may have monitoring programs in
24 place that would include in its scope all customer transactions, for example, which,
25 presumably, may include credit card purchases wherever or things of that nature.

1 [2:43 p.m.]

2

BY [REDACTED]

3

Q How would a financial institution be able to tell what kind of media or book

4

is being purchased, according to these indicators?

5

A I don't know.

6

Q Does it concern you that FinCEN is listing the purchases of religious texts as

7

potential indicators of extremism?

8

A I'm not sure I'm really credible to speak on that, my personal views.

9

Q I'd be interested in that.

10

A I'm going to decline to answer that.

11

[REDACTED] In the calls that were happening in January 2021, do you recall any of

12

the parties, whether it's FinCEN, the FBI, other government agencies, any of the private

13

sector representatives, raising concerns of whether some of the assessments being

14

conducted, the typologies, implicated First Amendment concerns?

15

[REDACTED] I don't recall.

16

[REDACTED] Were these discussions fulsome conversations or was it more

17

thanks for the information; we'll talk to you tomorrow?

18

[REDACTED] More the former, more fulsome than thanks for sending, see ya.

19

[REDACTED] And on none of those calls, to your recollection, were people

20

saying this might be going a step too far?

21

[REDACTED] I don't recall that. I mean, it's three and a half years ago, and I'm

22

an old man. I don't remember what I had for breakfast yesterday, so --

23

BY [REDACTED]

24

Q Do you recall, during any of the calls, whether there was points of tension,

25

differing views, things that needed to be sorted out?

1 A I don't recall. The best of my recollection is that it was collaborative. You
2 know, whether institutions chose to do something or not, I couldn't tell you, but I don't
3 recall there being any tension or points of issue in the discussions.

4 Q For category two here where there's talk about violent extremism indicators,
5 and it looks like it's coming from previous work product, let's say it is from the
6 Intelligence Division, if there are issues that start to touch upon First Amendment
7 concerns, is your office looped into that process at all?

8 A We likely would not be, no.

9 Q Which -- besides counsel office itself, which offices or divisions would have
10 been involved in the preparation of that type of work product?

11 A Counsel would be the only logical assessment, in my view, but I don't really
12 know one way or the other.

13 Q At a very high level, not to implicate, what types of issues from your office
14 would require the counsel's office to make assessments?

15 A We're not a big office. That's a very broad question. I'm not really sure
16 how to answer that, right. I'm -- I mean, if my team was in a BSAAG conversation and
17 heard something that we thought was useful to someone else at FinCEN, or that we
18 thought someone at FinCEN should consider, or that -- you know, it's very subjective.
19 That's a very hard question to answer. I'm sorry.

20 It's no different than what I experience in any other job, right. I mean, when do
21 you tell your -- when do you raise something for your boss or handle it yourself? Or
22 when do you -- right? I'm not sure I can give at that high level a better answer than that.

23 Q Obviously, we're trying to work with you.

24 A Yeah, I know. Fair.

25 Q On a granular level, you know, sometimes, right, you're not able to recall

1 what discussions did or did not take place, so just trying to get a sense at a higher level.

2 A Fair. Yeah, I mean -- as an example, I mean, it's not as relevant to this, but
3 on the data access side, if my team was conducting a review of the FBI's usage of BSA
4 data or LAPD and saw something of note, that maybe Officer Jenkins was doing
5 something, that might be something that would hit my desk, and I may tell leadership,
6 you know, that sounds like something that somebody should know about, right, just as an
7 example, right.

8 But, again, it falls subjectivity and judgment as to whether something needs to be
9 escalated or not to a higher level or the, you know, counsel needs to be consulted.

10 Q Generally, if an issue that was within your purview and you felt may warrant
11 being considered by counsel, is that a decision you can make or would you tell one of the
12 folks above you and ultimately they would make a decision whether to loop it to counsel?

13 A It's hard to answer that hypothetically. I mean, if I saw something in the
14 normal course that I think I needed a lawyer's input on, I would likely just go to counsel.
15 If I thought it was something that needed to be escalated, whether it had legal questions
16 or not, I would probably go to my leadership, as a general matter.

17 [REDACTED] As part of the approval process when you were sending out this
18 information, do you know if the counsel's office was looped in as well?

19 [REDACTED] I think we're coming pretty close on the privilege line there.

20 [REDACTED] I don't know if you want to try to rephrase it. I think at a high level,
21 we can -- without implicating the privilege.

22 [REDACTED] I think if you guys want to ask about discussions that FinCEN
23 counsel had with others at FinCEN, you can direct those to us and not to him in an
24 interview. Like, those are pretty squarely within the privilege.

25 [REDACTED] Okay. We can talk more, obviously, off the record, but I think there

1 will be interest from the committee to have an understanding of what guardrails were put
2 in place and what those look like. And the witness is representing he was not privy to
3 those, so, you know, we'll take that in good faith. But that is information that the
4 committee will be interested in.

5 [REDACTED] I'm happy to follow up with you guys.

6

BY [REDACTED]

7 Q Does FinCEN rely on MCC codes in its investigations?

8 A What's MCC?

9 Q Merchant category codes.

10 A Not to my recollection.

11 Q Do you know whether your office or other offices ever provided financial
12 institutions with how to use merchant category codes?

13 A No, I don't know. I would actually go so far as to say I have an affirmative
14 recollection that I'm not aware of that happening. I don't remember hearing MCC at all
15 when I was at FinCEN.

16 Q I'll just move to the KeyBank slideshow. Do you recall receiving this email
17 from -- this in an email from KeyBank?

18 A Not specifically.

19 Q Okay. I'll introduce -- I'd like to now introduce an email from KeyBank to
20 [REDACTED] dated January 15, 2021, with the subject line "Inauguration Task Force" into
21 the record as exhibit 8.

22 [REDACTED] Exhibit No. 8.

23 was marked for identification.]

24 [REDACTED] You guys went inkjet on this one, huh.

25 Okay.

1

BY [REDACTED]

2

Q Had you received slideshows like this before or after from financial

3

institutions?

4

A I'm sorry, before or after this particular email, you mean?

5

Q Yeah. Did you receive slideshows like this from financial institutions?

6

A I don't recall.

7

Q Do you recall receiving this email?

8

A I mean, I do now. I don't have a specific recollection beyond what's on the

9

page.

10

Q Do you recall, once you received this from KeyBank, what you did with it?

11

A No.

12

Q Did you review the material?

13

A Same answer as before, I'm sure I read it, but it wasn't my job to evaluate or

14

do anything with it, other than, if necessary, disseminate it.

15

Q And so looking at the --

16

[REDACTED] Do you guys have the attachment to this email?

17

[REDACTED] Yeah, it's the KeyBank slideshow that's --

18

[REDACTED] Okay. Do you have it attached to this email so he knows that

19

it's the same document, for purposes of the record?

20

[REDACTED] Not right now.

21

I'll represent for the record that the attachment states, "KeyBank Query Logic for

22

Active Shooters 01-15-2021," and that the slideshow entered as exhibit 7 is KeyBank

23

Query Logic for Active Shooters and is named as the same attachment in Bates stamp 5

24

that's named in Bates stamp 235.

25

[REDACTED] Thanks.

1 [REDACTED] Can I just point out, for what it's worth, though, that I don't know if
2 there is a time change that's causing this to be screwed up here, but --

3 [REDACTED] There is. They're not converted. That's minus five and this
4 is just regular.

5 [REDACTED] Oh, so this happened before this?

6 [REDACTED] Yep.

7 [REDACTED] Got it. Okay.

8 [REDACTED] So could you just briefly explain what the slideshow is?

9 [REDACTED] Not beyond what's on the page itself. I didn't create it. I didn't
10 do anything with it, other than be copied on an email in which it was disseminated.

11 [REDACTED] But you received it as well?

12 [REDACTED] Based on this email, that's what it appears. I don't specifically
13 recall beyond what's on the email.

14 [REDACTED] I will also note that Anthony Harris received this one.

15 [REDACTED] Right.

16 I mean, I'm not trying to be cagey. My staff and I were the ones that were
17 organizing these events. So not all the time but much, maybe most, I couldn't really
18 necessarily say, but certainly much of the information that was being sent and received
19 was coming through us. That was what our responsibility was, but that was really the
20 limit of what my staff and I were doing.

21 In terms of, like, oh, now we have this information, let's do something with it, I
22 was neither involved in that, nor am I necessarily aware of what was being done
23 internally.

24 BY [REDACTED]

25 Q Which team or division would your team share this slide deck with?

1 A So there was a -- I don't remember specifically who, but there was certainly a
2 group of people at FinCEN involved in these conversations broadly that would have -- we
3 would have disseminated that internally to that group; you know, the most relevant of
4 which, to the best of my recollection again, would be Jimmy and Kim and their staff in ID.

5 Q Besides Jimmy and Kim, any other offices that --

6 A I don't specifically remember which of their staff members was involved in
7 this topic.

8 Q Both the offices themselves and individuals or --

9 A Correct. I'm not even sure I can name the offices of ID. I don't think I
10 could even when I was at FinCEN, but, no, because Jimmy and Kim ran the division, and
11 they definitely did have offices and sections. But I don't recall which personnel or which
12 offices or sections were involved in this.

13 Q Do you recall, outside of the Intelligence Division, which other divisions
14 would have had a practice during this time period you likely would've looped in?

15 A Yeah, so certainly Strategic Operations, which -- right. I have a vague
16 recollection that there would've been one or two people from our Policy Division because
17 that's the division that does oversee our advisory program. But beyond that, I don't
18 recall.

19 Q What about the Enforcement Division?

20 A I don't recall whether they were included or not.

21 BY ██████████

22 Q So once you receive something like this, do you -- I know you stated that you
23 kind of just distribute it. Did you feel any responsibility to evaluate the material? Was
24 that a part of your --

25 A It would not have been a part of what I was asked to do at FinCEN, and I

1 don't believe I would have.

2 Q Was there any material that you received from outside entities that you
3 didn't distribute?

4 A My answer is going to be I don't recall either way. I'm not sure if you mean
5 on this particular topic or ever at FinCEN, but I don't recall either way.

6 Q I mean, while in your role as the director of the stakeholder engagement
7 division.

8 A I mean, the question is generally whether I ever received things that I didn't
9 disseminate?

10 Q Well, I'm trying to understand, if there are things that you didn't
11 disseminate, that suggests you may have evaluated it and thought it's not worth
12 disseminating.

13 A It may be possible that at some point I was sent something or not that I may
14 or may not have disseminated. It was never a result of my evaluation or my staff's
15 evaluation of the content. We didn't do that.

16 Q Did anyone at FinCEN evaluate this content?

17 A I can confidently say that we would have. I don't know who, and I wasn't
18 involved in the evaluation of it.

19 Q Were you at all concerned about sharing information without evaluating it?

20 A I did not have a concern because I was under the impression that those
21 charged with evaluating the information were doing so.

22 Q Which would have been whom?

23 A It depends on the information, but, you know, substantively, most likely the
24 Intelligence Division.

25 Q Okay. So it could have been that you received this email with the KeyBank

1 slideshow, and you shared that with the Intelligence Division, and they say -- they sign off
2 on whether or not they think it's good to distribute?

3 A I don't recall specifically whether that's what happened.

4 Q Is that something that could have happened or has happened while you
5 were at FinCEN?

6 A I'm trying to remember whether I ever accepted what ID said or whether I
7 went to my own leadership for confirmation that they were comfortable with sending it
8 out.

9 [REDACTED] Is your leadership on this email incoming from KeyBank?

10 [REDACTED] Yeah. So at this point in time, AnnaLou was my division head, and
11 she was on this comm. I don't specifically recall from whom I obtained approval to
12 disseminate this.

13 [REDACTED] Would it have been typical for you to just chat with AnnaLou and
14 say, do you think this is good to go?

15 [REDACTED] I mean, I spoke to my boss pretty frequently, so that was typical.
16 And this is something I expect I would have sought approval on. That's a half answer.

17 BY [REDACTED]

18 Q Why?

19 A Why?

20 Q Yeah, just what about this one?

21 A Just as a general matter, you know, in the context of disseminating
22 information to the private sector, I would've -- especially, you know, in connection to a
23 topical event, I would have sought confirmation from my superiors that that
24 dissemination was appropriate.

25 Q For any topical event, not necessarily January 6th, do you recall any

1 instances where one of your superiors told you that information would not be
2 appropriate for dissemination to private sector partners?

3 A I don't recall one way or the other.

4 Q Were you ever asked to weigh in on whether dissemination would be
5 appropriate, or was it more you're just receiving instruction or approval?

6 A I don't have any specific recollection. I do have a general recollection that
7 that kind of conversation may have taken place with me on the phone. Like, I have a
8 general recollection that I was on a call or in a discussion where that topic was being
9 discussed, but it wouldn't have been my place to weigh in one way or the other. It's just
10 not what I did there.

11 [REDACTED] I think we can go off the record.

12 [Recess.]

13 [REDACTED] We are back on.

14 BY [REDACTED]

15 Q Okay. So I would like to start and just take a step back. You said
16 something and I believe counsel said something during the previous hour. Counsel said
17 something about, you know, were you concerned about the banks might flag transactions
18 that, you know, look like they're perfectly legal. And you had given an example of, you
19 know, somebody writes, this is for an FCAA tournament in March. And then you
20 qualified that by saying, well, that actually could still be a code for something.

21 The vast majority of financial transactions on their face look legal, correct?

22 A Correct.

23 Q I mean, it would be very unusual to see a Zelle message that says this is for
24 fentanyl?

25 A Here's the problem and why it's very, very complex but it kind of reinforces

1 the point. It depends on the context, right, and your bank knows a lot of info about you.
2 So if your bank -- if you make 40 grand a year, your bank knows that. If you've got a
3 balance of about a thousand dollars for the last 3 years, your bank knows that.

4 If you send a Zelle -- if you receive a Zelle for 15 grand, that's going to stick out for
5 that person, regardless of what it says; whereas, the guy who's making six figures, who's
6 maintaining a \$20,000 balance in his savings account, that's not going to flag anything.

7 So it's totally contextual, which is generally why no one red flag would ever be
8 something that people would say, oh, that's definitely suspicious. It really is contextual,
9 and it depends on the compilation of factors.

10 Q And depending on the scenario, whatever type of suspicious activity you're
11 looking for, and then depending on the type of customer, that compilation of factors is
12 going to be different, correct?

13 A Yes.

14 Q Okay. And banks have to look at a variety of factors and, really, the totality
15 of all of the circumstances in order to determine if a transaction is suspicious?

16 A Yes.

17 Q And they make those determinations often with the benefit and insight of
18 information that FinCEN has shared, either that FinCEN has developed or that law
19 enforcement has developed, with information about current trends in money laundering,
20 terrorism, financing, and the other crimes that FinCEN focuses on, correct?

21 A Yes.

22 Q And, you know, just as another example of a type of reporting, I
23 mean -- well, let me step back.

24 The Bank Secrecy Act requires the reporting of any transaction and cash
25 transaction of \$10,000 or more, correct?

1 A Yes.

2 Q Even if there's nothing else?

3 A Correct.

4 Q It could be completely out -- you know, completely consistent, the person
5 could do it every day, but --

6 A Absolutely. That's just a rules-based if it's 10k of cash, it's a report, full
7 stop.

8 Q But outside of that kind of line drawing, there's so many different factors
9 that are involved?

10 A Yeah. I mean, so there's -- there are many reports required by the BSA.

11 Most of them are just, like, if you have a foreign financial account, you have to file it.

12 There's no subjectivity there. Ten thousand in cash, you have to file it.

13 SARs are much more subjective.

14 Q Right. And because of the subjectivity, FinCEN is trying to provide
15 information to help banks be effective in identifying those transactions that, standing
16 alone on their face might look perfectly innocent but, in combination with other factors,
17 might be indicative of criminal activity?

18 A Yes.

19 Q Now, I want to turn to the exhibit 7, which was the email from Anthony
20 Harris, with the list of indicators. So I'm looking at -- it's HJC118 Bates stamp 6.

21 So -- now, you said this repeatedly, but just to be clear. It was not FinCEN's
22 intent, and your belief is that it was not the banks' intent, for any one of the terms listed
23 here with percentage marks on either side to trigger a SAR, correct?

24 A Correct.

25 Q There would have to be many other factors before a SAR?

1 A I wouldn't necessarily say many, you know, but it would -- the existence of
2 this -- of one of these terms would not generally by itself make something suspicious.

3 Q So if somebody sent a Zelle payment message, and in the message it said
4 "Trump," even after January 6th, that would not by itself -- it was not FinCEN's intent by
5 forwarding this to say, file a SAR for every message that has Trump in it?

6 A It was absolutely not FinCEN's intent to say that, correct.

7 Q And if somebody were to say otherwise, if somebody were to say, FinCEN
8 was flagging Zelle messages that used the words "Trump" or "MAGA," that would be
9 incorrect? Well, would that be correct? I don't want to do --

10 A Yeah. Can you restate that? I'm sorry.

11 Q If somebody were to look at this email and say, FinCEN was flagging Zelle
12 messages that used the word "Trump" as suspicious transactions, that would be an
13 incorrect statement, correct?

14 A Correct.

15 Q Okay. And the same for any of these terms on this list?

16 A Correct.

17 Q Okay. In and of themselves?

18 A Correct.

19 Q And --

20 A It's very hard for me to say that because of the subjectivity, right. I mean, it
21 is possible that, you know, a third-year analyst at J.P.Morgan sees a Zelle that says
22 "murder" and may choose to file a SAR because it says murder. I mean, I can't say not,
23 you know.

24 Q And that's fair. And that raises a good point, which is that some of these --

25 A I wouldn't call --

- 1 Q -- some of these terms --
- 2 A -- all these terms like -- exactly.
- 3 Q They are not alike, correct?
- 4 A They're not necessarily alike with each other, correct.
- 5 Q Some are names, like Trump, correct, and some are things like murder,
- 6 death?
- 7 A And that's -- I mean, again, I can't speak for anybody, but at a just -- as a
- 8 hypothetical, it might be reasonable for somebody to see a payment that says "murder"
- 9 and consider that suspicious. I would say it would be unreasonable for somebody to see
- 10 a payment that says "Capitol" or "patriot" and think that that's alone suspicious, right. I
- 11 mean, so they're definitely not the same.
- 12 Q And it was not your intent to have any one of these by themselves trigger a
- 13 SAR?
- 14 A Correct.
- 15 Q Okay. And this email in particular has been cited by the majority as
- 16 evidence of FinCEN targeting bank customers with conservative viewpoints, and the focus
- 17 was on words like "Trump" and "MAGA" and "America first." But as counsel pointed
- 18 out, there's other terms on this list, such as "Kamala," correct?
- 19 A Correct, that is on the list.
- 20 Q Biden is on the list?
- 21 A Correct.
- 22 Q Antifa is on the list, I believe?
- 23 A Correct -- yes.
- 24 Q Pelosi, correct? It's the third one down.
- 25 A Yep.

1 Q And the last one is Schumer.

2 A Yep.

3 Q And there were others, like "storm the" is a term --

4 A Right. And also, back up to -- I believe your original question said that this
5 is being used as evidence that FinCEN -- these terms did not come from FinCEN. FinCEN
6 disseminated them, but these terms were provided to FinCEN by a financial institution.

7 Q Now, I want to look at the list right below that, the Lone Actor/Homegrown
8 Violent Extremism Indicators. Again, just as with the list above, none of these
9 indicators, to your understanding, was intended to be taken by itself as a sufficient basis
10 for a SAR?

11 A That is correct. I don't recall FinCEN ever disseminating anything, to my
12 recollection, where we ever said or expected somebody to determine that something was
13 suspicious on the basis of a specific indicator.

14 Q So -- and, again, just to be clear, if someone were to say that by
15 disseminating this FinCEN was asking banks to flag any transportation charge as
16 suspicious, that would be incorrect?

17 A To my knowledge, that is not what we intended. That would be incorrect.

18 Q And when you look at this list of indicators here, is there anything on this list
19 that targets conservative viewpoints?

20 A I don't think I'm in a position to opine on that.

21 Q Fair enough.

22 You were asked in the previous hour if FinCEN monitored American's
23 transportation. Does FinCEN have the ability, re access to the data, to be able to
24 monitor that?

25 A I mean, generally, no. If there were transportation-related transactions

1 that were filed in a SAR or something else, then theoretically that would be available to
2 FinCEN.

3 Q And it would be available because somebody in a bank's AML/CFT
4 department determined, through its consideration of a variety of factors, that that
5 transaction was suspicious?

6 A Correct.

7 Q And --

8 A If it was a SAR.

9 Q If it was a SAR.

10 A Right.

11 Q Okay. Now, I want to look at just some of these indicators. If you look at
12 just the first two: The long periods of account inactivity, or normal usage, but in the
13 months or years preceding an attack, a sudden surge of activity -- a change in activity
14 type. And then if you look at the second one: Sudden purchase of firearms, firearm
15 parts and accessories, ammunition, tactical gear at outdoor supply stores, purchases at
16 shooting ranges not commensurate with previously known customer behavior. And
17 then you look at some of the others, like the next several ones on -- the next several
18 indicators on the next page.

19 If you saw all of those indicators for a particular customer, that might be the kind
20 of customer for which a SAR should be triggered, correct?

21 A I mean, it would be subjective, right. Certainly an investigator might come
22 to that conclusion.

23 Q Right. And sometimes different investigators are going to reach different
24 conclusions?

25 A Correct.

1 Q Because it is so subjective?

2 A Correct.

3 Q And, again, as you said, banks had information about their customers that
4 FinCEN, that law enforcement simply don't have?

5 A Correct.

6 Q Banks know their account history, their account usage, their income or their
7 relative income, how much money is coming into the bank, that sort of thing?

8 A Correct.

9 Q Okay. Now, when FinCEN received these from -- this list of indicators from
10 a bank and then forwarded them to other institutions, was FinCEN endorsing the use of
11 these indicators?

12 A So I don't have firsthand knowledge, but on the face of this, this second
13 batch of indicators appears to be FinCEN-developed, but I don't -- I would -- wasn't
14 involved with and don't have any knowledge with how they were developed.

15 Q Fair enough.

16 What about the first one that says "bank submission" that your understanding is
17 that the bank developed?

18 A That was a bank that sent us those indicators.

19 Q And in forwarding these indicators, whether they were developed by FinCEN
20 or developed by the bank, was FinCEN asking the banks to file SARs?

21 A No.

22 Q Was FinCEN encouraging the banks to file SARs?

23 A No.

24 Q Now, in the majority's March 2024 report, it states that this list
25 demonstrates that the Federal Government broadly enlisted financial institutions to flag

1 certain kinds of purchases that the government deemed to be unnecessary.

2 Is that an accurate statement?

3 A No.

4 Q Now, I want to take a look at the PowerPoint that was also attached to this
5 email. Again, as with the previous attachment, the previous typologies, this was not a
6 request by FinCEN to file SARs that matched any of the indicators in this PowerPoint?

7 A Correct.

8 Q And this was not a request by FinCEN to flag any particular transactions or
9 anything like that?

10 A What do you mean by flag?

11 Q Well, I guess the only -- is there a way to flag a transaction other than by
12 filing a SAR?

13 A Not --

14 Q A suspicious --

15 A There's no way to flag transactions for FinCEN and law enforcement's
16 visibility without filing a BSA report.

17 Q Now -- give me 1 minute.

18 If you take a look at exhibit 8, which is the email to you and your colleague from a
19 redacted employee at KeyBank, the employee describes the PowerPoint as, "a typology to
20 detect potential active shooters that we are using right now to see if we have parties of
21 concern."

22 Law enforcement actually wants to prevent active shooters from committing acts
23 of --

24 A I would certainly hope so.

25 Q -- mass shooting, correct?

1 And your understanding is that part of FinCEN's mission is to help identify those
2 folks and prevent those crimes from happening?

3 A Absolutely.

4 And can I just point out, I mean, I think there's a lot of talk about what FinCEN
5 expected or didn't expect. I mean, I think it's instructive to see the words on the page
6 from one of the bank participants where they're characterizing this whole thing as,
7 typologies to detect potential shooters that we are using right now to see if we have
8 parties of concern.

9 So, again, it's instead of looking for that needle in a haystack in millions of
10 transactions, it's let's take a narrow subset that fits certain characteristics and look at
11 those to evaluate whether they are suspicious.

12 Are we going to miss some that aren't in that batch? Probably. Are we going
13 to be overly inclusive in looking at things that we decide are not suspicious? Absolutely.
14 But it makes it manageable. It makes it much more efficient and effective to generate
15 high-quality reviews. That was the purpose and, I think at least in this instance, that was
16 what was understood by the participants.

17 Q Thank you. That's very helpful.

18 And I want to take your advice and focus on the language of the PowerPoint itself
19 that KeyBank sent to you. So I'm looking at the page that starts -- that says, "Active
20 Shooter Detection - Methodology 1." And this is where you have, under Transaction
21 Population, it says, "Query for credit/debit card purchases involving any of the following
22 MCC codes."

23 Do you see that?

24 A Yeah. Do you mind if I -- when I first got this, I didn't really look at the deck
25 at all just because I didn't think -- give me a minute or two to --

- 1 Q Absolutely. Take all the time you need.
- 2 A -- just acclimate myself with the deck, please, yeah.
- 3 Q And please don't feel rushed.
- 4 A All right. Thank you.
- 5 Okay. Great. Thank you.
- 6 Q Thank you. I appreciate that.
- 7 Okay. So the very first section under the title has a list of MCC codes.
- 8 A Uh-huh.
- 9 Q And it says: "Query for credit/debit card purchases involving any of the
10 following MCC codes," correct?
- 11 A Yes.
- 12 Q Okay. And then there is a very long list of keyword exclusions, correct?
- 13 A Yes.
- 14 Q Okay. Now, the slide itself, if you continue to look at it, makes clear that
15 not every transaction involving the listed MCC codes is going to be reported, correct? If
16 you look at the third bullet point about the 60-day rollback period.
- 17 A Correct.
- 18 Q Okay. There's several parameters from just the bank's own methodology
19 that must be met. So number one is there have to be five or more distinct and different
20 merchants/vendors of the above population set by the customer, correct?
- 21 A Uh-huh.
- 22 Q And there has to be an aggregate purchase transaction totaling \$2,500 or
23 more from the above MCC codes by the customer, correct?
- 24 A Uh-huh, yes.
- 25 Q And the number of transactions at the above MCC codes have to be greater

1 than 50 percent of the total number of transactions by the customer, and the aggregate
2 purchase amount at the above MCC codes has to be 50 percent of total purchases by the
3 customer, correct?

4 A Yes.

5 Q So if somebody were to characterize this slide as KeyBank saying they're
6 going to file a SAR for any purchase from an MCC code related to pawnshops or arms
7 stores or sporting goods stores, that would be incorrect, wouldn't it?

8 A It most certainly does not clearly indicate that this will lead to the filing of a
9 SAR. I'm not sure that it excludes the possibility that somebody could interpret that to
10 be the outcome here, right. I mean, if they -- in other words, if there were transactions
11 that fit all of these parameters, maybe they would file a SAR. I don't know that I can tell
12 from the face of the slide, but it certainly doesn't indicate that a SAR would or must be
13 filed.

14 Q And to that point, it would have to be not just that a purchase involved one
15 of the following MCC codes, but also meet those four parameters that I just read, correct?

16 A Correct, and exclude all of these others.

17 Q And exclude all of the others.

18 A Right.

19 Q So for someone to say that -- if someone were to say that FinCEN was
20 distributing a slide deck asking banks to flag purchases from MCC codes relating to
21 firearms, any purchase relating to firearms, that would be incorrect?

22 A That would be incorrect.

23 Q Okay. And the same goes for methodology number 2, correct?

24 A Correct.

25 Q Okay. And, again, when FinCEN forwards this type of information from one

1 bank to other banks, it is not asking or encouraging them to file SARs based on the
2 methodologies or typologies contained in these types of documents?

3 A Correct.

4 Q The banks are expected to use their own judgment and their own analysis,
5 based on their knowledge of their customers' database, on how best, if at all, to
6 incorporate the information in these slide decks?

7 A Correct.

8 Q Okay.

9 [REDACTED] Okay. We can go off the record.

10 [Discussion off the record.]

11 [REDACTED] We can go back on.

12 So I'd like to start by entering into the record an email from [REDACTED] dated
13 January 16th, 2021, with the subject line "Capitol Riots" into the record as exhibit 9.

14 [REDACTED] Exhibit No. 9.

15 [REDACTED] was marked for identification.]

16 [REDACTED] Okay.

17 [REDACTED] I'm also going to enter an excerpt from the Institute for Strategic
18 Dialogue's report titled, "Bankrolling Bigotry: An Overview of the Online Funding of
19 American Hate Groups" into the record as exhibit 10. This is attached to the email that
20 we just introduced -- or is linked to the email that we just introduced.

21 [REDACTED] Exhibit No. 10.

22 [REDACTED] was marked for identification.]

23 [REDACTED] Okay.

24

BY [REDACTED]

25 Q Okay. Do you remember sending this email?

1 A No.

2 Q Do you recall if you reviewed the information in the links that were included
3 in the email before you shared it with these financial institutions?

4 A I can confidently say I did not review for the purpose of evaluating or making
5 any determination. I don't recall whether I looked at it or reviewed it.

6 Q Do you know if these materials were shared with any other Federal agency?

7 A I don't know.

8 Q So among other links in this email, it includes links of the Anti-Defamation
9 League's hate symbol database, and to a report that we introduced, authored by the
10 Institute for Strategic Dialogue, titled, "Bankrolling Bigotry."

11 Does FinCEN maintain a list of American hate groups or hate symbols?

12 A Not to my knowledge. I do recall in the general context of this topic that
13 there was a list that someone at FinCEN had, but I don't know what that was derived
14 from. It may have come from these same sources or something else. I don't know.

15 Q Does FinCEN often rely on groups like these in making those determinations
16 as to what is a hate symbol?

17 A I couldn't tell you. I don't know.

18 Q Did you ever speak with the Anti-Defamation League regarding the links
19 shared?

20 A I did not.

21 Q What about with the Institute for Strategic Dialogue?

22 A I did not.

23 Q Do you know if FinCEN, anyone else at FinCEN works with groups like ADL
24 and ISD --

25 A I do not.

1 Q -- to understand their methodology?

2 A I don't know.

3 Q When you sent this email -- when did you become aware of this hate symbol
4 database, if you recall?

5 A What do you mean by hate symbol database?

6 Q It's the --

7 A Are you referring to the ADL website?

8 Q The ADL website.

9 A Oh, I don't recall.

10 Q Do you recall anyone at FinCEN having concerns about sending this report to
11 financial institutions?

12 A Not that I recall.

13 Q Did any financial institutions express any concerns when they received it?

14 A Not that I recall.

15 Q Did FinCEN intend that banks would investigate these groups that were
16 included in these lists when sending this information?

17 A I would not say that we intended any specific action. We viewed this as
18 providing information that would be helpful to them during whatever analyses they were
19 conducting.

20 BY [REDACTED]

21 Q Who at FinCEN conducts the assessment to determine what's valuable or
22 potentially valuable to private sector partners?

23 A That's a great question. Probably a lot of different divisions. I mean,
24 certainly my own division, the Strategic Operations Division, you know, that's a
25 conversation that came up a lot in the BSAAG context, you know, financial institutions

1 asking for more information to help inform their efforts instead of kind of operating blind.

2 So from a policy perspective, SOD or Policy Division might have gotten that
3 feedback or have an input on that. You know, enforcement, intelligence from a
4 substantive perspective. Front office, Main Treasury, politic -- I have no idea. I mean,
5 it could be any number of inputs.

6 Q For the inputs in this email, for example, the link from ADL, is that something
7 you would have found on your own? Is that information that's being transmitted to you
8 in preparation for drafting this email?

9 A So I have zero recollection of where any of these came from, other than to
10 tell you that it wasn't my job to generate any of this. So it didn't come from my staff or
11 me. But I don't remember who at FinCEN or other stakeholders provided these.

12 Q With the understanding you don't have a specific recollection for this email
13 and how it was prepared, for content like what's in the first paragraph, the link to the ADL
14 website, which division or, more specific, office within FinCEN would it have fallen within
15 their purview to find this kind of information and also have it transmitted to you and your
16 team?

17 A As a general matter, that kind of substantive analysis would generally be the
18 Intelligence Division.

19 Q And independent of this email, just so the record is clear, understanding you
20 didn't have any interactions with ADL about this link, just generally as part of your role at
21 FinCEN in any context, did you have any interactions with ADL?

22 A Not to my recollection.

23 Q Same with ISD?

24 A Correct. Not to my recollection.

25 Q And what about the Global Disinformation Index?

1 A Not to my recollection.

2

BY [REDACTED]

3 Q You also stated these might be of value to the financial institutions. How
4 can a financial institution use these?

5 A Is that what's in the email when I said -- saying it had value?

6 Q In response to an earlier question.

7 A Oh, is that what I said? You know, it's data points, right. When an
8 investigator or a bank is looking at a set of transactions or a customer and evaluating
9 whether the transactions or the conduct of the customer is something that warrants a
10 SAR or not, data points are helpful. So I think it's just additional data for them to have
11 access to.

12 Q So a bank might be able to take that list of groups and see, do I have any
13 customers that are these groups, and review some of their transactions to see if there's
14 suspicious activity?

15 A That might be something a bank chooses to do or not based on the receipt
16 of this. That is certainly something they could do.

17 [REDACTED] Your office specifically is not assessing the value of links and
18 documents like this, though, is that it?

19 [REDACTED] Correct. Correct.

20 [REDACTED] That would be the Intelligence Division, most likely?

21 [REDACTED] Yeah. I mean, I say as a general matter just because, right,
22 everybody brings in their own experience, right. Did we have senior advisors that
23 worked with the director that were former prosecutors that had info?

24 I mean, info could theoretically have come from any FinCEN -- you know, from a
25 personal matter. But in terms of the structure of FinCEN, that kind of substantive

1 analysis was generally the Intelligence Division.

2 I should also say that FinCEN has a division that was newly stood up while I was
3 there. I believe it's called Global Investigations. I don't recall it being a division at this
4 time. I don't remember one way or the other, and I don't recall, given the domestic
5 nature, that it was involved at all. But I wanted to raise that because most of my
6 answers when I say things like the substantive analysis would generally be ID, I would add
7 that, if appropriate, it would also be the Global Investigations Division.

8 I've sort of forgotten them. Don't tell Matt, if it's still Matt.

9 So that would be the second sort of primary division that substantively crunches
10 BSA data for that purpose.

11 [REDACTED] Who's the head of that division?

12 [REDACTED] When I was there, it was a guy named -- was it Matt Stiglitz?

13 [REDACTED] Uh-huh. Still is.

14 [REDACTED] Still is. So he's the head of that division.

15 But, again, I'm not even sure if it was a division at this time, nor, given the global
16 nature of it, do I think it was involved. I just -- you've asked a lot of general questions of
17 who would it be, who would it be, and I keep saying ID, ID. And just occurred to me it's
18 probably also GID in many cases.

19 BY [REDACTED]

20 Q In early 2021, do you have a sense of how big the Intelligence Division is?

21 A I have a general sense. It was one of FinCEN's larger divisions. Certainly
22 less than a hundred. I'm pretty sure more than 30 or 40. I'm not sure I can get much
23 more specific, but it was one of the larger divisions.

24 Q Understanding you didn't have any interactions as part of your role, to your
25 understanding, did others at FinCEN have any relationships or just even points of contact

1 with ADL?

2 A Not that I'm aware of.

3 Q This is intended just as a general question, if you have any awareness. In
4 response to an earlier question, you mentioned that providing data points -- that data
5 points could be helpful. In any context, are you aware of any assessment being
6 conducted about whether certain data points came from political sources or sources with
7 certain political objectives that might change how the dataset was compiled or would
8 raise any concerns about the impartiality of it?

9 A I don't recall those conversations one way or the other.

10

BY [REDACTED]

11 Q The email also states that MUFGE kindly circulated the ISD report. Did you
12 ever speak with MUFGE about their report?

13 A I don't have a specific recollection. I mean, I can confidently say I would
14 not have had a substantive conversation with them. Was I the person who received it or
15 not? I may have been. I don't recall.

16 Q Do you recall if they indicated how it was using their report when they sent it
17 to you?

18 A No.

19 Q Do you know if they had had any conversations with ADL or ISD?

20 A I do not.

21 [REDACTED] Who was your primary point of contact at MUFGE?

22 [REDACTED] I don't recall having a specific primary point of contact. Generally,
23 whoever it was in the context of this activity would probably be the folks on this email.

24 Give me a second and let me see if I can refresh my recollection.

25 I believe of these folks that are listed on the email, it was M. Roth is my

1 recollection of being the primary.

2 [REDACTED] Do you recall for this individual what their first name was?

3 [REDACTED] I don't. I feel like I want to say Monique, but I don't know for
4 certain.

5 [REDACTED] I'd now like to enter an email from [REDACTED] dated
6 January 18, 2021, with the subject line "Capitol Riots" into the record as exhibit 11.

7 [REDACTED] Exhibit No. 11.

8 [REDACTED] was marked for identification.]

9 [REDACTED] This is January 18th, right?

10 [REDACTED] Yes.

1 [3:58 p.m.]

2

BY [REDACTED]

3

Q Do you remember sending this email?

4

A Not specifically, no.

5

Q Can you explain what the purpose of the email is?

6

A Not beyond the words on the page. It appears it was more information

7

that could potentially be used to narrow the scope of activity that they were looking at.

8

Q Narrow the scope of activity to what? What do these identify?

9

A So I have a general recollection that some of the funding, we were aware -- I

10

don't recall how, whether from law enforcement or whomever -- that some of the

11

funding mechanisms that supported the events of January 6th were through

12

crowdfunding websites.

13

So the thinking was, by identifying possibilities of what those funding mechanisms

14

were, it could be, again, another data point that could be used to try to understand a

15

particular customer's activity or, broadly, customers' activity.

16

Q So the email also states that FinCEN has observed people using the site to

17

post an event and sell tickets, including bus tickets, to the demonstrations, and then

18

identifies a transaction reference.

19

Is selling tickets to events or demonstrations evidence of potentially suspicious

20

activity?

21

A So, first, I would note there's no indication that FinCEN said this. I don't

22

recall what the source of this info was. The info says, "People have been observed using

23

this site." I don't -- that could have come from law enforcement, it could have come

24

from a bank that shared it. I don't recall where it came from. So I don't know for a fact

25

that this was FinCEN saying.

1 But, no, like everything else, no specific data point was intended to convey a
2 determination of suspicion. It was just a data point, a factor.

3 Q And what is a transaction reference?

4 A To the best of my knowledge, like if you were to go and log into your bank
5 app right now and look at your own card purchases, like if you're not filling anything out
6 when you use your card, whether it's the merchant or whomever, I'm not certain, like
7 there's some reference that's attached to those card purchases.

8 So I believe that's what this is a reference to.

9 Q And so in this instance, what are those transaction references identifying?

10 A It appears the use of Eventbrite. It also specifies a particular phone
11 number. I don't know what that phone number is. I'm not really sure that I can
12 answer that, actually.

13 Q One of the things the email mentions is, for example, "EB March for TR."
14 Are you aware of what that was short for?

15 A No.

16 Q Could it have been Eventbrite, March for Trump?

17 A I don't know.

18 Q And you're not aware of how you became aware of this transaction
19 reference?

20 A Correct. I have no recollection of what the source of this info was.

21 Q And so if a financial institution --

22 [REDACTED] Is this -- do you have -- it looks like a whole email chain. I'm not
23 sure if there's more info --

24 [REDACTED] There is.

25 [REDACTED] -- in other parts of this chain. But --

1 [REDACTED] Not relevant to this topic.

2 [REDACTED] No? Okay. I mean, I --

3 [REDACTED] Well, I think that's for him to decide.

4 [REDACTED] Yeah, I don't know one way. Certainly, I have no recollection, nor
5 on the face of this does it give me any information to answer that question.

6 [REDACTED] So if a financial institution that's on this email inserted the
7 transaction reference that you identified, what would that return?

8 [REDACTED] I'm not sure I understand. Insert -- inserted that where?

9 [REDACTED] Well, that's my question. I'm trying to understand how this
10 transaction reference is used.

11 [REDACTED] If you know.

12 If that would be a question for him or the financial institutions as to how they're
13 going to use it.

14 [REDACTED] Yeah. I mean, again, I think I kind of addressed this earlier. Like,
15 it would depend, I suppose, on what systems they have in place to query their own data.
16 I can't even represent that all of these institutions have the ability to query in that
17 manner. I don't know.

18 BY [REDACTED]

19 Q For an email like this one, obviously there's a list of names, and based off
20 your recollection very likely received that from someone else within FinCEN.

21 So the text of Eventbrite, for example, are you on the receiving end of that text,
22 you're just copying and pasting it into the email, or are you playing some role in the
23 editing process summarizing what you received?

24 A I did not make any substantive edits to the information that I received from a
25 substantive perspective. I also wouldn't assume this came from FinCEN. I don't know

1 what the source of this info was.

2 Again, I was disseminating it. It may have come from another financial
3 institution, it may have come from law enforcement, it may have come from FinCEN. I
4 don't recall. And my staff and I would not have played any role in changing any of that
5 content.

6 Q Even down to the -- for example, for an email like this, typically, that would
7 be --

8 A None of this --

9 Q That was already -- whoever it was, whether it was --

10 A None of this is my work product or my staff's.

11 [REDACTED] And just so we're clear for housekeeping, the email you guys
12 are asking about is an internal email that was just among the banks, if you look at the top.
13 You've just been asking him questions about the email that he sent below.

14 But just so the record is clear, that top part should probably be redacted.

15 [REDACTED] And for what it's worth, when you forward something along, you
16 can edit it. So I'm -- I can't even represent that this is an accurate depiction of what I
17 sent. I don't think it matters one way or the other because I don't recall. But, I mean,
18 technically. But yeah, I mean, sort of the messenger here.

19 BY [REDACTED]

20 Q I'll represent that we received this exact email from several different
21 financial institutions.

22 Had you used transaction references before?

23 A Meaning like has FinCEN ever disseminated information about transaction
24 references?

25 Q Sure. Have you disseminated information about transaction references

1 before or after this one?

2 A I have a general recollection that some advisory or advisories along the way
3 would have referenced maybe, for example, like wire details or some sort of reference
4 number information. It's not an uncommon factor.

5 Q When the email says observing people, do you know what that means,
6 "People have been observed"?

7 A I do not.

8 Q And you're unaware of how those people may have been observed?

9 A Correct.

10 Q Does FinCEN monitor crowdfunding sites?

11 A I have no knowledge one way or the other.

12 Q And did you ever communicate with Eventbrite?

13 A No.

14 Q GoFundMe?

15 A None of these names I have ever communicated with.

16 Q Are you aware of anybody else at FinCEN who may have communicated with
17 these crowdfunding sites?

18 A Not that I'm aware of.

19 Q And I assume you didn't inform these crowdfunding sites that these
20 transaction references may be being monitored?

21 A I personally did not. I don't have any knowledge of whether that had
22 happened.

23 Q The second line of the email states "Anedot.com,"
24 and follows with, "You may see a Card Purchase with the transaction reference in the
25 following format: 'A [a message or like a cause or candidate] with the phone number in

1 the following format,'" and then has the phone number.

2 What is Anedot.com?

3 A I have no idea.

4 Q Do you have any idea why Anedot was targeted?

5 A I'm not sure I would agree with the premise of that question, but I don't
6 have any knowledge either way.

7 Q Do you have any idea what transactions this transaction reference might
8 identify?

9 A No.

10 [REDACTED] Do you know if this refers to political contributions?

11 [REDACTED] I do not know one way or the other.

12 [REDACTED] Did you have to seek any approval or discuss with anyone any of
13 the transaction references in this email before sending it?

14 [REDACTED] I don't recall.

15 [REDACTED] During this time period, are you aware of any contents, whether it be
16 tied to this email chain, of where political donations were a typology or something that
17 contributed to?

18 [REDACTED] I'm not aware of that, no.

19 [REDACTED] Can we just go off the record?

20 [Discussion off the record.]

21 [REDACTED] We can go back on.

22 Okay. I'd now like to enter an email from [REDACTED] dated January 16th,
23 2021, and one of the attachments, "MUFG Typology slide," with the subject line "Capitol
24 Riots," into the record as exhibit 12.

25 [REDACTED] Exhibit No. 12.

1 was marked for identification.]

2 [REDACTED] Okay.

3 BY [REDACTED]

4 Q Do you remember sending this email?

5 A No.

6 Q Do you recall if there were any discussions at FinCEN before sending this
7 email?

8 A No. I don't recall.

9 Q The email states that the attachments are from MUFG.

10 Do you have any idea why MUFG sent these attachments or shared these
11 attachments?

12 [REDACTED] Just for the record, I think he only has one of the two
13 attachments on this actual exhibit, right?

14 [REDACTED] Yeah. I only entered one of the attachments into the record.

15 [REDACTED] Okay. Yeah. I mean, well, as a general matter, that's what these
16 discussions were, a forum for the sharing of information if anyone was so inclined. So
17 you can infer that MUFG felt inclined to share this.

18 BY [REDACTED]

19 Q And do you remember discussing these materials with MUFG?

20 A No.

21 Q Do you remember in those discussions just trying to elicit some of this
22 information sharing?

23 A I don't remember any such discussions one way or the other.

24 Q Do you recall, once you received these materials from MUFG, what you did
25 with them?

1 A I do not specifically recall. I can confidently say that I would have
2 disseminated them internally to the appropriate group, and then, again, either sought
3 approval to disseminate or at the time felt that it was something that I had approval to
4 disseminate.

5 Q And who would be the appropriate groups to disseminate something like
6 this to internally?

7 A I think I addressed this earlier. I don't specifically recall. I mean, there
8 was definitely an internal group of FinCEN folks that were generally working on this topic
9 and involved, ID folks being the most prominent to my recollection. But I don't really
10 recall beyond that.

11 Q Turning to the slide itself.
12 Do you recall whether you reviewed this slide?

13 A I don't recall one way or the other. Again, I would note that I would not
14 have reviewed it -- I wouldn't have done anything but read it. I wasn't evaluating or
15 reviewing it for substance.

16 Q How would a bank use the typology and the MCC Codes it lists to review
17 certain transactions?

18 A Well, to the extent that they're able to search those types of information in
19 their systems, they would, I guess, search for that code and isolate for review those
20 transactions, I guess, or would be one factor that they would use to apply in a search.

21 Q And this slide lists transfers to GiveSendGo or other crowdfunding sites.
22 Are you aware of whether FinCEN or MUFG was scrutinizing these kinds of
23 transactions?

24 A I'm not aware.

25 Q The note at the bottom also mentions DIA.

1 Do you know what DIA is?

2 A My assumption, based on nothing but the page, is that it's the Data Insights
3 and Analytics team at MUFG, which is in the title of the slide.

4 Q And it also mentions may warrant escalation.

5 A I think what it actually says is that there's no single hit may warrant
6 escalation, but more than one could.

7 So it reinforces the notion that these banks understood that they weren't being
8 told that any one of these factors was requiring or expecting or should lead to a SAR.

9 It was a data point that they could use if they wanted to for evaluation. I think
10 that's, essentially, what MUFG is saying there.

11 Q And so the question I was going to ask is, when it says warrant escalation,
12 what does that mean to you?

13 A Warrant escalation -- well, it depends on the parlance of the individual bank.
14 I read this, I think they mean file a SAR. It could just be a reference to some step prior to
15 that internally.

16 I mean, they may have a -- some banks have, like, a level one, and if they see
17 something that's a maybe, it goes to the level two that are a little more experienced to
18 make those determinations.

19 So I don't know what they mean here, but one of those.

20 Q It also mentions that DIA will, quote, "look to sort for these typologies via
21 in-person versus online purchases."

22 Do you have any idea what that means?

23 A I do not.

24 [REDACTED] So you've mentioned the Intelligence Division and the Global
25 Investigations Division.

1 Are there any other divisions that review and analyze and evaluate BSA data?

2 [REDACTED] So I definitely answered this earlier. I mean, several divisions do
3 for different reasons. I mean, Policy for policy reasons and advisory reasons,
4 Enforcement for enforcement activity. Some folks in SOD for -- we have the global FIU
5 component.

6 So many, if not most, divisions of FinCEN may have some reason to review BSA
7 data. And, of course, best ask FinCEN that question. I don't know.

8 BY [REDACTED]

9 Q Turning back to the previous exhibit, the typologies via in-person versus
10 online, independent of this email, just at a high level, are you aware of any sort of
11 discussion as to what that might mean, how typologies might apply for in-person
12 transactions but be different if the transaction is made online?

13 A I'm sorry. Will you restate that question for me?

14 Q Sure. Independent of this email, during your time at FinCEN, do you recall
15 any sort of discussions about typologies applying for in-person purchases as opposed to
16 online purchases, whether they be different lists or prioritizing different typologies.

17 A Yeah. I mean, I definitely do not recall some, like, standalone factor turning
18 on whether it was in-person or online. Like that doesn't really make sense to me.

19 Totally separate from anything we've been discussing, there are certain red flags
20 that may only be present in person.

21 So, for example, bank tellers are generally trained to spot people that are antsy
22 and uncomfortable. Or you'll commonly see a SAR where somebody tries to withdraw
23 10,000 bucks, they get asked to fill out a form, and they say, "Oh, just kidding, I only need
24 9,000." They're supposed to file a SAR because that's somebody avoiding.

25 That would only generally be in person. Cash, of course, would only be in

1 person.

2 Online you get a whole different -- you talked about identity fraud and login
3 credentials.

4 So there are certainly significant differences there. But in terms of, like, here's a
5 type of conduct and it only is meaningful in one, that, I don't -- that's not familiar to me.

6 [REDACTED] We can go off the record.

7 [Discussion off the record.]

8 [REDACTED] Back on the record.

9

BY [REDACTED]

10 Q I want to start with exhibit 12, the slide from MUFGB, the "GFCD Intelligence
11 & Analytics, Data Insights and Analytics."

12 A That's the most recent? Okay. Yep. Got it.

13 Q Okay. So you pointed out the note on the bottom of the slide, which says,
14 "DIA plans on looking at these typologies holistically, that is no single hit may warrant
15 escalation but more than one could."

16 A Uh-huh.

17 Q And that is consistent with all of your testimony about how these typologies
18 are intended to be used and, in your experience, how they are used by banks, correct?

19 A Yes.

20 Q Okay. Now, in the majority's March 2024 report, it states that, according to
21 this particular slide, quote, "Account information and transactions meeting any of the 11
22 typology criteria may have been flagged and shared with Federal law enforcement as
23 being suspicious," end quote. And that's on page 29 of the report.

24 Is that an accurate statement based on your understanding of this --

25 A No. It's contradicted on its face by the incident.

1 Q Okay. Now, going back to the exhibit number, which I can't
2 remember -- exhibit 10 -- or I guess it was 9 and 10, the email that had several different
3 links attached, including -- and then exhibit 10 is the excerpt from the ISD report.

4 Let's start with exhibit 10. And this should be clear from all of your testimony so
5 far, but just for the record, in circulating this you did not intend to suggest that
6 membership in any one of the organizations here was sufficient to trigger a suspicious
7 activity report, correct?

8 A Correct.

9 Q Okay. Now, the majority's report claims that FinCEN's distribution of this
10 ISDN report and the ADL link amounts to an approval of its contents, methods, and
11 conclusions.

12 Do you agree with that statement?

13 A No. And I'm not sure I'm the right person to ask that question, but I don't
14 personally agree with that, no.

15 Q Fair enough. Okay.

16 Now let's take a look at exhibit 11, which is the exhibit with a list of crowdfunding
17 sites.

18 Now, you noted that at the bottom of this exhibit it is clear that this is part of an
19 email thread, and the bottom of this exhibit shows the "from" and "to" line of an email
20 you sent on Sunday, January 17th, 2021, at 4:06 p.m.

21 And I am just going to represent for the record that that email was an email from
22 you to these recipients with a link to a list from the Department of Justice of individuals
23 who had been charged with offenses related to their roles in January 6th.

24 A Okay.

25 Q Does that sound familiar, like something you might have sent?

1 A I mean, I don't have any recollection. It sounds on brand of what we were
2 doing, but --

3 Q Fair enough.

4 Okay. Now, by sending this list of crowdfunding sites, were you asking financial
5 institutions to file SARs for any transactions with crowdfunding sites?

6 A No.

7 Q And did you -- were you trying to hint to them or encourage to them that
8 any crowdfunding site transaction should be flagged?

9 A No.

10 Q Now, in the majority's report they stated that, according to this email, simply
11 purchasing a ticket to an event was enough for FinCEN to consider this activity as
12 suspicious.

13 Is that accurate?

14 A No.

15 Q And they also say that FinCEN was soliciting and encouraging financial
16 institutions to report on the accounts of any persons involved in crowdfunding events or
17 demonstrations in support of President Trump.

18 Is that accurate?

19 A No.

20 Q The majority has alleged that FinCEN has engaged in a pattern of financial
21 surveillance aimed at millions of Americans who hold conservative viewpoints or who
22 simply exercise their Second Amendment rights.

23 What's your response to that allegation?

24 A I never encountered any information or discussion that made me think that
25 while I was at FinCEN.

1 Q And the majority claims that FinCEN and law enforcement commandeered
2 financial institutions to spy on Americans.

3 What's your response to that allegation?

4 A Did not happen.

5 Q All of FinCEN's communications with financial institutions were pursuant to
6 Federal statutes, correct?

7 A To the best of my knowledge.

8 Q Thank you very much.

9 A And I wasn't the person in charge of evaluating that.

10 Q Fair enough.

11 [REDACTED] And with that, we can go off the record.

12 [Whereupon, at 4:27 p.m., the interview was concluded.]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Certificate of Deponent/Interviewee

I have read the foregoing ____ pages, which contain the correct transcript of the answers made by me to the questions therein recorded.

Witness Name

Date



Domestic Terrorism: A Threat to the Financial System

American Bankers Association Webinar
Wednesday, September 28, 2022
2:00 – 3:00 p.m. ET

© 2022 by American Bankers Association.

Presenters



FTI Consulting



Wells Fargo



AML Associates

Peter Sullivan
Senior Private Sector Partner Outreach
Counterterrorism Division, Strategic Partner Engagement Section
Federal Bureau of Investigations

aba.com1-800-BANKERS



© 2022 by American Bankers Association.

Disclaimer

This webinar will be recorded with permission and is furnished for informational use only. Neither the speakers, contributors nor ABA is engaged in rendering legal nor other expert professional services, for which outside competent professionals should be sought. All statements and opinions contained herein are the sole opinion of the speakers and subject to change without notice. Receipt of this information constitutes your acceptance of these terms and conditions.

Attendance Poll

**Thank you for participating in
today's attendance poll.**

CONTINUING EDUCATION CREDITS REQUIREMENTS

- You **must be registered**, and your attendance **must be validated** in order to earn continuing education credits for this live broadcast.
- Responses to 3 random prompts must be made within 30 seconds of viewing each prompt
- Attendance will be validated by ABA
- A **certificate of completion** will be available on your transcript in your ABA eLearning account
- You will receive an email with instructions on how to access your certificate within 5 days post-webinar

Agenda

- Understanding the Landscape
- Ideology & Radicalization
- Cases/Trends/Typologies
- Private-Public Sector Partnership

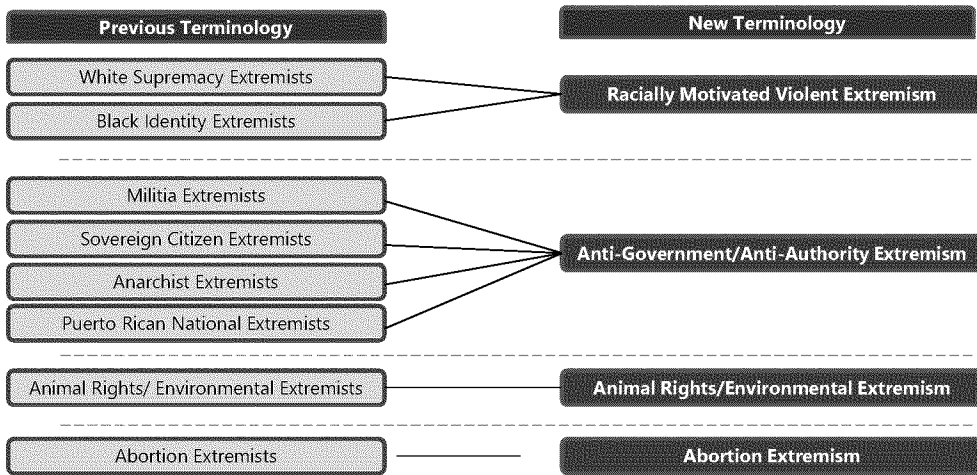
Terrorism Threat to U.S. Homeland



aba.com1-800-BANKERS



Domestic Terrorism Threat Categories



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Priority Terrorism Threat: *Domestic Violent Extremists*

Hate is not a crime
We **cannot** investigate First Amendment protected speech

- FBI is the **lead US agency** responsible for domestic terrorism.
- Racially Motivated Violent Extremists are responsible for the **most lethal activity**.
- **Lone offender attacks** have served as the dominant mode for lethal violence, primarily using firearms
- **Anti-Authority/Anti-Government** Violent Extremism is an emerging threat which includes several sub-categories such as Anarchist Violent Extremism and Militia Violent Extremism
- The FBI currently has ~2,000+ pending DVE investigations spanning all 50 states

FBI's Authority to investigate Domestic Terrorism requires the following...*

The existence of a potential federal violation	The unlawful use of force or violence	The existence of ideological motivation
---	--	--

aba.com1-800-BANKERS

UNCLASSIFIED//FOR OFFICIAL USE ONLY

9

 American Bankers Association
*Source: 18 U.S.C. 2331(5)

Situational Awareness from a Terrorist Financing Perspective

- Situational awareness is being aware of your physical surroundings for personal safety and security
- Situational awareness from a terrorist financing perspective should focus on and *understand*:
 - The threat
 - The threat environment
 - Current and emerging trends
 - Who you are dealing with
 - Organizations (global / regional / local)(centralized or decentralized)
 - Individuals (inspired / enabled / directed)
 - Funding flows
 - Sources / methods / access
 - Raise→**Placement**→Move→**Layering** →Store→**Integration**→Spend



FinCEN AML/CFT National Priorities June 30, 2021

- Terrorist financing
 - Since 9/11, threat has evolved significantly
 - *Terrorists require financing to recruit and support members, fund logistics, and conduct operations*
 - *Terrorist financing includes lone actors using small amounts of money to self-fund attacks, as well as more complex schemes and networks that may be embedded within existing money laundering methods used to support logistical networks, operations, and the procurement of materials*
 - International terrorism
 - Most terrorist groups still primarily rely on banks, MSBs and cash couriers to transfer funds
 - ISIS & al-Qaeda now rely more on self radicalized individuals & HVEs
 - Carry out low cost & unsophisticated but deadly attacks
 - Domestic terrorism
 - DVEs are individuals based & operating primarily within U.S. jurisdiction
 - Seek to further their ideological goals through unlawful acts of force or violence
 - RMVEs & militia violent extremists present the most lethal DVE threats

aba.com1-800-BANKERS

11



2022 National Terrorist Financing Risk Assessment

- Issued 2/2022, by U.S. Treasury Department
 - Methodology based on FATF guidance
 - Underlying concepts for risk assessment are threats, vulnerabilities, consequences and risk
 - Consistent with 2020 National Terrorist Financing Risk Assessment
 - FinCEN AML/CTF 2021 National Priorities based on 2020 Risk Assessments
- **2022 Threats & Vulnerabilities**
 - **Threats**
 - ISIS
 - al-Qaeda
 - Hizballah
 - Other foreign terrorist groups
 - Domestic violent extremists
 - **Vulnerabilities**
 - Banks
 - MSBs
 - Unlicensed money transmission
 - Cash
 - Virtual currency
 - Misuse of charitable organizations

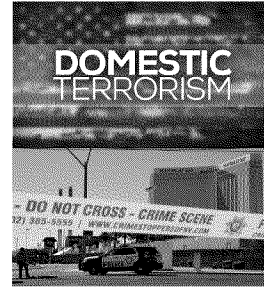
Greatest Threat to U.S. Homeland

- Congressional testimony of FBI Director Christopher Wray on August 4, 2022 (Senate Judiciary Committee)
 - The nature of threat posed by terrorism, both international and domestic, continues to evolve
 - Posed by lone actors or small cells radicalized online who look for soft targets with easily accessible weapons
 - *Domestic violent extremists (DVEs)*
 - *Homegrown violent Extremists (HVEs)*
 - Two distinct threats, both of which located primarily in the U.S. and typically radicalize and mobilize to violence on their own
 - Foreign terrorist organizations (FTOs), such as ISIS and al-Qaeda, intend to carry out or inspire large scale attacks in U.S.
 - *ISIS / al-Qaeda advocate for lone offender (HVE inspired attacks)*
 - Iran and its global proxies and partners continue to attack and plot against U.S. and allies throughout Middle East
 - Hizballah, Iraqi Shia militant groups & Iran's Revolutionary Guard



Domestic Terrorist Threat Environment

- FBI classifies domestic terrorism into five categories:
 - ***Racially motivated violent extremism***
 - ***Most acute threat***
 - Anti-government / anti-authority extremism
 - Animal rights / environmental extremism
 - Abortion extremism
 - Other
 - Involuntary celibates (Incel)
 - Political extremism
- Drivers include
 - Perceptions of government or law enforcement overreach
 - Socio-political conditions
 - Reactions to legislative actions
- Radicalization increasingly taking place online
- Domestic terrorists increasingly communicate with like minded individuals overseas, to include overseas travel



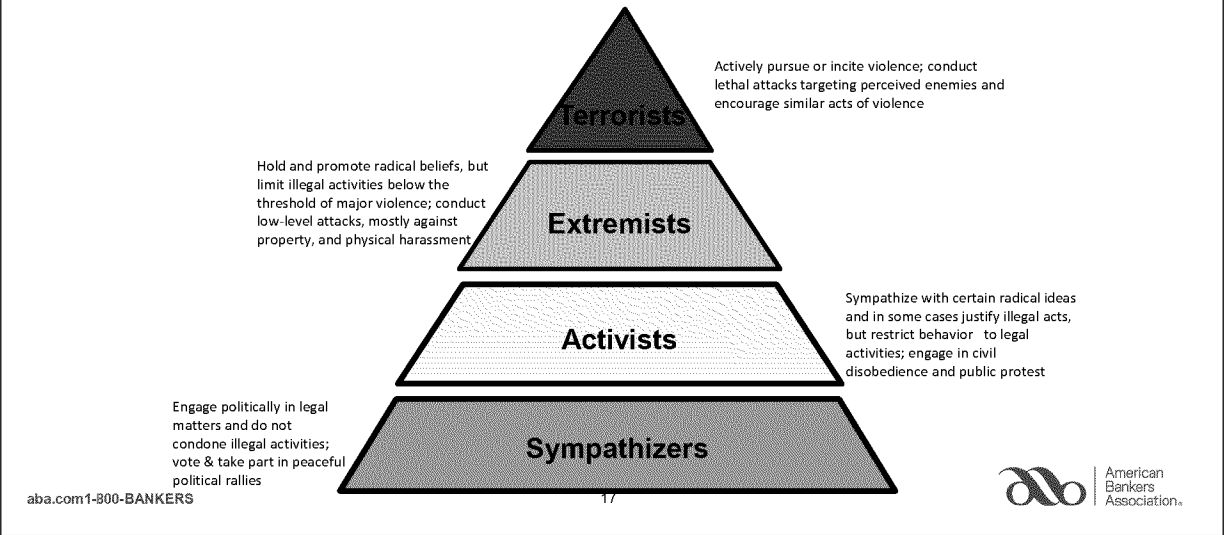
Comparing and Contrasting HVEs & DVEs

- Homegrown Violent Extremists (HVEs)
 - Individuals who have been radicalized primarily in the U.S.
 - Inspired by, but not receiving individualized direction from, foreign terrorist organizations (FTOs)
 - *8/20/2022 call by al-Qaeda for “lone wolves” to fight “enemies of Islam”*
- Domestic Violent Extremists (DVEs)
 - Individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government sentiment
 - The top threat from DVEs stems from those identified as racially / ethnically motivated violent extremists (RMVEs)
 - *Two Boogaloo Boys provided material support to Hamas to raise funds to open training camp; considered Hamas a likeminded anti-government group*
- Many violent extremists (HVEs & DVEs) are motivated and inspired by a mix of ideological, sociopolitical, and personal grievances against their targets
 - Radicalization is an extremely dynamic and highly individualized process
 - HVEs / DVEs select soft familiar targets

National Terrorism Advisory Bulletin

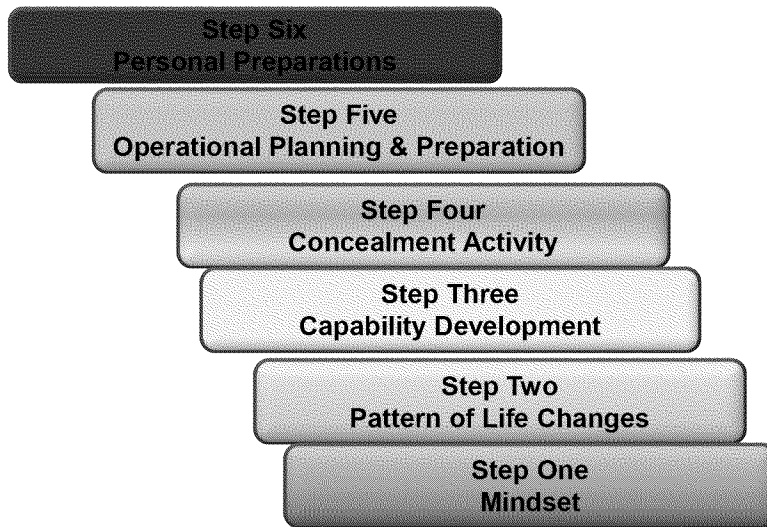
- Issued 6/07/2022 by Homeland Security replacing NTAS bulletin issued 2/07/2022 (expires 11/30/2022)
 - The U.S. remains in a heightened threat environment, as noted in previous bulletin
 - Threat environment expected to become more dynamic
 - High-profile events could be exploited to justify acts of violence
 - » *Mar-a-Lago search warrant on 8/08/2022 such a trigger event*
 - » Homeland Security issued threat bulletin to law enforcement on 8/12/2022
 - Threat actors have mobilized to violence due to factors such as personal grievances, reactions to current events, and adherence to violent extremist ideologies
 - Racially or ethnically motivated or anti-government / anti-authority violent extremism
 - Foreign terrorist organizations and nation states
 - ***Primary threat of mass casualty violence in U.S. stems from lone actors and small groups motivated by a range of ideological beliefs and / or personal grievances***

Taxonomies Shaping Terrorist Radicalization



© 2022 by American Bankers Association.

Financial Warning Signs in Steps to HVE & DVE Radicalization

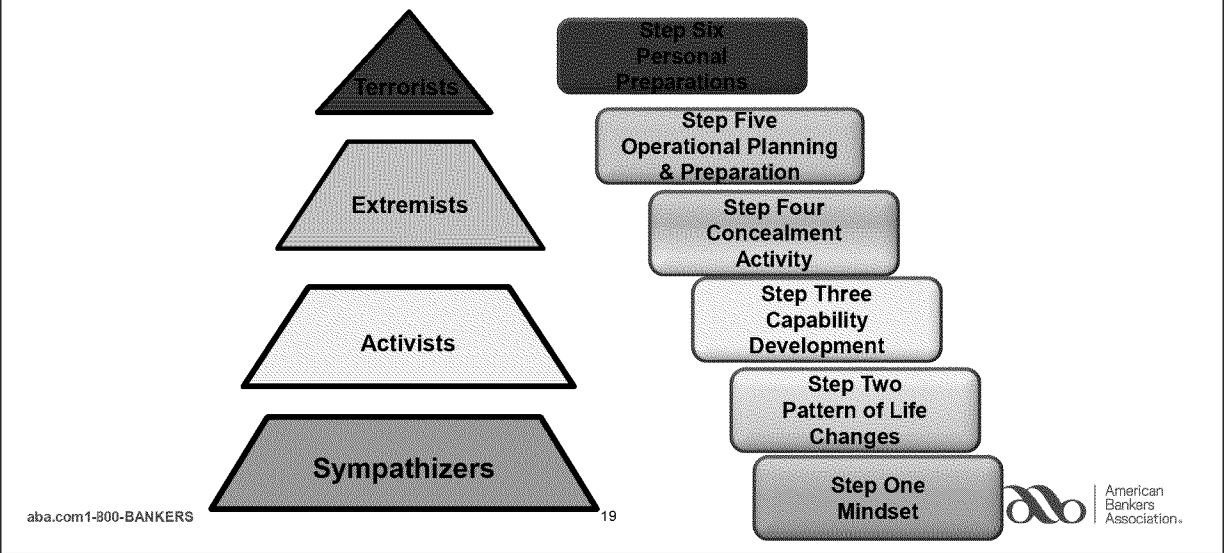


aba.com/1-800-BANKERS



© 2022 by American Bankers Association.

Steps to HVE & DVE Radicalization



© 2022 by American Bankers Association.

Radicalization & Warning Signs

- Sympathizer (interest in cause) → *legal*
 - Mindset
 - Payments related to extremist political activity or donations to the cause
- Activist (engagement in cause) → *legal*
 - Lifestyle change
 - More financial commitment to the cause
 - Capacity development
 - Purchase weapons, gear, literature & other inflammatory propaganda
- Extremist (as passion & commitment grow, escalates from non-violent to violent) → *from legal to illegal*
 - Concealment of activities
 - Realization that law enforcement might be looking at them (financial activity)
 - Operational planning & preparation
 - Plan, surveil, select targets, travel & other activity leading them toward action
- Terrorist → *illegal*
 - Personal preparation
 - Finalize their personal preparation, settle their business & move into action

Issues for Banks in Domestic Terrorism Scenarios

- No designated domestic terrorism groups
- No crime of providing material support to domestic terrorism groups
- Banks don't want to interfere with customer's First Amendment rights
- Banks are required to protect the privacy and information of their customers – where to draw the line?
- Banks have reputational risk concerns:
 - Don't want to be associated with groups that espouse racist or hateful political views
 - Don't want to de-risk customers based on political views

Private-Public Sector Partnership

- Value of SAR filings
- Important information in SAR narrative
- FIU information available to include
- Direct contact and engagement

2022 Upcoming Webinars

Fall / Winter 2022

- Regulatory Updates and Compliance Challenges (*October 19*)
- The Evolution of Economic Sanctions (*November 9*)
- Top Risks for Banks in 2023 (*December 15*)

Visit [ABA.com](https://www.aba.com). Webinars are always being added!



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

BSA CONFIDENTIAL

July 31, 2024

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Jordan:

I write in response to your April 24, 2024, letter requesting certain reports maintained by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). Following scoping discussions with your staff,¹ as well as necessary review and consultation with law enforcement, the Department has identified [REDACTED] that are responsive to your request. As described below, the Department is providing these documents to the Committee on the Judiciary.

As you know, SARs and information revealing the existence of SARs are highly sensitive and confidential. These documents contain personally identifiable information, details about financial transactions, and unconfirmed information regarding potential violations of law or regulation. The Bank Secrecy Act (BSA) authorizes the Department to require financial institutions to provide "certain reports or records that are highly useful in criminal, tax, or regulatory investigations, risk assessments or proceedings." 31 U.S.C. § 5311(1)(a). At the same time, the Department has an obligation to safeguard the confidentiality of BSA information. Any disclosure of BSA information to the public can compromise the national security of the United States and potential or ongoing law enforcement actions, as well as threaten the safety and security of those institutions and individuals who file such reports. Unauthorized disclosures also may cause unjustifiable and irreparable harm to an innocent party involved in a reported transaction.

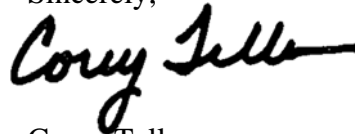
The Department is providing these documents to the Committee to accommodate its efforts to investigate the matters described in its April 24, 2024, letter, and the Department authorizes the Committee to review the documents for that purpose, subject to the condition that Committee Members and staff maintain the confidentiality of this material and the information therein. The BSA provides that a SAR and any information that would reveal the existence of a SAR are confidential. 31 U.S.C. § 5318(g)(2)(ii). These documents or the information therein should not be disclosed to, accessed by, or disseminated to unauthorized individuals in any fashion. Any member of the Chairman and Ranking Member's staff who learns of any

¹ As discussed with staff on May 7, 2024, this production contains [REDACTED]

unauthorized disclosure should promptly notify the Department of the nature of the disclosure and of any responsive measures taken by the Committee.

Given the highly sensitive nature of the documents we are providing, consistent with the Department's past practice and as the Committee has previously agreed, we will make the document production available for review by Committee Members and authorized staff in a reading room. Only those Members or staff with a "need to know" will be given access to the documents provided in the reading room. As you know, a reading room has been scheduled for [REDACTED], at the Department. To arrange future reading room access, as needed, please contact the Office of Legislative Affairs.

Sincerely,



Corey Tellez
Acting Assistant Secretary
Office of Legislative Affairs

cc: The Honorable Jerrold L. Nadler, Ranking Member

For Feedback: Third Party Vendors Working Group Draft White Paper

From: BSAAG <[REDACTED]@fincen.gov>
To: BSAAG <[REDACTED]@fincen.gov>
Cc: [REDACTED]@us.mufg.jp [REDACTED]@golden1.com
Date: Mon, 05 Feb 2024 08:42:38 -0600
Attachments: Third Party BSA Data Sharing Clean Draft Aug 2023 v5.docx (80.35 kB)

Good Morning BSAAG Members,

As we mentioned during the January 18th plenary meeting, we are circulating for your feedback the draft white paper from the Third Party Vendors Working Group. As always, BSAAG documents are confidential and may not be shared outside the BSAAG membership base.

This white paper addresses unique issues that arise with BSA data and third-party relationships, and offers tips and best practices for financial institutions and recommendations for FinCEN.

The objectives of this white paper are:

- To communicate to financial institutions (FIs) subject to BSA requirements clear, consistent, cross-industry guidance/practices for information security and confidentiality when sharing BSA data with third parties.
- To highlight for FinCEN various third-party relationship topics that it may wish to explore further, particularly as FinCEN considers establishing appropriate frameworks for information sharing among FIs, their agents, and service providers.

If you have any feedback, please reach out to [REDACTED] (MUFG) and [REDACTED] ([REDACTED] Golden 1 Credit Union)—both copied—who are the co-leads of this working group. Please provide feedback by March 1, 2024.

[REDACTED]
Liaison to Industry
FinCEN

CLEAN DRAFT – 8/25/23**Bank Secrecy Act Advisory Group (BSAAG) Information Security and Confidentiality Subcommittee****Sharing BSA Data with Third Parties: Guidance and Recommendations****I. Introduction / Scope****II. Definitions**

- A. BSA Data
- B. Third Party Relationships
 - 1. Business Relationships
 - 2. Affiliate Relationships
 - 3. Agency Relationships

III. Legal and Regulatory Framework

- A. Suspicious Activity Report Confidentiality and Sharing
 - 1. SAR Sharing with Affiliates located in the U.S.
 - 2. SAR Sharing with Business Relationship Partners.
 - 3. SAR Sharing with Agents
- B. Sharing Information Under Section 314 of the USA PATRIOT Act
- C. Sharing BSA Resources
- D. Anti-Money Laundering Act of 2020
- E. Other Requirements
 - 1. General Third-Party Risk Management Guidance
 - 2. Guidance on FinTech Business Relationships
 - 3. Gramm-Leach-Bliley Act Information Security Requirements
 - 4. Other BSA and Privacy Considerations
 - 5. Securities and Derivatives Requirements
 - 6. FINRA Requirements
 - 7. Casinos – Special Requirements

IV. Guidance / Best Practices Useful to BSA Regulated FIs**V. Recommendations / Observations / Suggested Action**

- A. Data Sharing with Specialized BSA Business Relationship Partners
- B. Third Party Data Security Protocols
- C. Contract BSA Investigative Resources
- D. Section 314(b) Information Sharing

I. Introduction / Scope

Section 6302 of the Anti-Money Laundering Act of 2020 (AML Act) authorized the Secretary of the Treasury to form the Subcommittee on Information Security and Confidentiality (the “Subcommittee”) within the BSAAG. The Subcommittee, a private/public partnership, exists to “advise the Secretary of the Treasury regarding the information security and confidentiality implications of regulations, guidance, information sharing programs, and the examination for compliance with and enforcement of the provisions of the Bank Secrecy Act.”

After its formation in 2021, the Subcommittee identified focus areas for further analysis. One focus area relates to the Bank Secrecy Act (BSA) information security and confidentiality risks that arise in third-party relationships. This white paper captures the Subcommittee’s analysis of this topic. It addresses these risks and has two primary objectives:

1. To communicate to financial institutions (FIs) subject to BSA requirements clear, consistent, cross-industry guidance/practices for information security and confidentiality when sharing BSA data with third parties. The white paper collects and summarizes existing rules and guidance that address third-party information sharing related to BSA data and provides citations to assist readers in gathering additional information.
2. To highlight for FinCEN various third-party relationship topics that it may wish to explore further, particularly as FinCEN considers establishing appropriate frameworks for information sharing among FIs, their agents, and service providers. As discussed further below, such topics may include:
 - a. Data Sharing with Specialized BSA Business Relationships. Business relationship partners may offer a broad range of BSA-related products and services, including so called “Financial Crimes Management” platform solutions. These comprehensive solutions may include transaction monitoring, customer due diligence, and other features in which an FI’s BSA data is stored with the vendor. FinCEN may want to establish appropriate frameworks for BSA data sharing with these specialized providers offering comprehensive Financial Crimes Management solutions, particularly those that offer cloud-based or other similar solutions in which BSA data, including Suspicious Activity Report (SAR) data, is stored on the business relationship partner’s platform.
 - b. Section 314(b) Information Sharing. Some vendors promote services in which they facilitate Section 314(b)-type information sharing between and among FIs that use a business relationship partner’s products and services. FinCEN may wish to address the parameters for such information sharing consistent with Section 314(b) rules and guidance.
 - c. Contract BSA Investigative Resources. FIs may contract with vendors to augment their BSA staffing. FinCEN may wish to consider providing guidance for information sharing and confidentiality for such contractors’ handling of BSA data,

particularly in circumstances where the contract personnel may be assigned tasks in the review of transaction monitoring alerts, unusual activity investigation, or even SAR preparation process.

- d. Third Party Data Security Protocols. FIs may rely on agents, including attorneys, consultants, and BSA subject matter experts, to assist with BSA compliance obligations, or in response to demands of regulators, or to implement BSA-related projects and initiatives. For example, FIs may engage outside law firms and consultants for a variety of reasons, including forensic accounting and similar reviews. These agents may be subject to BSA supervision, but not directly subject to BSA rules and may have varying degrees of sophistication in matters relating to BSA data security. Moreover, sharing information with agents which operate internationally, e.g., an international law firm, may raise special BSA data security concerns. FinCEN may wish to establish a framework for promoting secure BSA data sharing between FIs subject to the BSA and their outside agents.

In addition, FinCEN may consider creating a pilot program, as that term is defined in the AML Act, where the issues identified in this white paper, and other issues, can be explored. The results of the pilot program may help inform FinCEN's review of BSA regulations and guidance pursuant to Section 6216 of the AML Act as well as potential rulemakings and guidance.

II. Definitions

E. BSA Data

This white paper provides guidance/best practices regarding the sharing of "BSA data," a term that is not defined in statute or regulation. For purposes of this paper, the term "BSA data" refers to any data, including analyses and reports, created under the Anti-Money Laundering (AML) program, including data created pursuant to reporting or recordkeeping requirements of the BSA and its implementing regulations.

BSA data includes:

1. BSA Reports such as (a) Currency Transaction Reports (CTRs), (b) SARs and their supporting documentation, (c) monetary instrument logs, and (d) records relating to Customer Identification Program and Customer Due Diligence requirements;
2. any work papers or other information created in connection with BSA reports and recordkeeping requirements, such as automated transaction monitoring alerts;
3. audit findings, independent testing results, and management and board reports relating to BSA compliance. BSA data may include Personal Information (PI), as that term is defined by data privacy laws and regulations. BSA data generally does not include operational and transaction records prepared, received, and maintained by a financial institution (FI) such as SWIFT messages, funds transfers receipts, deposit items, or loan documents, unless

those documents: (1) are specifically required to be maintained under BSA recordkeeping requirements, such as records relating to certain international wire transfers; or (2) are deemed to be SAR supporting documentation and as such are considered to be a part of the SAR filing.¹

F. Third-Party Relationships

For the purposes of this white paper, third-party relationships are broken into three categories: business relationships, affiliate relationships, and agency relationships. The term “third party relationships” is an umbrella term meant to capture all three kinds of relationships unless stated otherwise.

1. Business Relationships

We use the term “business relationships” to refer to two different kinds of outside relationships. There are those outside relationships where an FI partners with a third party to advance shared business objectives (e.g., the relationship between a bank and a payment network such as VISA). And there are those relationships where the FI engages a third party to provide the FI with a product or service, e.g., the FI engages a consulting firm to provide it with consultative services.² For purposes of this paper we will use the term “business relationship” to refer to both types of outside relationships.

This treatment of the term “business relationships” is similar to how the Office of the Comptroller of the Currency (OCC) has defined a “business arrangement.” OCC Bulletin 2023-17 defines a third-party relationship as any “business arrangement” between the FI and another entity, by contract or otherwise.³ In this context, the term “business arrangement” is synonymous with the term third-party relationship.

2. Affiliate Relationships

An affiliate is an entity that controls, is controlled by, or is under common control with another entity. An affiliate⁴ relationship involves a relationship between (i) an FI and one of its domestic affiliates; (ii) an FI and one of its domestic affiliates within the FI’s “corporate organizational structure,” or (iii) between an FI and one of its foreign affiliates. The OCC’s and FinCEN’s SAR rules permit the sharing of SARs within an FI’s domestic corporate organizational structure. FinCEN has defined the term “corporate organizational structure” in the context of SAR sharing

¹ BSA data also does not include confidential supervisory information or information provided to an FI pursuant to the reporting provisions of Section 6201 of the AML Act.

² Service providers for banks and savings associations are typically subject to examination and enforcement by the FDIC, OCC, and FRB under the Bank Service Company Act, 12 U.S.C. 1864 *et seq.* In addition, NCUA and state supervisory authorities, as applicable, have access to the books and records of credit union service organizations, and the ability to review their internal controls under 12 CFR 712.3(d).

³ OCC Bulletin 2023-17: <https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf>; *see also* Final Interagency Guidance on Third Party Relationships: Risk Management, 88 FR 12340 (June 9, 2023) (defining the term “business arrangement” in terms similar to the OCC Bulletin).

⁴ For an example, see OCC’s definition: <https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/related-organizations/pub-ch-related-organizations.pdf>

to include only domestic affiliates that are subject to a SAR rule. SARs cannot be shared with foreign affiliates; however, under the AML Act, FinCEN has proposed a rulemaking to create a pilot program that would permit the sharing of SARs with foreign affiliates.⁵

3. Agency Relationships

In general, the term “agency relationship”⁶ refers to a business relationship of two parties in which one represents the other in transactions with third parties. The agent acts on behalf of the party at risk, who is known as the “principal.” An agency relationship is usually set out in contractual agreements. Under agency laws, the agent is empowered to act on behalf of the principal (as set forth in the contract) and the principal is bound by, and directly responsible for, the activities of its agent.

The BSA regulations define the term “financial institution” to include the FI’s “agent.”⁷ Thus, for BSA purposes, an agent, *e.g.*, an outside law firm engaged by the FI to represent it in connection with a BSA matter, is treated as though it is part of the financial institution. Nonetheless, and as discussed further below, the sharing of BSA data with an FI’s agent can create third-party type risks of a kind similar to those that exist in business relationships.

III. Legal and Regulatory Framework

Section 6101 of the AML Act provides, *inter alia*, that the duty to establish, maintain, and enforce an AML/Combating the Financing of Terrorism (CFT) Program shall be the responsibility of, and shall be performed by, persons in the United States who are subject to regulatory oversight and supervision. While placing AML/CFT Program responsibility on the FI, the AML Act nonetheless contemplates the need for an FI to share information. In particular, the AML Act expands the purposes of the BSA to include establishing appropriate frameworks for information sharing with third parties such as agents and service providers.

To date, the Federal Functional Regulators⁸ (FFRs) and FinCEN have not issued comprehensive rules or guidance relating to sharing BSA data with third parties, but they have addressed information sharing as it relates to selected kinds of BSA data. Specifically, they have addressed through regulation and/or guidance a range of topics that touch on third-party risks, including those relating to BSA data.⁹

⁵ 87 Fed. Reg. 3719 (January 25, 2022).

⁶ See the Restatement (Third) of Agency.

⁷ See 31 CFR 1010.100(t).

⁸ The Federal Functional Regulators are the Board of Governors of the Federal Reserve System (FRB), the Board of Directors of the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of Comptroller of the Currency (OCC), the Securities Exchange Commission, and the Commodity Futures Trading Commission. See 31 CFR 1010.100(r).

⁹ For example, the OCC, FRB, and FDIC recently issued joint guidance on third party risk management. See, *e.g.*, *Interagency Guidance on Third Party Relationships: Risk Management (June 9, 2023) FRB (SR 23-4)*, *FDIC (FIL-29-2023)*, *OCC (OCC Bulletin 2023-17)*. And, in 2021, the FBB published a *Guide to Community Banks on Conducting Due Diligence on Financial Technology Companies*.

A. Suspicious Activity Report Confidentiality and Sharing

1. SAR Sharing with Affiliates Located in the U.S.

A SAR, and information that would reveal the existence (or non-existence) of a SAR, are confidential and may not be disclosed.¹⁰ There are limited exceptions in the FinCEN regulations that permit the sharing of a SAR or SAR information, including sharing within an FI's corporate organizational structure for purposes consistent with Title II of the BSA, as determined by regulation or in guidance.¹¹ The OCC and FinCEN SAR rules and the 2012 FinCEN guidance permit the sharing of SARs with agents, including attorneys representing FIs. FinCEN has cautioned FIs to ensure that such agents are aware of the SAR confidentiality requirements.¹² This guidance is helpful but does not explicitly provide a framework for secure BSA data information sharing with such agents or identify the types of individuals or entities that may qualify as agents.

FinCEN and some of the FFRs have addressed the subject of SAR sharing with affiliates and parents of FIs through guidance statements. In 2006, the FinCEN, Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and OCC issued *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* ("2006 Guidance").¹³ The 2006 Guidance clarified that a U.S. branch of a foreign bank may share a SAR with its head office, and a U.S. bank or savings association may share a SAR with its controlling company, no matter where the entity or party is located. Such sharing is permitted because the bank's head office or controlling entity may have a need to discharge oversight responsibilities with respect to enterprise-wide risk management and compliance with applicable laws and regulations.¹⁴

In 2010, FinCEN amended SAR confidentiality rules to permit the sharing of SARs and SAR information within the corporate organizational structure for purposes consistent with Title II of the BSA as determined by regulation or guidance,¹⁵ and issued guidance on *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates* ("2010 Guidance"). The 2010 Guidance addresses sharing SARs, and SAR information, within a corporate organization that FinCEN considers to be "consistent with the purposes of the BSA."¹⁶ This guidance generally permits the sharing of SARs and SAR information by depository institutions with their affiliates that are subject to a SAR regulation. U.S. affiliates of depository institutions and mutual funds that are subject to SAR filing obligations include broker-dealers, future commission merchants

¹⁰ See 31 U.S.C. §5317(g)(2); 31 CFR 1020.320(e); 12 CFR 748(c)(5) (NCUA); 12 CFR 21.11(k) (OCC); 12 CFR 353.3(g) (FDIC); 12 CFR 208.62(j) (FRB).

¹¹ See 31 CFR 1020.320(e)(1)(ii)(A)(2) and (B); see also *Sharing Suspicious Activity Reports By Depository Institutions with Certain U.S. Affiliates*, FIN-2010-G006 (November 23, 2010).

¹² See SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions; FIN-2002-A002 (March 2, 20012).

¹³ *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* (Jan. 20, 2006); FRB (SR 06-1), FDIC (FIL-5-2006), OCC (Bulletin 2006-04) and *Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities* (January 2006).

¹⁴ See 31 CFR 1020.320(e)(1)(ii)(A)(2) and (B).

¹⁵ 75 F.R. 75593 (Dec. 3, 2010).

¹⁶ *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates*, FIN-2010-G006, Nov. 23, 2010.

(FCMs), money services businesses (MSBs), and residential mortgage lenders or originators.¹⁷ Sharing SARs with affiliates outside the United States is not permitted because these foreign affiliates are not subject to U.S. SAR regulations.

There may be circumstances where an FI, a branch, or a bank affiliate would be liable for direct or indirect disclosure of a SAR or SAR information by the affiliate. To protect the confidentiality of SARs, both the 2006 Guidance and the 2010 Guidance provide that the bank or branch, as part of its AML program, must have appropriate controls to protect the confidentiality of SARs.

2. SAR Sharing with Business Relationship Partners

a. Business Relationship Partners in the United States

Staffing. The FFRs and FinCEN have not comprehensively addressed the extent to which an FI can share information subject to the SAR Rule with business relationship partners, such as contractors, located in the U.S. For example, BSA-regulated FIs may engage contract resources to perform services related to financial crimes compliance, such as to address staffing challenges. These resources may be used to review automated transaction monitoring alerts, conduct case investigations, and perhaps even draft SARs for evaluation by the FI, under the supervision of the FI. Yet it is not entirely clear to what extent an FI may use contract resources to perform these functions consistent with SAR confidentiality rules and guidance.

Technology Solutions. The FFRs and FinCEN also have not addressed the question of whether information subject to SAR confidentiality rules may be shared with business relationship partners who provide transaction monitoring and other financial crimes management solutions located within the U.S. This question is particularly pertinent in situations where the business relationship partner is granted access to an FI's BSA data and/or provides a "cloud-based" automated transaction monitoring solution in which BSA-related data, including potential information that could disclose the existence of a SAR, is housed on the vendor's servers. Given FI operating models and technological advances, addressing these questions is important for effective and efficient financial crimes compliance in the modern era.

SAR-related data may be deemed more sensitive if the data discloses the SAR itself or any information that would reveal the existence of a SAR to the third-party business. At the outset, as set forth in the regulation, SARs and SAR information can only be shared within an FI's corporate organizational structure. As a result, outsourcing arrangements with unaffiliated third-party businesses involving SARs typically relate to services that precede the ultimate SAR determination and filing, e.g., the review of automated transaction alerts and case investigation.¹⁸ The ultimate decision to file SARs based upon alerts and case investigation must be retained by the FI and the SAR filing must generally take place within the FI.

Notwithstanding these requirements, the assessment and classification of the BSA data contained in shared alert information and any shared SARs is important. An FI must have a clear

¹⁷ See 31 CFR 1023.320 (broker-dealers); 31 CFR 1026.320 (FCMs); 31 CFR 1022.320 (MSBs); 31 CFR 1029.320 (loan or finance companies).

¹⁸ See https://www.fincen.gov/sites/default/files/shared/guidance_faqs_sar_10042006.pdf.

understanding of what data it needs to share, as opposed to what data the third-party business is requesting to access, or house. The size, complexity, and status (public or private company) of the third-party business handling BSA data could influence the risk and impact of a breach.

If an FI contracts with a third party (e.g., a consultant, contractor, vendor, etc.) to conduct any customer transactions, the FI is still responsible for those transactions. Transactions conducted by a third party on behalf of the FI are considered to have been conducted by, through or to the FI. The FI remains responsible for monitoring transactions for and filing SARs and CTRs, maintaining BSA records, and complying with ID requirements. If the third party is also an FI, that FI may also have a requirement to monitor transactions for and file a SAR and CTRs, maintain BSA records and comply with ID requirements.

b. Business Relationship Partners Outside the United States

These questions take on an added layer of complexity when the business relationship partner accesses or houses data subject to the SAR confidentiality rules from a place outside of the United States. The SAR Confidentiality Rule and regulatory guidance do not expressly prohibit, nor expressly permit, overseas outsourcing of activities involving access to SAR-related information. In issuing the SAR Confidentiality Rule, FinCEN refused to take a position on overseas outsourcing of SAR-related functions, stating it was “intentionally silent” on the issue, that it “has been studying the issue while considering additional future guidance” on outsourcing, and that the “final rulemaking takes no position on the matter.¹⁹” Notwithstanding, FinCEN prohibits FIs from sharing SARs even with their own foreign branches for risk management purposes. There are two areas in which there is some recognition that outsourcing arrangements with SAR access may currently exist. The first is in the mutual fund context. Specifically, in the preamble to FinCEN’s SAR Confidentiality Rule, FinCEN reiterates that the Rule is not intended to supersede previous guidance for mutual funds, which clarifies that mutual funds can contractually delegate SAR functions to transfer agents. The second area is in a general paper on outsourcing by the FRB. In this, the FRB warns of the complexities associated with outsourcing confidential SAR-related functions generally. However, it has been interpreted²⁰ that this type of outsourcing, as in the context of mutual funds, was done so domestically.

3. SAR Sharing with Agents

The term “financial institution” as used in the BSA’s implementing regulations includes an FI’s agent.²¹ It is incumbent on FIs that their agents understand the SAR confidentiality rules and establish appropriate levels of data security. For example, an attorney representing a bank in a BSA regulatory or enforcement matter may share SAR-related information with an expert witness or a consultant without considering SAR confidentiality rules or guarding the information under the same data security standards applied by its principal. These considerations suggest that banks should closely monitor the BSA data they provide to their agents, particularly SAR-related information.

¹⁹ 75 FR 75,793, 75,601 (Dec. 3, 2010).

²⁰ FinCEN Final Rule, *supra* note 4, at 75601, 75607. *See also* FinCEN, “Frequently Asked Questions Suspicious Activity Reporting Requirements for Mutual Funds,” (Oct. 4, 2006).

²¹ 31 C.F.R. 1010.100(d).

B. Sharing Information Under Section 314 of the USA PATRIOT Act

The topic of information sharing arises under Section 314 of Title III of the USA PATRIOT Act. Section 314(a) and its implementing regulations enable law enforcement agencies to “ping” more than 14,000 FIs to locate accounts and transactions of persons who may be involved in terrorism or money laundering. FinCEN acts as a gatekeeper, sending notifications to its designated contacts within FIs at least once every two weeks. The FIs then query their records for data matches and if a match exists, the FI replies to the notification.²² Both the fact of the Section 314(a) notification and any response may be used only for limited purposes. The regulations implementing Section 314(a) provide that an FI shall not disclose the fact that FinCEN has requested or has obtained information under this section, except to the extent necessary to comply with such an information request.²³ Thus, “section 314(a) subject lists cannot be shared with any foreign office, branch, or affiliate (unless the request specifically states otherwise), and the lists cannot be shared with affiliates, or subsidiaries of bank holding companies, if the affiliate or subsidiaries are not FIs as described in 31 U.S.C. 5312(a)(2).”²⁴ Section 314(a) information may, however, be shared with third-party service providers. “For the purposes of assisting a financial institution in complying with [a Section 314(a)] request, a financial institution may provide a list of named subjects to a third-party service provider or vendor so long as the institution takes those steps necessary to ensure that the third party safeguards the information.”²⁵

Section 314(b) permits FIs and associations of FIs, under the protection of a statutory safe harbor from liability, to share information with any other FI or association of FIs for purposes of identifying and reporting activities that the FI or association suspects may involve possible terrorist activity or money laundering.²⁶ FinCEN guidance permits information sharing under the Section 314(b) safe harbor even if an FI or association does not have specific information indicating that the activity is suspicious and has not conclusively determined whether to file a SAR. “Instead, it is sufficient that the FI or association has a reasonable basis to believe that the information shared relates to activities that may involve money laundering or terrorist activity” and it is sharing information for an appropriate purpose.²⁷ The regulations implementing Section 314(b) also provide that each FI that engages in the sharing of information shall maintain adequate procedures to protect the security and confidentiality of such information which shall be deemed satisfied to the extent the FI applies information procedures consistent with what the institution has established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801, *et seq.*) (GLBA), and applicable regulations issued thereunder, regarding the protection of its customers’ non-public PI. In this regard, each of the FFRs has issued regulations that address the information security requirements of the GLBA.²⁸

²² See generally FinCEN 314(a) Fact Sheet (June 14, 2022). As of June 14, 2022, FinCEN has processed 744 Section 314(a) requests relating to terrorism and 4,916 requests relating to money laundering.

²³ See 31 CFR 1010.520(b)(3)(iv)(B)(1).

²⁴ See FinCEN, *FAQs Concerning the 314(a) Process*, FAQs 31 & 32 (issued April 6, 2018).

²⁵ See FinCEN, *FAQs Concerning the 314(a) Process*, FAQ 28 (issued April 6, 2018).

²⁶ 31 CFR 1010.540(b).

²⁷ Section 314(b) Fact Sheet (December 2020).

²⁸ 15 U.S.C. §§ 6801(b), 6805(b)(2): <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314>; see also the Federal Trade Commission’s Standards for Safeguarding Customer Information.

Information sharing under Section 314(b) is generally limited to FIs subject to BSA requirements, but with an important qualification. Associations consisting exclusively of BSA-regulated FIs may share information under the Section 314(b) safe harbor. This is true even if the association is not itself subject to the BSA, and even if the association exists only as a contractual arrangement among FIs subject to the BSA. The breadth of Section 314(b) information sharing facilitated through “associations” has not been fully explored. One topic that FinCEN may choose to address through rule-making or further guidance is the extent to which vendors who contractually provide automated transaction monitoring and other financial crimes management solutions exclusively to BSA-regulated FIs can perform an association-like Section 314(b) information sharing function.²⁹

C. Sharing of BSA Resources

In 2018, some of the FFRs and FinCEN issued the *Interagency Statement on Sharing Bank Secrecy Act Resources*.³⁰ The 2018 Interagency Statement addressed instances when banks and credit unions may decide to enter a collaborative arrangement to share resources to manage their BSA/AML obligations more efficiently and collaboratively. Though not addressed specifically to BSA data, the 2018 Interagency Statement nonetheless highlighted data security risks that could arise in these collaborative arrangements. Specifically, it compared the collaborative arrangements to others involving third parties, noting that a “collaborative arrangement should be appropriately documented to define the nature and type of resources to be shared, define each institution’s rights and responsibilities, establish procedures for protecting customer data and confidential information, and develop a framework to manage risks associated with the sharing of resources.”

D. The AML Act

The AML Act contains certain provisions relating to information sharing with third party businesses. Section 6303 requires each FFR to appoint a BSA Information Security Officer that will be consulted on information sharing policies under the BSA, including those that allow FIs to share information with each other and with foreign affiliates, and those that allow Federal agencies to share with regulated entities.

Section 6212 of the AML Act adds to the BSA a new subsection that requires the Department of the Treasury (Treasury) to issue rules establishing a pilot program for FIs to share information related to BSA reports with their foreign branches, subsidiaries, and affiliates. The AML Act sets a new foundation for cross-border information sharing relating to SARs. Section 6212(a) of the AML Act directs Treasury to establish a three-year pilot program that allows FIs to share information related to SARs, including that a SAR has been filed, with foreign branches, subsidiaries, and affiliates. Such sharing must be subject to appropriate data security requirements related to PI. The pilot may not be extended to branches, subsidiaries and affiliates in Russia or China, or in jurisdictions that are state sponsors of terrorism, subject to sanctions, or that Treasury has determined cannot reasonably protect the information. As part of the pilot, Treasury must have

²⁹ For example, one BSA/AML service provider promotes on its website a “centralized platform for information sharing that allows investigators at 314(b)-registered financial institutions to easily send, receive, and respond to requests for information directly in our secure environment, expediting decision making in the investigation process.”

³⁰ *Interagency Statement on Sharing Bank Secrecy Act Resources* (issued October 3, 2018).

the means to hold a foreign affiliate liable for the unauthorized disclosure of SAR information. Importantly, FIs participating in the pilot program may not offshore BSA compliance functions. “No FI may establish or maintain any operation located outside of the United States the primary purpose of which is to ensure compliance with the Bank Secrecy Act as a result of the sharing granted under this subsection.”³¹ Section 6212 of the AML Act does not address cross-border sharing of SAR-related information with other categories of offshore persons and entities, e.g., third-party service providers. Nonetheless, the explicit and carefully defined parameters set forth in Section 6212 may be read to limit the sharing of SAR-related information only to eligible branches, subsidiaries, and affiliates.

The AML Act also addresses new frameworks for information sharing. It does so by expanding the purpose of the BSA to include establishing appropriate frameworks for information sharing among FIs, their agents and service providers, their regulatory authorities, associations of FIs, the Treasury, and law enforcement authorities to identify information, stop, and apprehend money launders and those who finance terrorists, expanding upon section 5311, part 5, of the BSA. This statutory provision provides an opportunity for FinCEN to provide additional guidance on sharing BSA data with third-party service providers. For example, FinCEN could establish a pilot program for this type of data sharing, including with third parties.

E. Other Requirements

1. General Third-Party Risk Management Guidance

Controlling for these unique BSA risks may require enhanced processes for managing business relationships in which BSA data is shared. In addition to OCC Bulletin 2023-17 and the accompanying FAQs, several of the FFRs have issued guidance addressing third-party relationships. Further, in June 2023, the FRB, OCC, and FDIC issued Interagency Guidance on Third Party Relationships: Risks Management.³² The final Interagency Guidance specifically highlights that a third party may perform activities subject to applicable laws and regulations. The final Interagency Guidance highlights the need for relevant contracts to ensure compliance with laws and regulations and considers relevant guidance and self-regulatory standards. FIs subject to the Interagency Guidance should also assess the third party’s ability to comply with rules and regulations, including BSA regulations.

2. Guidance on FinTech Business Relationships

In the banking sector, the FRB, OCC, and FDIC released joint guidance³³ in 2021 to help FIs that partner with FinTech companies. FIs are entering into business arrangements with FinTech

³¹ 31 U.S.C. § 5318(g)(10).

³² *Final Interagency Guidance on Third Party Relationships: Risk Management*, Federal Register Doc. 2023-12340 (June 9, 2023); see also SR Letter 13-19/CA Letter 13-21, *Guidance on Managing Outsourcing Risk*, (December 2013, updated February 26, 2021); OCC Bulletin 2013-29, *Third-Party Relationships: Risk Management Guidance* (October 30, 2013); FDIC, FIL-44-2008, *Third-Party Risk: Guidance for Managing Third-Party Risk* (June 8, 2008); NCUA Supervisory Letter 07-01 (October 2007).

³³ *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks* (Aug. 2021): <https://www.federalreserve.gov/publications/files/conducting-due-diligence-on-financial-technology-firms-202108.pdf>

companies to offer enhanced products and services to their customers, increase efficiency, and reduce internal costs. The joint guidance covers six key areas of due diligence that community banks can consider when exploring arrangements with FinTech companies: business experience and qualifications, financial condition, legal and regulatory compliance, risk management and control processes, information security, and operational resilience.³⁴ The guidance also reminds banks that partnerships do not diminish a bank's responsibility to comply with "federal consumer protection laws and regulations, just as if the bank were to perform the service or activity itself." FIs exploring business relationships with a FinTech company should carefully examine the company's qualifications, compliance systems, and information security practices.

3. Gramm-Leach-Bliley Act Information Security Requirements

Section 501 of the GLBA requires certain federal and state regulators to establish appropriate standards for the FIs subject to their oversight relating to administrative, technical, and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

On February 1, 2001, several FFRs published the Interagency Guidelines Establishing Information Security Standards that require banks to implement a comprehensive written information security program to manage and control these risks.³⁵ As it concerns service providers, the Interagency Guidelines direct every bank to:

1. Exercise appropriate due diligence in selecting its service providers;
2. Implement appropriate measures via contracting to meet the objectives of these Guidelines; and
3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required.

The GLBA Safeguards Rule³⁶ issued by the Federal Trade Commission (FTC) and certain state laws and regulations³⁷ also contain these requirements.

Accordingly, banks should review audits, summaries of test results, or other equivalent evaluations of their service providers. Under these requirements, an FI that enters third-party relationships with

³⁴ Though targeted to community banks, the guidance emphasizes that the fundamental concepts may be useful for banks of varying size and for other types of third-party relationships.

³⁵ FRB Appendix F to 12 CFR Part 225; FDIC Appendix B to 12 CFR Part 364; NCUA 12 CFR Part 748, Appendices A and B; OCC Appendix B to 12 CFR Part 30.

³⁶ FTC Safeguards Rule (GLBA), 16 C.F.R. Part 314.4(f)d. ("Each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers."). *Id.* "Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; (2) Requiring your service providers by contract to implement and maintain such safeguards; and (3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards."

³⁷ See, e.g., NY Department of Financial Services Cybersecurity Regulation, 23 CRR-NY 500.11(a) ("Third-Party Service Provider Policy").

vendors who access or house BSA data must be mindful of audit rights, breach notification, data security, and other contracting considerations.

4. Other BSA and Privacy Considerations

In addition to limitations that may exist under U.S. law on SAR sharing within corporate organizational structures (see Section III.A. above), global FIs should be aware of potential sharing limitations that may arise under foreign laws. These limitations may mirror U.S. law limitations but may nonetheless permit sharing of aggregate SAR information, e.g., volumes and frequencies, money laundering typologies, risk scoring metrics, etc. In this scenario, FIs should conduct their aggregate data collection such that the identity of a person(s) subject to a SAR cannot be reverse engineered with the aid of publicly available information sources.³⁸

Furthermore, FIs should consider local and regional data privacy and protection laws and regulations and establish adequate data privacy and protection controls. Examples of controls, as required by the European Union's General Data Protection Regulation (GDPR), include but are not limited to, inter-affiliate data processing and transfer agreements, standard contractual clauses, notice and consent, record of processing activities, and the appointment of data privacy officers to oversee data subject access rights and privacy impact assessments.

Consistent with sound vendor management practices, FIs should carefully manage the contract termination phase of third-party relationships, particularly those that may affect the disposition of BSA data. For example, BSA data housed with a third party that is subject to BSA record retention requirements needs to be brought within the FI's control prior to contract termination. In other instances, the FI may have relied on unique third-party data analytics to produce customer risk profiles. The FI needs to evaluate if it can retrieve the customer risk profile information prior to termination, and if not, how it intends to create substitutes for the customer risk profile information it may no longer be able to access or maintain.

5. Securities and Derivatives Requirements

In the securities sector, the Financial Industry Regulatory Authority (FINRA) published a Notice reminding member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures, for any activities or functions performed by third-party vendors, including any sub-vendors.³⁹ The FINRA Notice contains third-party vendor management guidance that may be useful not just to FINRA member firms, but also to FIs generally. In its annual Examination Findings report, FINRA also observed that firms are relying on third-party vendors' tools without performing adequate due diligence or understanding how the vendor-supplied controls operate. In one example provided by FINRA a third-party vendor did not configure its cloud-based server correctly, install antivirus software, or implement encryption for the firm's account applications and other brokerage records containing customers' PI. As a result, foreign hackers successfully accessed the cloud-based server and exposed firm customers' PI.

³⁸ Examples include corporate registers, news media, or other.

³⁹ See FINRA Notice 21-29, FINRA Reminds Firms of Their Supervisory Obligations Related to Outsourcing to Third-Party Vendors (2021).

In the derivatives sector, the National Futures Association (NFA) has issued an Interpretive Notice that provides guidance for its members (Commodity Futures Trading Commission (CFTC) registrants) when they outsource NFA and CFTC regulatory requirements to third-party service providers or vendors. The Notice provides that members must have a written supervisory framework that includes: (1) an initial risk assessment to determine if outsourcing a particular regulatory function is appropriate and to identify any associated risks; (2) onboarding due diligence to ensure the service provider is able to successfully carry out the outsourced function(s); (3) ongoing monitoring to ensure the third party can continue to carry out the outsourced function(s); (4) termination provisions to ensure the member is provided sufficient notice of any termination of outsourcing; and (5) recordkeeping provisions to ensure that if a member outsources a required function to a third-party service provider, the member maintains records to demonstrate it has addressed the four areas listed above. The Notice also reminds members that outsourcing does not relieve them of their obligation to comply with applicable NFA and/or CFTC regulatory requirements.

6. Casinos – Special Requirements

For casinos, unlike other FIs, the applicable BSA obligations attach only to the casino licensee. Thus, if the licensee is a subsidiary of another legal entity, the parent entity is simply a related non-financial trade or business and not an FI. FinCEN's Casino SAR Sharing Guidance⁴⁰ notes that casinos may share SAR data with their U.S. parent or affiliate consistent with FinCEN's amendments to the confidentiality provisions of its SAR regulations in 2010. The 2017 guidance states in a footnote, "An 'affiliate' is a financial institution that is required under rules implementing the BSA to report suspicious transactions and that is controlled by, or is under common control with, the casino filing the SAR."⁴¹

IV. Guidance / Best Practices Useful to BSA Regulated FIs

A key objective of the BSAAG subcommittee on Information Security and Confidentiality is to advise on confidentiality implications raised by BSA laws and implementing regulations. The sharing of BSA data with third parties carries elevated risks, beyond data privacy and security risks related to all third-party relationships. Most BSA data, by definition, is highly confidential and sensitive. Its wrongful disclosure carries at least two unique risks. First, it can undermine criminal money laundering and terrorist financing investigations and prosecutions. Second, it can reveal information about an FI's internal BSA controls and processes in ways that make them less effective, thus compromising an FI's efforts to maintain an effective BSA/AML program.

Another unique risk arises from outsourcing certain BSA-related functions to a business relationship partner or agent. An FI subject to BSA regulation can run afoul of the law and prudent practice by over delegating BSA-related functions to a business-relationship partner or agent without sufficient supervision, training, and oversight.

⁴⁰ FinCEN, *Sharing Suspicious Activity Reports with U.S. Parents and Affiliates of Casinos*, FIN-2017-G001 (Jan. 4, 2017): <https://www.fincen.gov/resources/statutes-regulations/guidance/sharing-suspicious-activity-reports-us-parents-and>

⁴¹ *Id.* note 3.

Information sharing plays a vital role in allowing FIs, law enforcement, and FFRs to better deploy resources using a risk-based approach to combat money laundering/terrorist financing. However, there remain obstacles to effective information sharing that can obstruct this progress and create legal and regulatory uncertainty.

Based on these risks, FIs sharing data with business relationship partners and agents should consider the following when sharing BSA data:

1. FIs should take adequate steps to ensure that all documentation, including copies of identification data, are received or available to them without delay from the business relationship partner or agent. FIs should ensure that contractual agreements set forth requirements for identification data, including the relevant time frames for receiving data. They should also be satisfied that the business relationship partner or agent is regulated, supervised, or monitored appropriately and has measures in place for due diligence and record-keeping compliance.
2. FIs should assess the business relationship partner or agent's ability to protect sensitive firm and customer PI, have controls in place to mitigate potential conflicts of interest in the outsourcing selection process, and assess the extent of potential damage if there is a security breach (e.g., number of customers or prospective customers impacted). FIs should consider the reputation and history of the business relationship partner or agent, including the representations made and information shared regarding how the vendor will secure the firm's information.
3. An FI's auditors, whether internal or external, should review services being outsourced or business provided, and the systems utilized, as appropriate, and provide comprehensive reports and workpapers that can be reviewed by the FI and its regulators. Depending on the affiliated business relationship, the FI should have sufficient authority and the ability to effectively train, manage, designate, or assign responsibilities to affiliated employees working on behalf of the FI, including shared or dual-status employees.⁴² Depending on the business arrangements and whether the FI has BSA responsibilities, effective controls should be in place to ensure that the FI has access to all data and recordkeeping, that the integrity of the data is protected,⁴³ and the FI is promptly informed if there is a SAR disclosure or a breach or compromise of its customer information and data. When an arrangement involves a foreign jurisdiction, the FI should have a thorough understanding of the legal framework of the applicable jurisdiction, including any limitations on the flow of information that may impact its ability to appropriately maintain the confidentiality of a SAR or SAR information, manage and conduct oversight activities, or otherwise limit the ability of the FFRs to supervise or examine the FI's activities. The FI should be able to promptly produce records in a timely manner upon request by the FFRs, consistent with U.S. law.

⁴² Shared or dual-status employees are: (i) employees of the FI that are also employees or agents of the service provider, head office or controlling shareholder or (ii) employees of the service provider, head office or controlling shareholder that are also employees or agents of the FI. *See e.g.*, 12 C.F.R. 7.3001 (OCC).

⁴³ For example, there can be no data or wire transfer "stripping" for SAR monitoring, OFAC compliance or other purposes.

V. Recommendations / Observations / Suggested Actions

This white paper has highlighted topics where FinCEN may through rulemaking or guidance provide greater clarity to BSA-regulated FIs regarding data security and confidentiality in third-party relationships. In the Introduction, we highlighted four specific topics for FinCEN to consider as it evaluates establishing appropriate frameworks for secure BSA data sharing with vendors and other third parties.

A. Data Sharing with Specialized BSA Business Relationship Partners

Business relationship partners may offer a broad range of BSA-related products and services, including so called “Financial Crimes Management” platform solutions in which the vendor promotes comprehensive transaction monitoring, customer due diligence, and other solutions where BSA data is stored on the vendor’s platform. BSA data security controls may need to be tailored depending on the sensitivity of the information stored on these platforms. FinCEN may want to establish appropriate frameworks for BSA data sharing between the FI and these business relationship partners, particularly those that offer cloud-based or other similar solutions in which BSA data, including SAR data, may be stored or accessed on the business relationship partner’s systems or platforms.

B. Third-Party Data Security Protocols

FIs may rely on outside agents, including attorneys, to assist them in discharging their obligations under the BSA. While potentially subject to BSA rules, these agents may have varying degrees of sophistication in matters relating to BSA data security. Moreover, some of these agents may be international partnerships or companies, raising special concerns when sharing information with them that could reveal the existence or non-existence of a SAR. FinCEN may wish to establish a framework for promoting secure BSA data sharing between FIs subject to the BSA and their agents.

C. Contract BSA Investigative Resources

FIs may enter into contracts with vendors to augment their BSA staffing, particularly in circumstances where the FI may face a transaction monitoring alert or investigative backlog or be conducting a “look-back.” FinCEN may wish to consider providing guidance for information sharing and confidentiality for such contractors’ handling of BSA data, particularly in circumstances where the contract personnel may be assigned tasks in the case alert review, investigation, or even SAR preparation process.

D. Section 314(b) Information Sharing

Some vendors promote services in which they facilitate Section 314(b)-type information sharing between and among FIs that use their products and services. FinCEN may wish to address the parameters for such information sharing consistent with Section 314(b) rules and guidance.

As FinCEN works to develop appropriate frameworks for information sharing, it could consider initiating a pilot program. Such an approach might allow FinCEN to gather information and test assumptions and understanding before engaging in any rulemaking.

From: [REDACTED]@fincen.gov]
Sent: 5/5/2021 5:30:59 PM
To: [REDACTED]@bofa.com]
Subject: RE: 314(b) related escalation

[REDACTED] that's obviously troubling. I will escalate this immediately and revert once we have a path for further discussion.

Regards,
[REDACTED]

[REDACTED]
Director, Office of Stakeholder Integration and Engagement
Strategic Operations Division
Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury
[REDACTED] (mobile)

From: [REDACTED]@bofa.com>
Sent: Wednesday, May 5, 2021 1:09 PM
To: [REDACTED]@fincen.gov>
Subject: [EXTERNAL] 314(b) related escalation

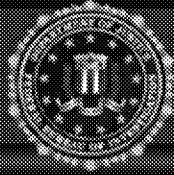
[REDACTED] – I have a 314(b) registration issue that I want to discuss with someone of appropriate seniority within FinCEN to make sure you are aware. It appears someone with no connection to Bank of America was able to register with FinCEN as Bank of America's 314(b) contact. I'd be happy to pull up with you to share what we know or if you want to direct me somewhere else that would be fine too.

Thanks,
[REDACTED]

[REDACTED]

This message, and any attachments, is for the intended recipient(s) only, may contain information that is privileged, confidential and/or proprietary and subject to important terms and conditions available at <https://hyperlink.services.treasury.gov/agency.fincen?origin=http://www.bankofamerica.com/emaildisclaimer>. If you are not the intended recipient, please delete this message.

UNCLASSIFIED//FOUO



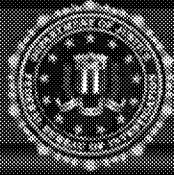
**Federal Bureau of Investigation
Charlotte Division
Joint Terrorism Task Force**

International Terrorism

**Special Agent [REDACTED]
Terrorism Financing Coordinator, FBI Charlotte Division**

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



How the FBI Categorizes Terrorist Actors



International Terrorism

International terrorists include members of designated Foreign Terrorist Organizations (FTOs), state sponsors of terrorism, and Homegrown Violent Extremists (HVEs)

Domestic Terrorism

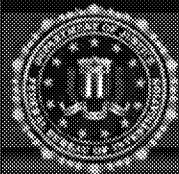
Domestic extremists are U.S. persons who commit criminal acts based on their political or social ideology rather than for monetary or personal gain (e.g., Sovereign Citizen Extremists)

~5,000
CT investigations

~1,000 each
HVE | ISIS | DT

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO







Homegrown Violent Extremists



There is no **useful demographic of HVEs.**

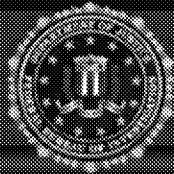
We have seen individuals of both genders, of many different ages and ethnicities, and with varying levels of education and occupations.

What Makes Someone an HVE?

 Inspired by the global jihad	 Based in the United States
 Radicalized in the United States	 No individualized direction from terrorist group

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



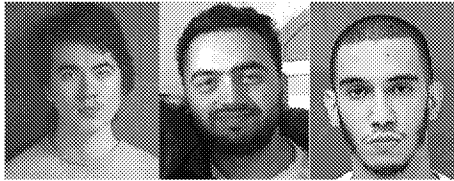
International Terrorism



U.S. Terrorism-Related Cases by Year

Cases include individuals who are charged with or died engaging in jihadist terrorism or related activities inside the United States, and Americans accused of such activity abroad. Years indicate the year that individuals were charged or, if they were not charged, the year that they died.

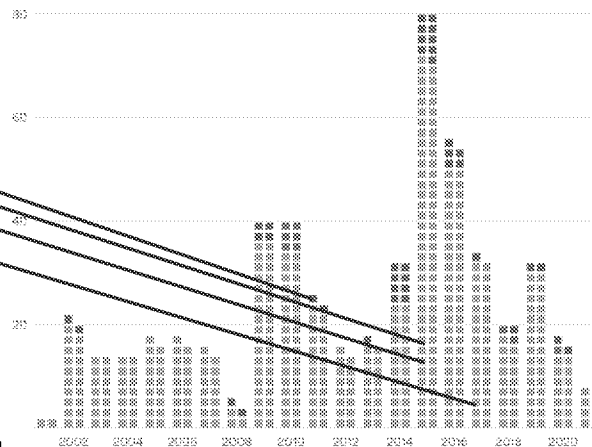
Hover over a square for more detail on an individual case.



471	9	39
Charged	Charged outside U.S.	Deceased

Western District of NC Cases:

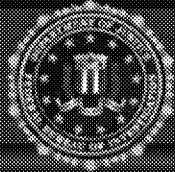
- Samir Khan, Killed 9/2011
- Justin Sullivan, 6/2015 arrest
- Saeed Kodaimati, 4/2015 arrest
- Alex Smith, 6/2017 arrest



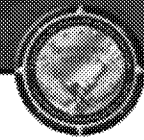
UNCLASSIFIED//FOUO

Source: newamerica.org, 4/1/2019

UNCLASSIFIED//FOUO



...but you can't always trust the numbers



2:1

Immigration
Charges

Tax Fraud
Charges



UNCLASSIFIED//FOUO

Financial Crimes

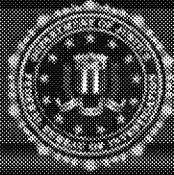
Conspiracy

Firearms
Charges

Unlicensed
Money Service
Business
Charges

Crimes
Against
Children

UNCLASSIFIED//FOUO

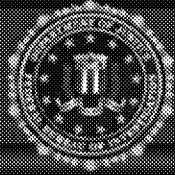


Publicity & Propaganda; Radicalizing & Recruiting

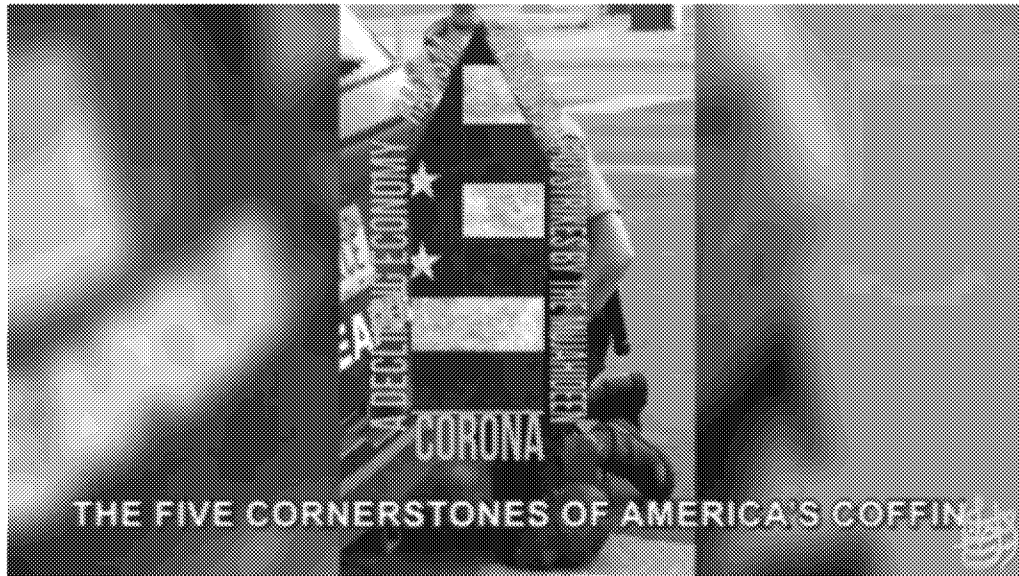
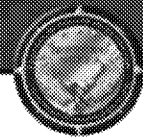


UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

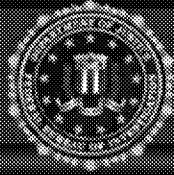


Publicity & Propaganda; Radicalizing & Recruiting

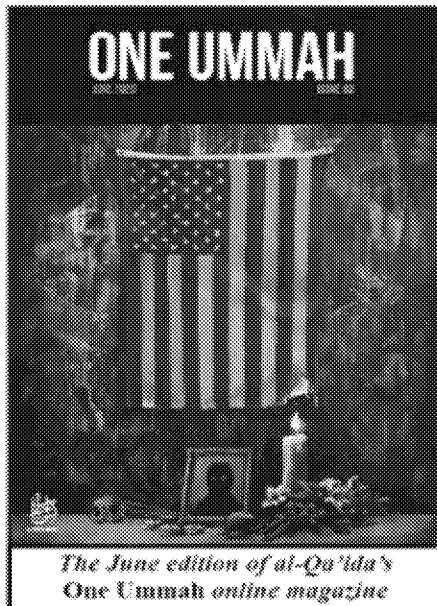


UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

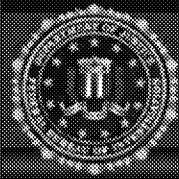


Publicity & Propaganda; Radicalizing & Recruiting

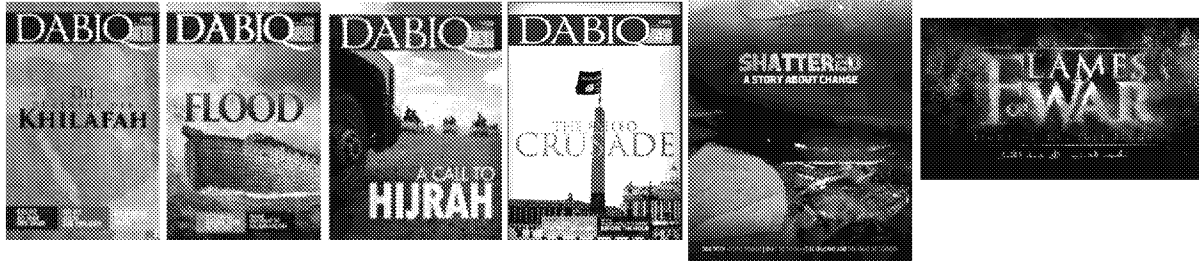
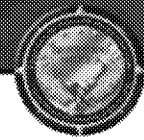


- "America Burns"
- "The Abysmal State of The US Economy"
- Manipulating the COVID-19 pandemic to claim US and Western countries were not interested in caring for and protecting the elderly.

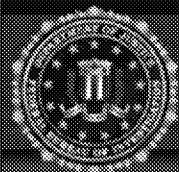
UNCLASSIFIED//FOUO



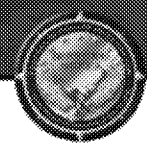
UNCLASSIFIED//FOUO
Publicity & Propaganda; Radicalizing & Recruiting
Historical



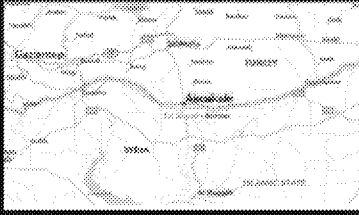
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO
Publicity & Propaganda; Radicalizing & Recruiting
Historical - EBOOKS



HIJRAH
to the
ISLAMIC STATE




What to Packup | Who to **Contact**
Where to **Go** | Stories
& more!

PREQUEL EBOOK:
THE ISLAMIC STATE (2015)

Summarized English Translation


Safety and Security guidelines
for Lone Wolf Mujahideen and small cells



أبي عبدة عبدالله العدم
حفظه الله

ترجمته: أبو عبد الله محمد بن عبد الله
Abu Usayb Abdullahu al-Adm

**HOW TO SURVIVE
IN THE WEST**



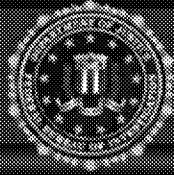
The book for how to
live in the West and how
to survive in the West
by Abu Usayb Abdullahu
al-Adm. It contains the
most important information
in the field.

**A MUJAHID GUIDE
(2015)**

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Training - Making Bomb Components

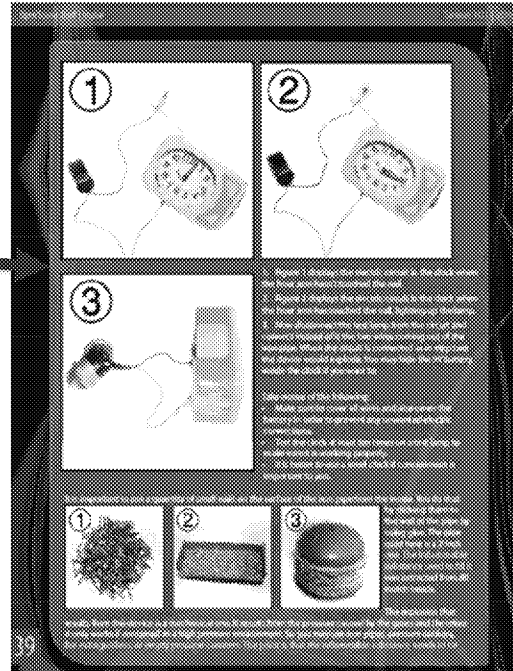
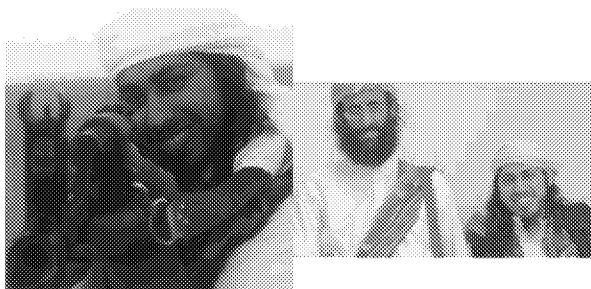


Samir Khan

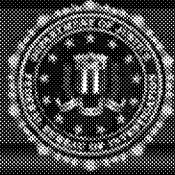
- Editor / Publisher of *Inspire*
- Left US for Yemen in 2009 (Age 23)
- Killed in drone strike of Anwar Al-Awlaki, September 2011

Inspire Issue 1:
 "Make a Bomb in the Kitchen of Your Mom."
 Authored by Samir Khan

Another Article by Khan: "I am proud be a traitor to America"



UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO
**Terrorism Financing:
Four Essentials Terrorists Need**



~~Ability to Travel~~

(Not needed for Homegrown Terrorist!)

~~Communications~~

(MINIMAL TO NONE for Homegrown Terrorist!)

~~Disposable Funds~~

(NONE Needed for Homegrown Terrorist!)

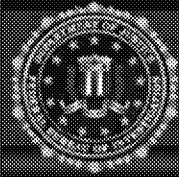
~~Training and Equipment~~

(MINIMAL for Homegrown Terrorist!)

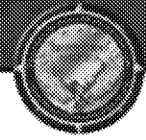
UNCLASSIFIED//FOUO

al-Qassam Brigades – Hamas Bitcoin Funding





al-Qassam Brigades – Hamas Bitcoin Funding



الارادة العنبري
الارادة العنبري

الرد الامثل على الصطبعين هو بتجريم الاحتلال
ودعم المقاومة بشتى الوسائل وفي مقدمتها
الدعم المالي..

عبر عنوان المحفظة الرئيسي والوحيد:

17QAWGVpFV4gZ25HQuq46e5m8ho4vDP6MD

#الناظر_حياته

UNCLASSIFIED//FOUO

Recent Terrorism Financing Charge

Former University of Alabama student
pleads guilty to helping al Qaeda

Updated Sept 11, 2019. Posted Sept 11, 2019.



Alaa Mohd Al-Absaad

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, September 13, 2019

Former Alabama Resident Pleads Guilty to Concealing Terrorism Financing

A criminal information was filed on Sept. 11, 2019, against Alaa Mohd Al-Absaad, charging her with concealment of terrorism financing, in violation of Title 18, United States Code, Sections 2389C and 2. Absaad pleaded guilty to the charge today. Assistant Attorney General for National Security John C. Dammers, United States Attorney Jay E. Byrum of the Northern District of Alabama, and FBI Special Agent in Charge Johnnie Sharp Jr. of the Birmingham Division made the announcement today.

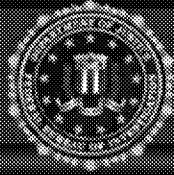
As set forth in the previously filed complaint, Al-Absaad instructed an FBI undercover employee (UCE) about how to send money to the mujahideen fighters engaged in jihad. Al-Absaad told the UCE that money "is always needed. You can't have a war without weapons. You can't prepare a soldier without equipment." Al-Absaad also advised the UCE on how to send money in a manner that would avoid detection by law enforcement, including by using fake names and addresses when conducting electronic money transfers. Subsequently, Al-Absaad introduced the UCE to a financial facilitator who could route the UCE's money to "brothers that work with us" (meaning in Qaeda).

The maximum penalty for concealment of terrorism financing is 10 years in prison and a \$250,000 fine, and up to a life term of supervised release.

Investigation of the case was conducted by the FBI, including FBI offices in Birmingham, Alabama, and Cleveland and Toledo, Ohio. The prosecution is being handled by Assistant United States Attorneys Henry Cornelius and Manu Balachandran and Trial Attorney Jennifer Lary of the National Security Division's Counterterrorism Section.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



Terrorism Costs: San Bernardino



Less than \$4,500

Pipe Bombs: \$959.45

\$300: 4 Remote Control Cars

\$550: Galvanized Pipe

\$100: 4 lbs explosive power (just show a DL)

Other small items (Christmas tree lights)

Guns/Ammo: ~\$3000

\$1450: 2 assault-style rifles

\$725: 2 handguns

~\$600: 1700 rounds of 9mm and .223 ammo

Target: Inland Regional Center

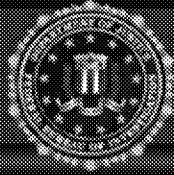
14 Killed & 22 Seriously Injured

Estimated Costs to the City/County: \$22.6M+



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



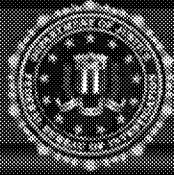
Terrorism Attack Costs



Event	Date	Estimated Cost
World Trade Center	2/26/1993	\$18,000
Oklahoma City Bombing <small>(Domestic Terrorism but included for Cost Comparison / HVE style)</small>	4/19/1995	\$4,320
East Africa Embassy Bombings	8/7/1995	\$50,000
Khobar Towers Bombing	6/25/1996	\$22,000
USS Cole Attack	10/12/2000	\$10,000
WTC/Pentagon	9/11/2001	\$400,000 To \$500,000
Jakarta JW Marriott Hotel Bombing	8/5/2003	\$30,000
Madrid Train Bombings	3/11/2004	\$71,460
London Bombings	7/7/2005	\$14,000

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



Info for BSA / AML Teams

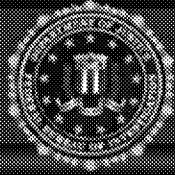


- SARS ARE SO IMPORTANT TO LAW ENFORCEMENT!
 - Today, tomorrow, next year...in 10 Years
 - Data mining by FBI
 - All cases are required to search FinCEN data including SARs/CTRs
- What can financial institutions do to help Law Enforcement?
 - Include as much IT biographical info in SARs as possible: email address, phones, IP addresses, App data (cookies / push tokens, etc.) EVEN OLD DATA!
 - Include location info for branches and activity (can help with venue)
 - Back up docs are great; continual/reoccurring SARs for updates
 - Put as many key words in the SAR write-up as possible. Think “What words would LE data mine that would hit on this SAR.”
- Why can't Agents tell bank investigators more? If you did, we could help you more...
 - Classification issues
 - Careful Agents
- Shift from NSLs to Other Legal process: Subpoenas and 2703d Court Orders
 - Legal requirement for organizations to comply (IT company issues)
 - Need a Non-Disclosure Court Order anyways (IT company issues)
 - Unclassified use

(side comment—IT companies are typically VERY responsive and helpful with Emergency Disclosures)
- **We use the data—and thank you for your help! (and Law Enforcement STINKS at telling investigators this!)**

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



Questions?

Special Agent [REDACTED]
Terrorism Financing Coordinator, FBI Charlotte Division
[REDACTED]
[REDACTED]@fbi.gov

UNCLASSIFIED//FOUO



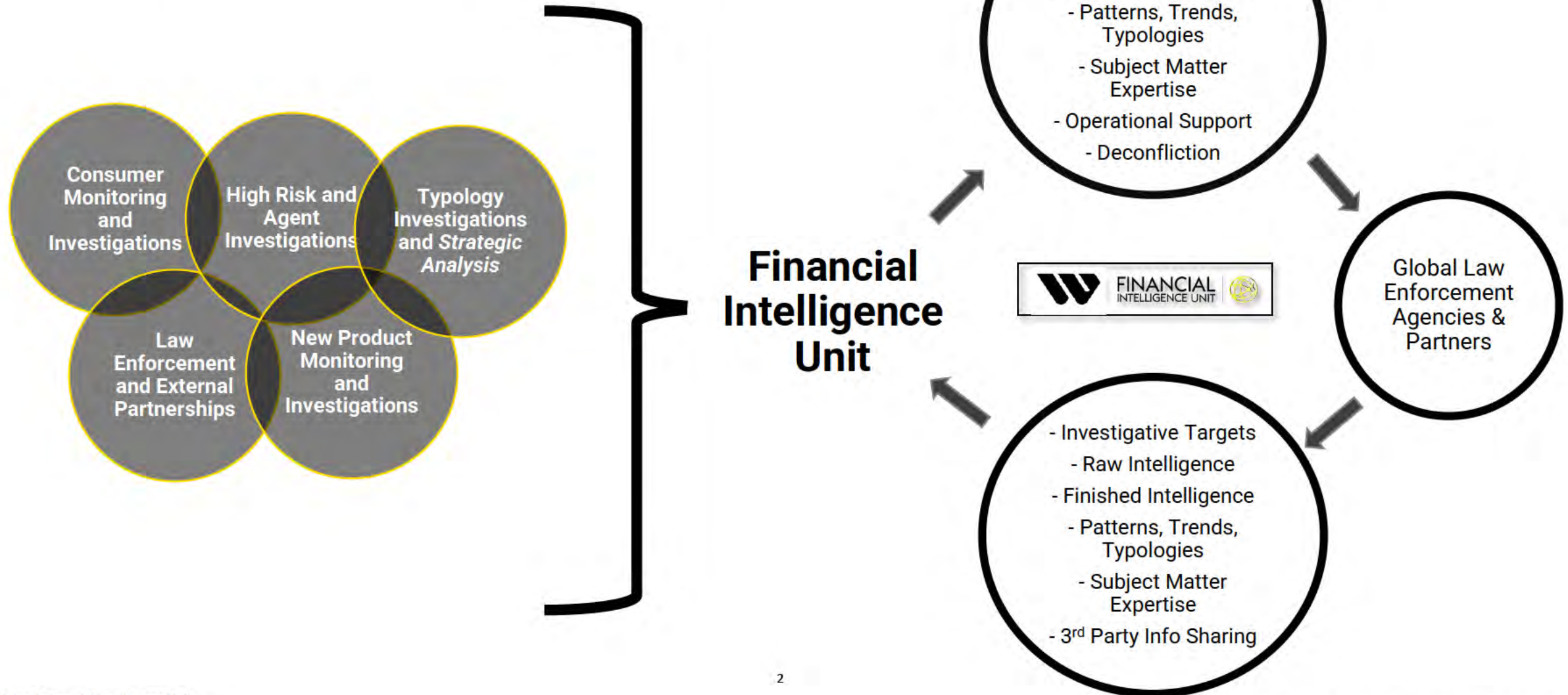
Using Strategic Intelligence to Combat Financial Crime

Presented by: [REDACTED]

March 2024



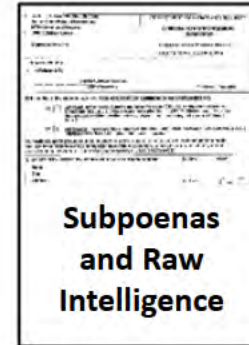
The Financial Intelligence Unit



The WU Financial Intelligence Unit Utilizes an “All Source” Approach to Drive the Detection of Suspicious Activity



Western Union Case History and Investigative Results



Transaction Red Flags





FIU Strategic Analysis Program



Core Program Mission

- ① To identify and evaluate WU's current exposure to significant illicit activity not otherwise fully mitigated at the tactical level (reactive).
- ② To identify and evaluate latent and emerging threats in order to mitigate risks before they fully manifest in our systems (proactive).



FIU Strategic Analysis Program



Example of Program Approaches:

- ① Typology to Target
- ② Intelligence Collection and Threat Tracking
- ③ Target to Typology

Target to Typology



1

Get Target from alert/LE/open source reporting



2



Search all WU Transactions



3



Analyze Results



5



Typology Characteristics

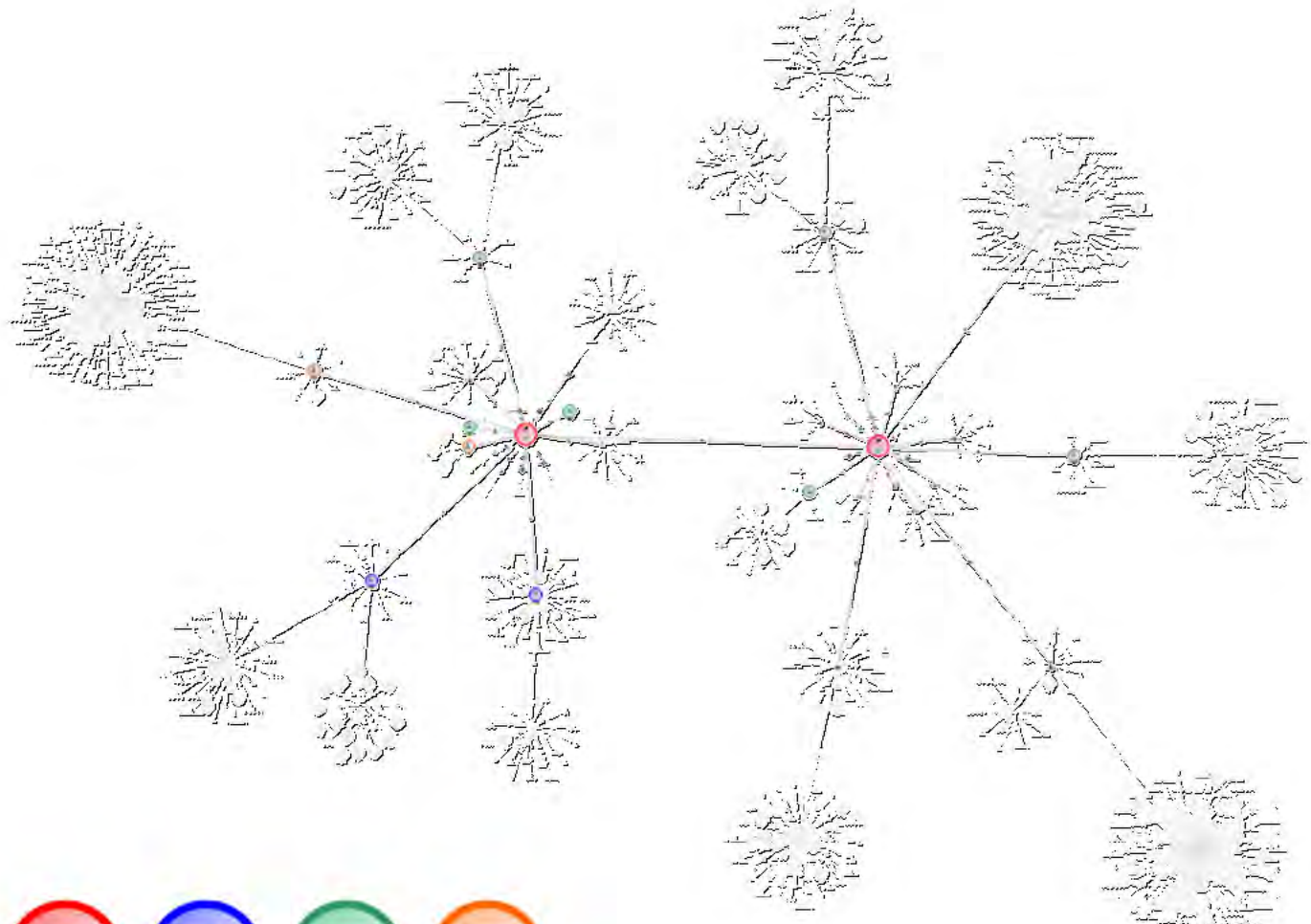


6

Generate New Targets



Tactical Analysis: Working from Specific Targets

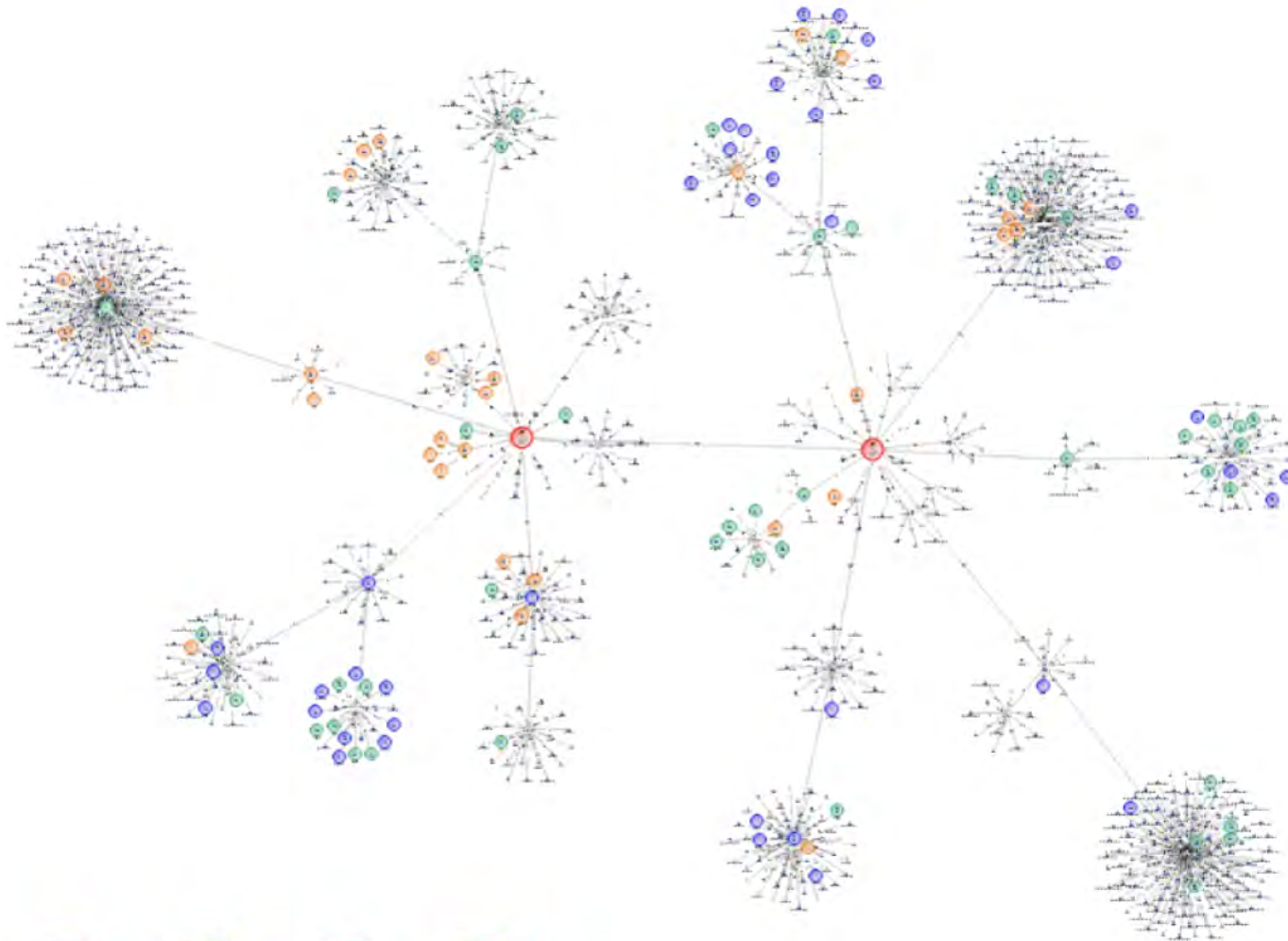


- 
Primary Target
- 
Turkey Subject
- 
Lebanon Subject
- 
US Subject





Tactical Analysis: Working from Specific Targets

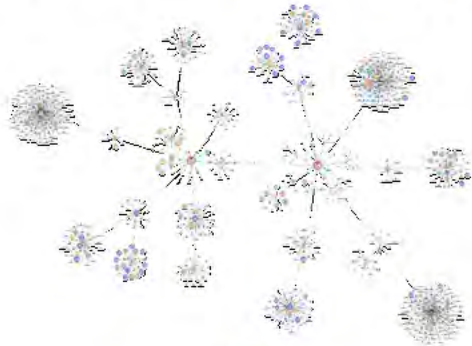


-  Primary Target
-  Turkey Subject
-  Lebanon Subject
-  US Subject





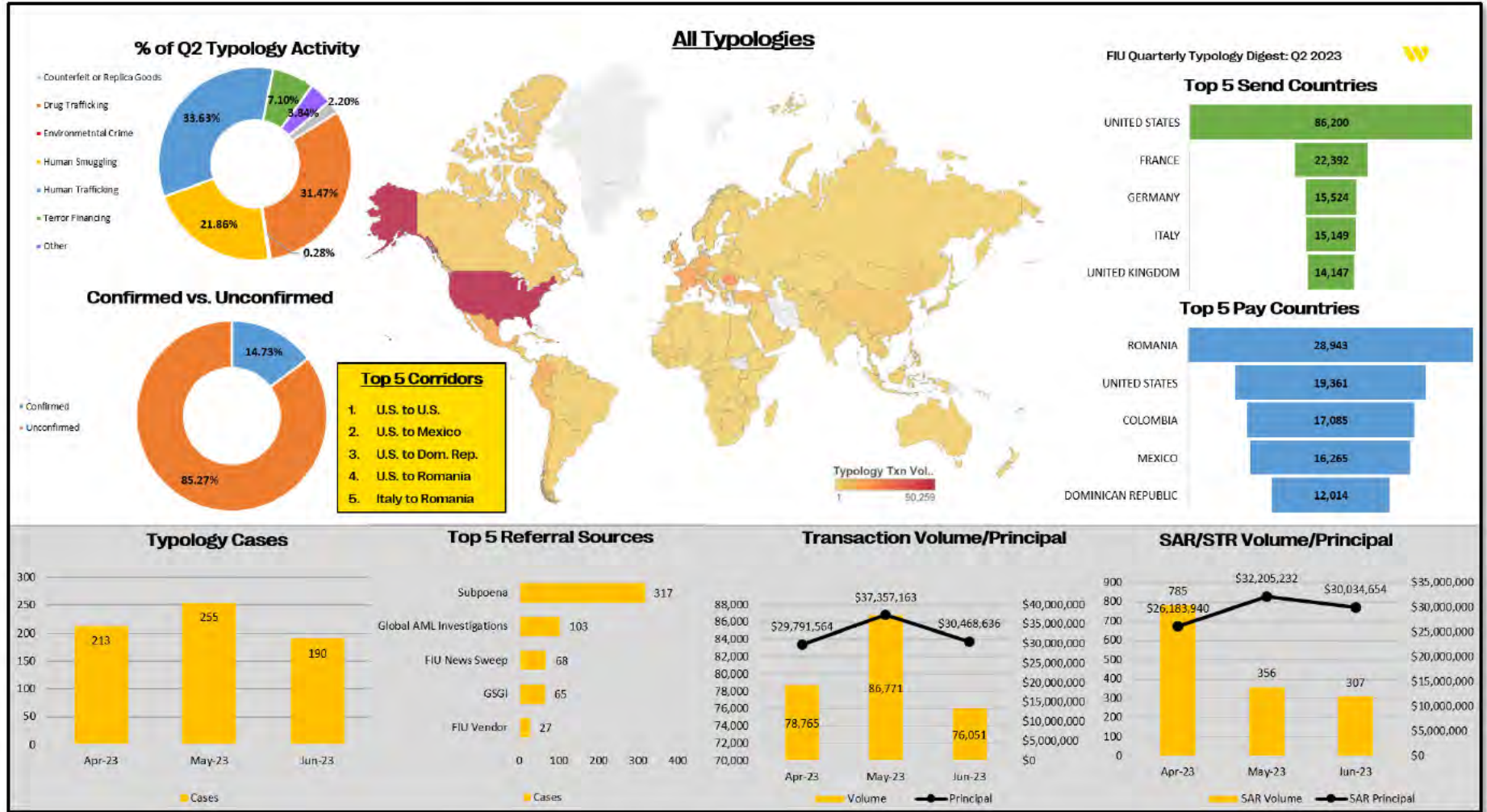
Tactical Investigations Drive Strategic Analysis



Typology Tracking

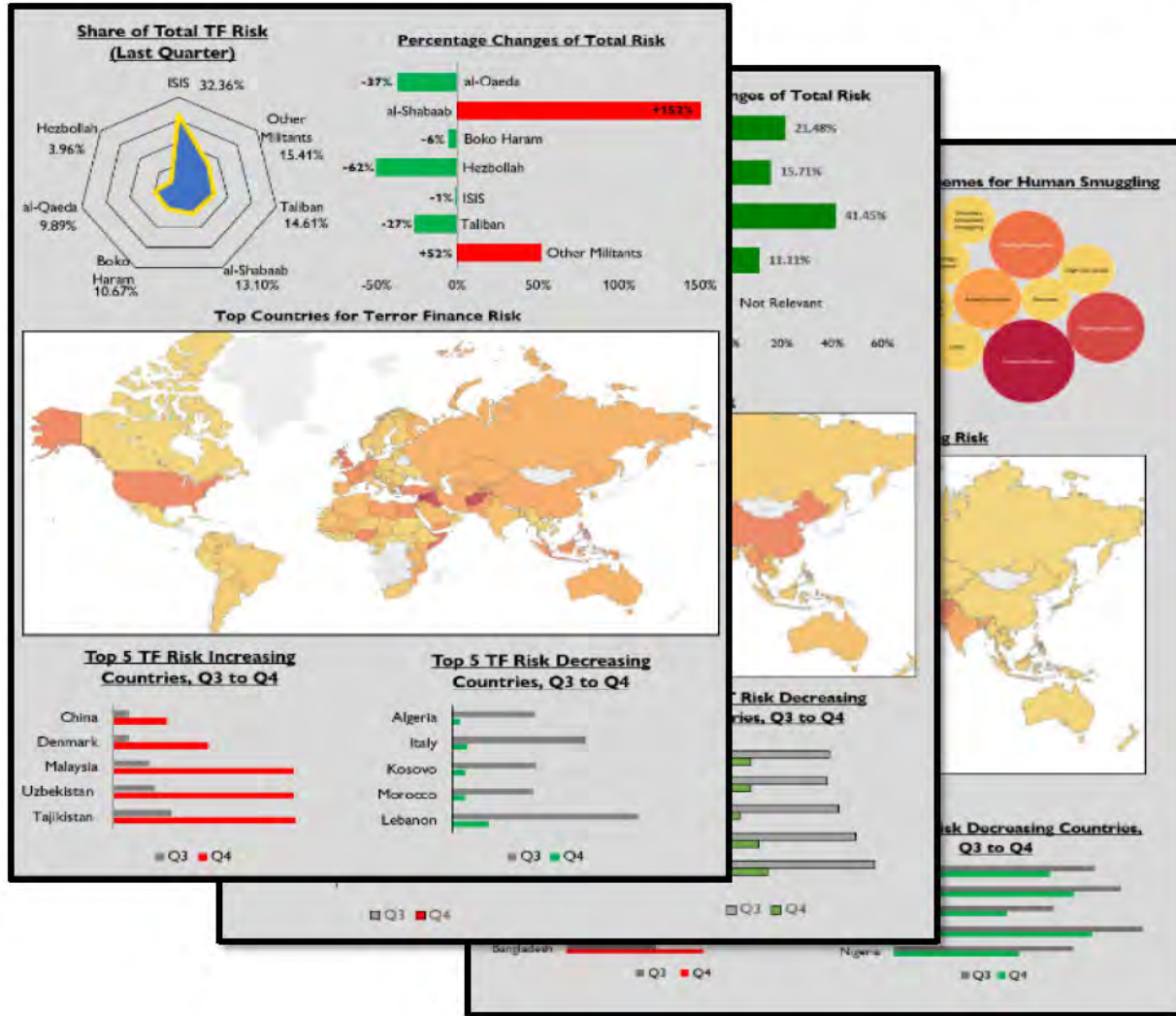


Strategic Analysis & Proactive Targeting

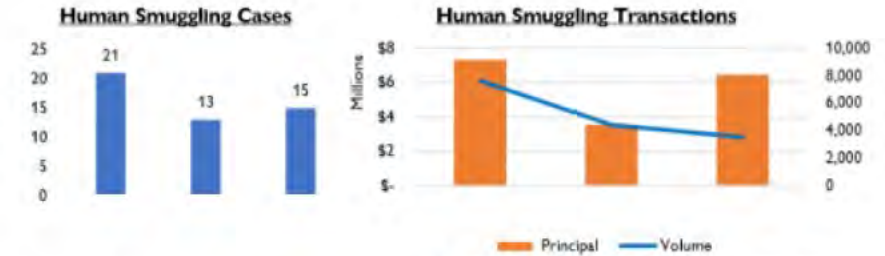




Integrated Real-Time View of Typology Risk



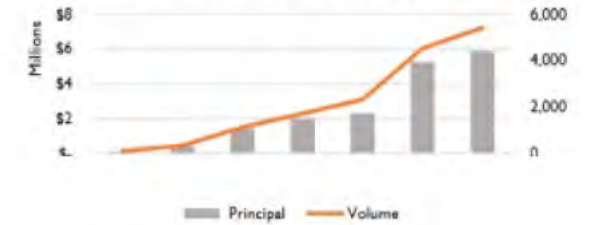
Human Smuggling Activity Identified



Confirmed vs Unconfirmed



Year of Send Date for Human Smuggling Transactions Identified in Q4



Human Smuggling Activity Conducted (Sent and Paid) in the Past 12 Months





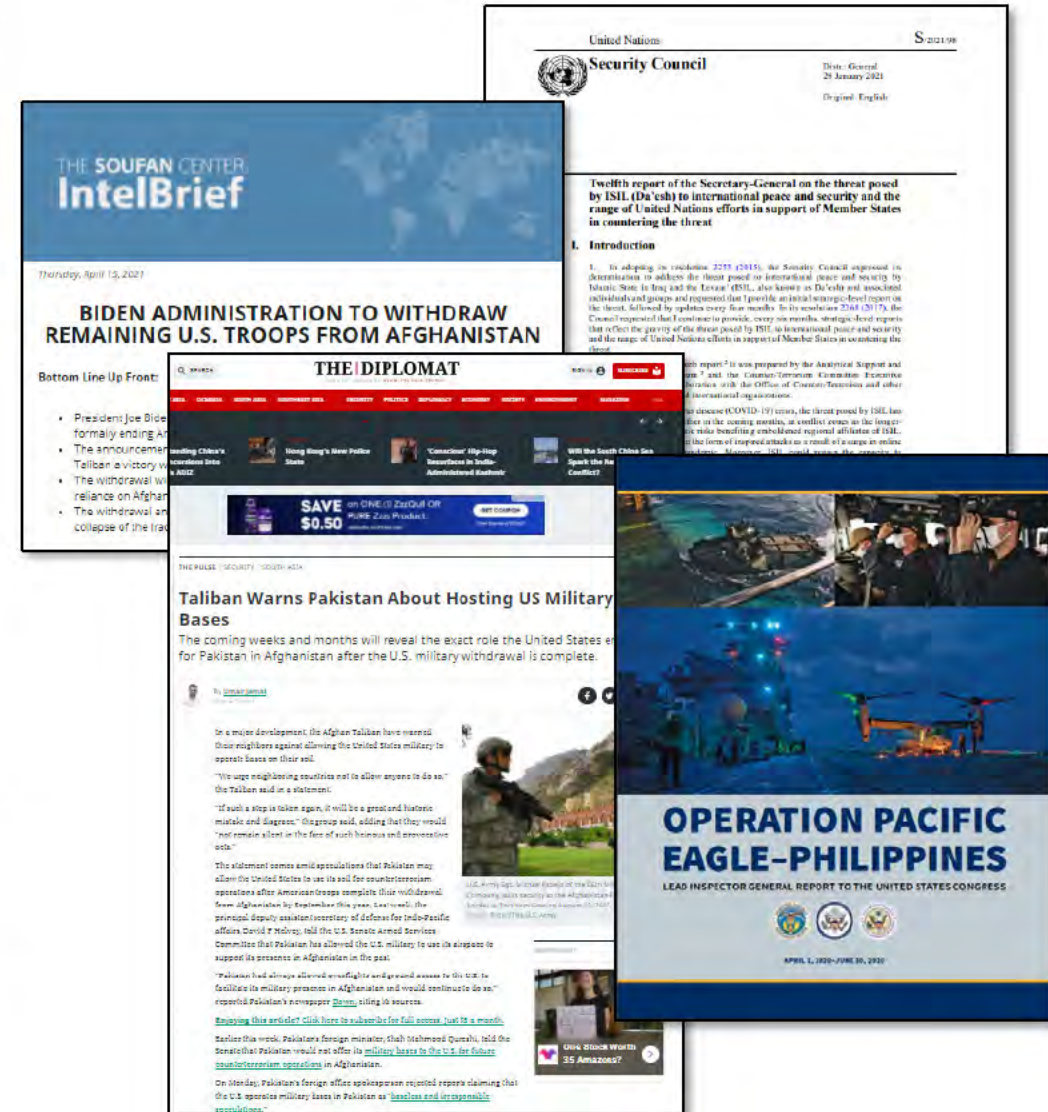
FIU Intelligence Collection and Threat Tracking

The **Intelligence Collection and Threat Tracking (ICTT)** program allows the FIU to monitor and evaluate developments external to the company in order to **maintain subject matter expertise and proactively identify threats** that are likely to impact Western Union and maintain subject matter expertise.

- The FIU uses ICTT to **systematically track the global threat environment** by integrating and synthesizing open-source intelligence, law enforcement intelligence, and other external information across major typologies, including:

- Terror Finance
- Human Trafficking
- Human Smuggling
- Drug Trafficking
- Counterfeit Goods
- Wildlife Trafficking

- Real-time updates to a **back-end data model** allow us to translate the intelligence into a functional framework for identifying and prioritizing threats across geographies and typologies.
- The intelligence model helps **guide and prioritize analysis** of potential threats as well as engagement with law enforcement and other partners.



Systematic Intelligence Integration and Threat Prioritization



Entry Title	Terror Group(s)	Country	Source Reliability	Credibility of Information	Relevance to WU
Syrians Arrested in Ankara, Turkey for Planning to Send Drone Equipment to IS in Syria	ISIS - Supports	Syria Turkey	Moderate	Moderate	Moderate
Arrest of Hundreds Suspected of ISIS Ties in Sweeping Counterterrorism Raids Across Turkey; Inability of Turkey's Law Enforcement and Legal System to Manage Such a High Number of Detainees	ISIS - Refutes	Turkey	High	Moderate	High
Overview: Hamza Al-Fandy ISIL Funding Network	ISIS - Supports	Syria Turkey	High	High	High
Devices Banned on Flights From 10 Countries Over ISIS Fears	ISIS - Supports	United Kingdom United States Jordan Egypt Turkey Saudi Arabia United Arab Emirates Kuwait Morocco Qatar	High	Moderate	Low
Greek Police Raid Amphetamine Lab Possibly Linked to ISIS	Other	Greece Turkey Syria	Moderate	Moderate	Moderate
Hamza Al-Fandy ISIL Funding Network	ISIS - Supports	Syria Turkey	Moderate	High	High
Alleged Smuggling of IS Fighters from Libya to Italy Using False Passports Through Special Medical Program	ISIS - Supports	Libya Italy Turkey	High	Moderate	High
Arrest and Sentencing of 27 Individuals in Beirut, Lebanon for Terror Finance Activities; Possible Use of OMT to Transfer Funds	ISIS - Refutes	Turkey United Arab Emirates Syria Lebanon Georgia Germany	Moderate	Moderate	High



Identifying and Prioritizing Threat Issues

Typology Specific Developments & Updates

FIU Quarterly Typology Digest: Q2 2023

Drug Trafficking

FIU Quarterly Typology Digest: Q2 2023

US Indicts Chinese Companies in New Approach to Fighting Precursor Chemicals

The U.S. government has brought its first-ever criminal charges against four China-based companies and eight employees for allegedly trafficking precursor chemicals used to produce fentanyl into the U.S. Prosecutors claim that the companies knowingly marketed and distributed their products for illicit use, citing evidence including advertisements explicitly targeting fentanyl producers in Mexico and the US, efforts to disguise their products from customs checks, and instructions for altering these chemicals to produce fentanyl. Then, criminal groups like the Sinaloa Cartel and the Jalisco Cartel New Generation (Cartel de Jalisco Nueva Generación - CJNG) got involved: purchasing, stockpiling and transporting the drug across the US-Mexico border.

Terror Finance

FIU Quarterly Typology Digest: Q2 2023

Israel Seizes \$1.7MM in Crypto from Terror Finance Operation Run by Hezbollah and Iran's IRGC-Quds Force



In late June 2023, Israel's National Bureau for Counter Terror Financing (NBCTF) disrupted a crypto-based terrorism financing infrastructure jointly run by Hezbollah and Iran's IRGC - Quds Force in which they seized roughly \$1.7 million worth of cryptocurrency. The operation represents the first time any agency has seized cryptocurrency from the two organizations, both of which are designated as Foreign Terrorist Organizations (FTOs). The disrupted Hezbollah/IRGC-QF crypto operation is also notable as one of the first publicly available examples of terrorism financing via cryptocurrency that goes beyond

Human Smuggling

FIU Quarterly Typology Digest: Q2 2023

U.S. Administration Expands Migration Policy to Additional Countries to Address HS Surge at Southwest Border



The U.S. Department of State and Department of Homeland Security announced a new initiative, which formally started on July 10, allowing eligible migrants from Colombia, El Salvador, Guatemala and Honduras to fly to the U.S. and gain government work permits if they have relatives who are U.S. citizens or legal residents and have filed visa applications on their behalf. This expands the current policy permitting Venezuelans, Nicaraguans, Cubans, and Haitians to enter the U.S. under mostly identical stipulations as of several months ago. These policies are coupled with tightened asylum rules and increased deportations for those who do not use these programs and are smuggled into the U.S.

Investigative Journalism Reveals Two Primary HS Routes Pakistani Migrants Utilize to Reach Europe

A recent report detailed the two primary routes that Pakistani migrants are currently using to reach Europe, according to several interviews with migrants. The first route begins at the Pakistani border city of Taftan, before travel to Mashaad in Iran, Maku in Turkey, and then eventually crossing the western Turkish border into Greece.

The second route involves a flight from Karachi, Pakistan to Dubai and then Cairo, Egypt. Then travel to Benghazi, Libya occurs, passing through Tabarak, Egypt, where a cross-Mediterranean trip is made towards Italy. This second route was the route utilized by the human smuggling network who contributed to the deaths of up to 300 Pakistani migrants in June. Pakistani migrants are the third-most common nationality observed utilizing the Central Mediterranean migration route, the most popular in Europe in 2023.

Routes used by Pakistan's Human Traffickers



any other drug in ysis has identified emical companies sing. For example,



Working Group of the Hezbollah operation



so continues its



Threat Intelligence Drives Strategic Projects

Typology Specific Developments & Updates

Drug Trafficking

US Indicts Chinese Companies in New Approach to Fighting Precursor Chemicals

The U.S. government has brought its first ever criminal charges against the Chinese chemical companies and eight employees for allegedly trafficking precursor chemicals used to produce fentanyl. The U.S. Prosecutors claim that the companies knowingly marketed and distributed their products for illicit use using extensive international transportation networks involving tertiary producers in Mexico and the US, which to bypass their own customs checks, and transactions for selling these chemicals to produce fentanyl. They, instead, engage the United States and the United Kingdom to help identify and prosecute these companies. For example,...

Terror Finance

Israel Seizes \$1.7M in Crypto from Terror Finance Operation Hunted by Israeli Hishvalet and Israel's HRC-Q

In June 2023, Israel's Internal Security Authority (ISA) and Israel's Hishvalet (HSH) identified a crypto-based terrorism financing infrastructure primarily run by Hezbollah and Iran's HRC-Q. Data from the seizure totaled roughly \$1.7 million worth of cryptocurrency. The operation represents the first time any seizure has been reported from the two organizations both of which are considered as Foreign Terrorist Organizations (FTOs). The identified Hezbollah/HRC-Q crypto operation is also notable as one of the first publicly available examples of terrorism financing via cryptocurrencies that have been seized by a national law enforcement agency.

Human Smuggling

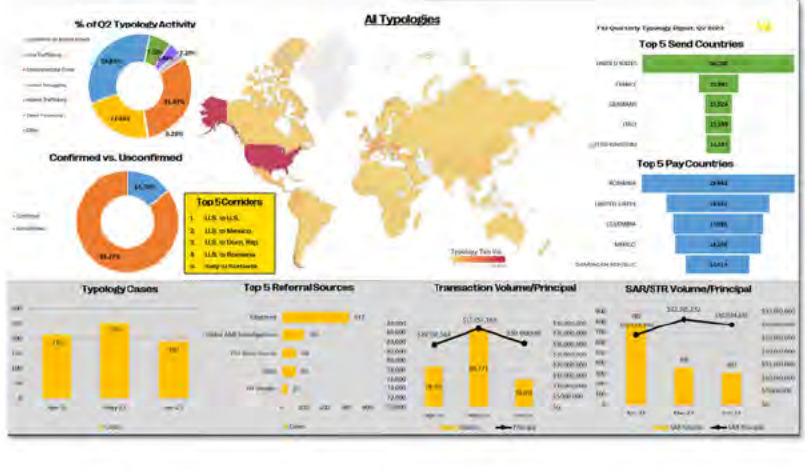
U.S. Administration Expands Repatriation Policy to Additional Countries to Address HS Surge at Southwest Border

The U.S. Department of State and Department of Homeland Security announced a new initiative, which formally started on July 10, allowing eligible migrants from Colombia, El Salvador, Guatemala and Honduras to fly to the U.S. and gain government work permits if they have relatives who are U.S. citizens or legal residents and have filed an application on their behalf. This expands the current policy permitting Venezuelans, Nicaraguans, Cubans, and Haitians to enter the U.S. under mostly identical stipulations as of several months ago. These initiatives are coupled with tightened system rules and increased deportations for those who do not follow program rules and who are ineligible for the U.S.

Human Trafficking

Routes used by Pakistan's Human Traffickers

A recent report detailed the key primary routes that Pakistani migrants are commonly used to reach Europe, centered by several intermediate safe harbors. The first route begins at the Pakistani border city of Tattar, before travel to Istanbul in Turkey, and subsequently crossing the western Turkish border into Greece. The second route involves a flight from Karachi, Pakistan to Dubai and then Cairo, Egypt. From there, they travel to Benghazi, Libya, passing through Palermo, Egypt, where a cross-Mediterranean trip is made towards Italy. This second route was the most common for the human smuggling network to be reported on in a series of up to 300 Pakistani migrants in June. Pakistani migrants are the most common nationality observed utilizing the Central Mediterranean migration route, the most popular in Europe in 2023.



Proactive / Strategic Threat Analysis Projects

WU Faces High Terror Finance Threat in the Sahel

This product was prepared by the FIU Office of Typology Investigations & Strategic Analysis to inform Comptroller and a specific AM-CTI threat issue that could impact Western Union (WU) products and services. This document and all associated content, are confidential and may not be disseminated outside WU. Compliance department will not be approved from the FIU. Please direct any questions to [redacted].

WU Faces a High Threat of Terror Finance in the Sahel; Analysis Identifies 213 Potential Terror Finance Facilitators

Background: Open-source reporting confirms a steep increase in jihadist violence in the Sahel region of Africa, especially in Mali, Burkina Faso, and Niger since at least 2019. Over the wide body of intelligence reporting, the FIU reviewed 183 potential exposures to the evolving threat.

Scope: The FIU reviewed activity conducted by potential terror finance facilitators whose activity included higher-level transactions patterns within the Sahel region in the Sahel region. The FIU conducted analysis between 5/1/2022 and 8/19/2023 ("Review Period").

Key Finding: The FIU judges with moderate confidence that WU faces a high threat of terror finance in the Sahel region.

This assessment is based on the following factors:

- A wide body of open-source reporting indicates the central Sahel region of Mali, Burkina Faso and Niger is now the world's deadliest for terror attacks and is considered the "global epicenter for jihadism."
- The analysis identified 213 potential terror finance facilitators ("primary subjects") who matched higher-level transaction patterns that have historically been associated with terror finance. These 213 potential facilitators conducted \$3.5B in transactions totaling \$1.5 million during the review period.
- Approximately 32% (67/203) of these primary subjects sent transactions to counterparties at 83 AGI Agent locations in multiple, emerging global hotspots around the world.
- Approximately 7% (14/203) of the primary subjects had transaction links to prior FIU investigations primarily related to terror finance, weapon trafficking, or human trafficking.
- Our confidence level is not higher due to a lack of corroborating law enforcement referrals to match the open-source information and plausible alternative explanations, such as familial relationships between France and the Sahel, as well as legitimate commercial travel between the same and full countries such as South Africa, Kuwait and the United Arab Emirates.

Sahel Emerges as World's Most Violent Region for Jihadist Activity; Seizes Few External TF Referrals

Central Sahel region of Mali, Burkina Faso and Niger is now the world's deadliest for terror attacks. In 2023, this region led for "45 percent of the world's reported deaths" from Asia and the Middle East region combined. The region's fatalities in 2023, which is four times more deadly than 2019, that pace mostly continued in the first half of this year.

Increasing security situation is made worse by recent political gains in the region. The countries of Mali, Burkina Faso, Niger, have been at least successful since 2021.

Primary terror groups maintain a presence in the region of Mali, Burkina Faso and Niger. The "Islamic State of Greater Sahara" (ISGS) is a militant group active in Mali, Niger, Burkina Faso and a large province, controlling large swaths of the Sahel. ISGS has also been expanding with aggressive and credible attacks. They are mostly confined to northern Mali and northern Niger.

ISGS and ISGS appear to have mostly relied on networks of fighters, and have increased local positions for funding, which is reportedly to be used to expand into neighboring countries of Topo, Benin, Gambia and potentially northern Ghana.

ISGS reportedly 248 agents in high-risk "red" or "orange" zones, such as Central and the "Tuareg" area of Mali, Niger, Burkina Faso. These agents make up 9% of agents in total three countries.

Informational outreach suggests that the ISGS is poorly understood for intelligence purposes. There were just 3 cases between 2023 and 2021/2023 with confirmed threat intelligence conducted at that location in the Sahel, a steep drop from 2019 year when there were 20 similar cases.

Primary Subjects Identified as Potential Terror Finance Facilitators; Additional Indicators

WU 203 potential terror finance facilitators and their direct counterparties conducted 4,472 activities worth \$3.5 billion from July 01, 2022 to August 07, 2023. These consumers displayed the following indicators:

- Links to Confirmed TF Activity (7%)** - In June 2018, last primary subject had sent a three-bank network with at least 20 counterparties to a confirmed terror finance entity.
- Links to Direct Targets (2%)** - These subjects were part of a three-level network with at least one consumer who is a direct target of a terror finance entity.
- Recent Links to Prior TF Connections** - In 5/2023, these subjects were part of a two-level network with 10 counterparties who appeared in a prior terror finance investigation.
- Risk Senders to Many Global Jihadist Hotspots (2%)** - The first of the primary subjects transacted at WU locations in the Gulf states of Saudi Arabia, Kuwait or United Arab Emirates and sent to counterparties at WU locations in the Sahel and at least two other emerging finance hubs across the world, 14 of these agents had large amounts (i.e. \$1,000) in remote parts of the world.
- Risk Nationalities in the Sahel (14%)** - These consumers had a majority of up to 10 locations from Lebanon, Syria, Yemen, Venezuela etc.
- Risk Travel (9%)** - These consumers last transacted at least one high-risk country for terrorism, including, Syria, Yemen or Ethiopia and then transacted for the first time in the Sahel, indicating a high-risk figure pattern of movement.

Risk Sahel City (9%)

These consumers appeared in remote towns of Gao or Mopti that are the most at-risk hotspots for terror finance in the Sahel.

Top with Previous FIU Investigations (7%) - This includes 4% that appeared in a FIU-related FIU report issued in 2018, which either originated in the Sahel or involved a human trafficking or terrorism investigation.

2023 of Primary Subjects Linked to Potential Human Smuggling through a Transit City of Agadez or Tahoua in Niger

2023 of these subjects were identified in Agadez, a city in northern Niger that has long served as a hub for human smuggling, attempting to reach Europe.

70% of these subjects had an address that matches a unique agent in Agadez concerning the United States.

Primary subject illustrates the potential connections between human smuggling and terror finance in a consumer in Tahoua, Niger, which has emerged as an emerging alternative to Agadez, received over 20,000 from 31 airlines in France and other countries in both Niger and France during the review period.

Additional consumers in the primary subject's network appeared in terror finance cases. All of these were based in Niger and received from many of the same banks in France.

Operational Actions

Reports

Standardized 708 consumer who met the following criteria:

- Matched 213 potential terror finance facilitators
- Matched with 213 counterparties previously investigated by the FIU for terror finance as the result of law enforcement referrals (37)
- Matched with multiple indicators above

Notes

WU and its subsidiary WU Agent concentrations or indications of potential Agent contact that would either analyze WU FIU data. As a result, no Agent locations were referred.

WU is reviewing a potential threat to terror finance in the Sahel region which may be sending to many other high-risk jurisdictions for terror finance globally.

Confidence

Confidence is generally means the information could be interpreted in various ways. We have reviewed views of the information is credible and plausible but not sufficiently corroborated to warrant a high level of confidence. Transaction patterns are characteristic of specific risk exposure behavior, a portion of the activity may have plausible alternative (not or illicit) explanations.

Confidence

Confidence generally means the information is scarce, questionable, or very fragmented and it is hard to make solid, unique inferences, or we have significant concerns or problems with the information. Transaction patterns may be consistent with certain illicit behavior, but significant portions of it is very plausible alternative (not or illicit) explanations.

Some analytic judgments also include language that reflects the FIU's sense of probability that a threat event will occur. Using phrases like "likely," "probable," or "reasonable," we cannot state "we cannot discount" or "we are unlikely" or "we are more likely" or "we are more confident" as such terms lack meaningful, words such as "may be" and "suggest" are also in situations where we are unable to be confident because current information is sparse or not sufficiently clear to justify a more confident.

Confidence Gaps & Assumptions

The FIU included referrals from the enforcement of external support to terror finance facilitators in the Sahel, which were not confirmed views of any direct activity involving the Sahel and using WU. These examples did not provide a comprehensive picture that could be adapted to look for additional cases.

A high-risk national for terror finance transacting with a consumer in the Sahel who is currently a higher risk for terror finance, especially within a network that contains additional high-risk nationalities.

Confidence Levels

Confidence is generally means the information could be interpreted in various ways. We have reviewed views of the information is credible and plausible but not sufficiently corroborated to warrant a high level of confidence. Transaction patterns are characteristic of specific risk exposure behavior, a portion of the activity may have plausible alternative (not or illicit) explanations.

Confidence

Confidence generally means the information is scarce, questionable, or very fragmented and it is hard to make solid, unique inferences, or we have significant concerns or problems with the information. Transaction patterns may be consistent with certain illicit behavior, but significant portions of it is very plausible alternative (not or illicit) explanations.

Some analytic judgments also include language that reflects the FIU's sense of probability that a threat event will occur. Using phrases like "likely," "probable," or "reasonable," we cannot state "we cannot discount" or "we are unlikely" or "we are more likely" or "we are more confident" as such terms lack meaningful, words such as "may be" and "suggest" are also in situations where we are unable to be confident because current information is sparse or not sufficiently clear to justify a more confident.

Confidence Gaps & Assumptions

The FIU included referrals from the enforcement of external support to terror finance facilitators in the Sahel, which were not confirmed views of any direct activity involving the Sahel and using WU. These examples did not provide a comprehensive picture that could be adapted to look for additional cases.

A high-risk national for terror finance transacting with a consumer in the Sahel who is currently a higher risk for terror finance, especially within a network that contains additional high-risk nationalities.

Confidence Levels

Confidence is generally means the information could be interpreted in various ways. We have reviewed views of the information is credible and plausible but not sufficiently corroborated to warrant a high level of confidence. Transaction patterns are characteristic of specific risk exposure behavior, a portion of the activity may have plausible alternative (not or illicit) explanations.

Confidence

Confidence generally means the information is scarce, questionable, or very fragmented and it is hard to make solid, unique inferences, or we have significant concerns or problems with the information. Transaction patterns may be consistent with certain illicit behavior, but significant portions of it is very plausible alternative (not or illicit) explanations.

Some analytic judgments also include language that reflects the FIU's sense of probability that a threat event will occur. Using phrases like "likely," "probable," or "reasonable," we cannot state "we cannot discount" or "we are unlikely" or "we are more likely" or "we are more confident" as such terms lack meaningful, words such as "may be" and "suggest" are also in situations where we are unable to be confident because current information is sparse or not sufficiently clear to justify a more confident.

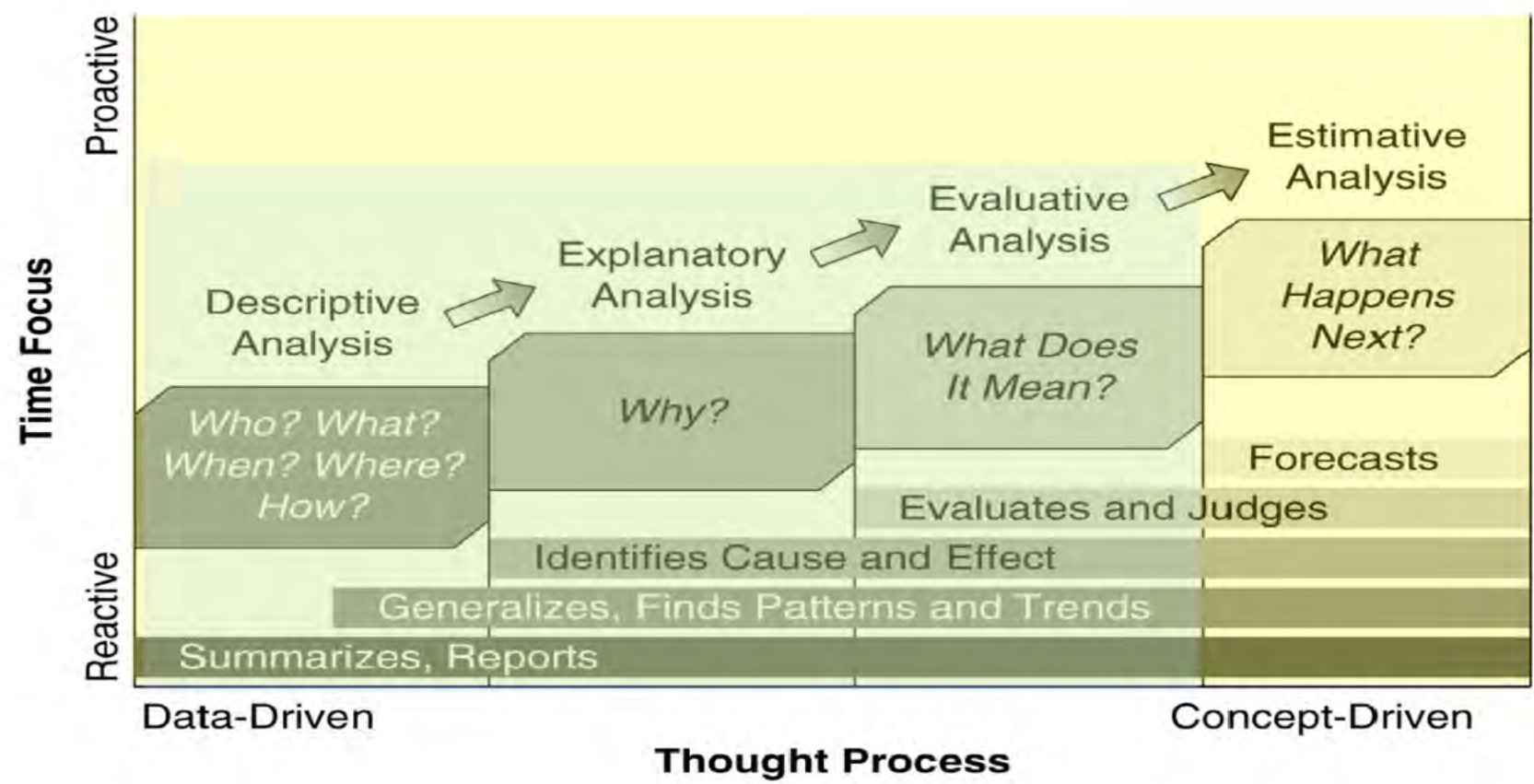
Confidence Gaps & Assumptions

The FIU included referrals from the enforcement of external support to terror finance facilitators in the Sahel, which were not confirmed views of any direct activity involving the Sahel and using WU. These examples did not provide a comprehensive picture that could be adapted to look for additional cases.

A high-risk national for terror finance transacting with a consumer in the Sahel who is currently a higher risk for terror finance, especially within a network that contains additional high-risk nationalities.

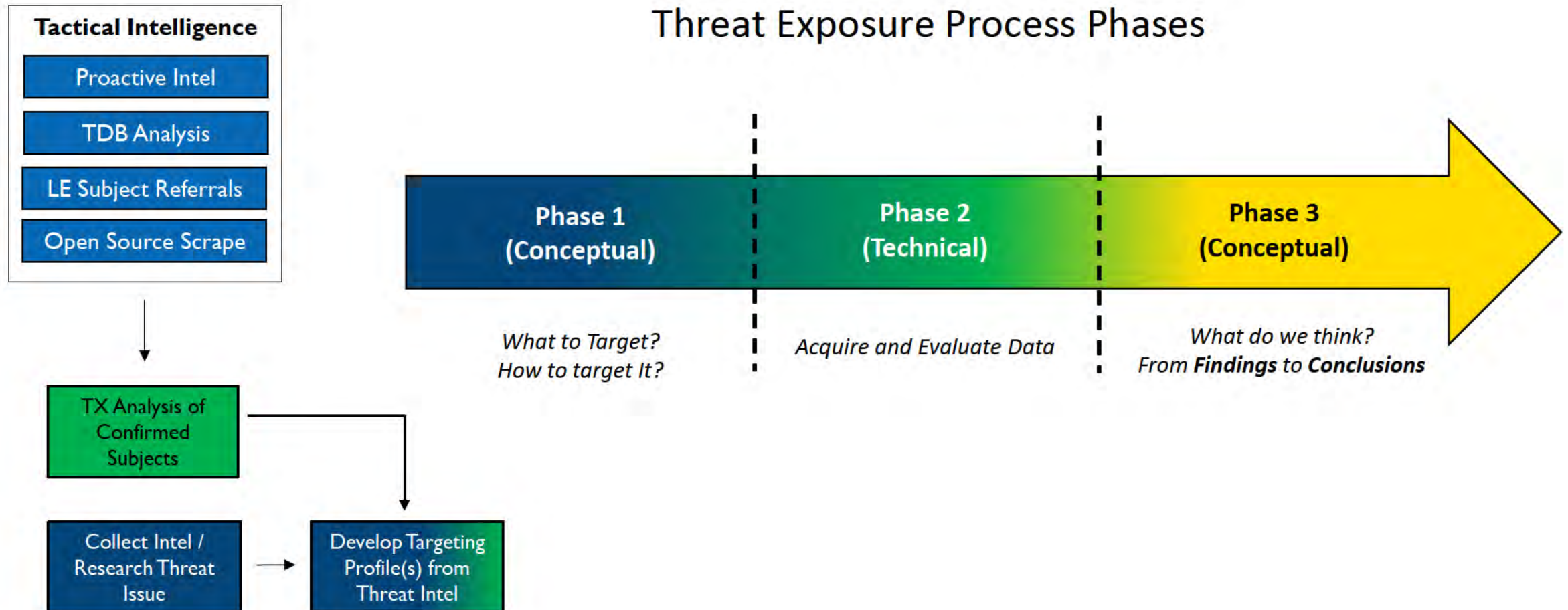
Strategic Analysis Project Process Overview

The primary purpose of projects is to draw **analytic judgements** (conclusions) about **the nature and extent** of Western Union exposure to a **particular AML/TF threat issue** or **set of referred activity**.



Strategic Analysis Project Phases

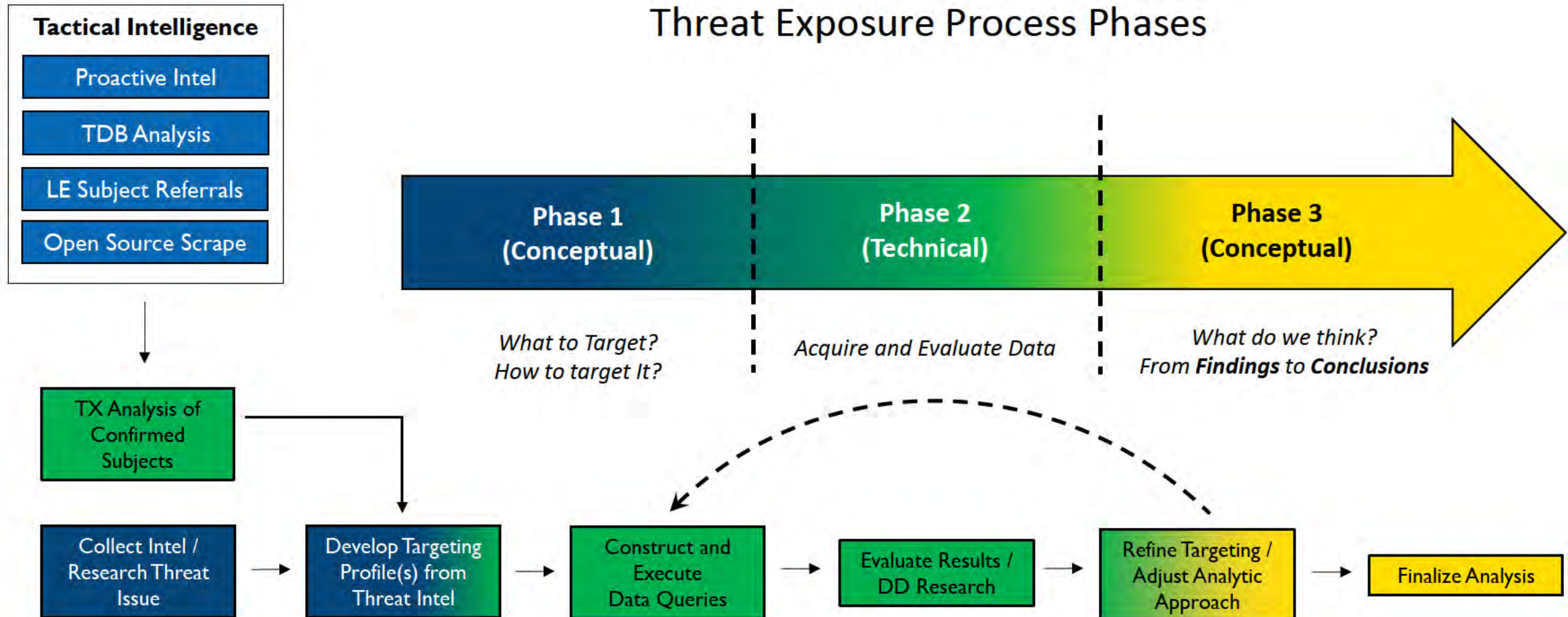
The primary purpose of projects is to draw **analytic judgements** (conclusions) about **the nature and extent** of Western Union exposure to **a particular AML/TF threat issue or set of referred activity**.





Strategic Analysis Project Phases

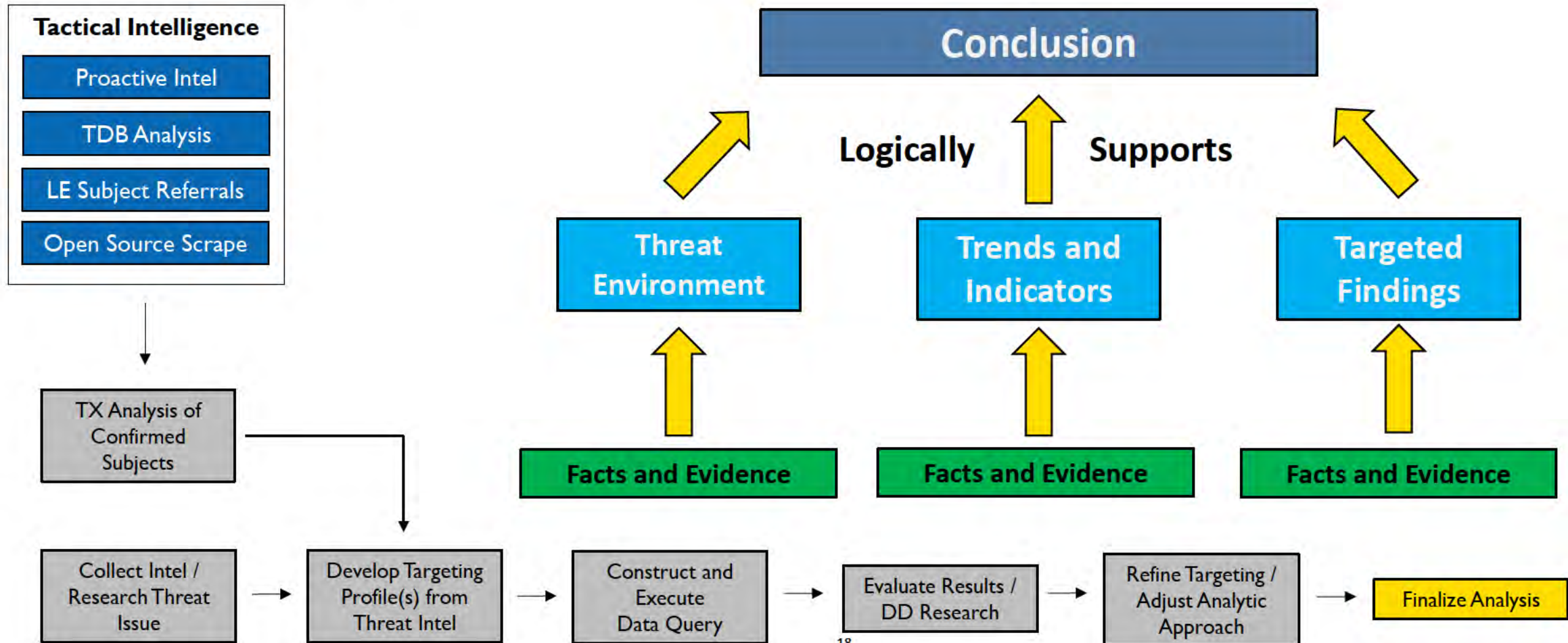
The primary purpose of projects is to draw **analytic judgements** (conclusions) about **the nature and extent** of Western Union exposure to a **particular AML/TF threat issue** or **set of referred activity**.





Strategic Analysis Project Process Overview: Making Judgements

The primary purpose of projects is to draw **analytic judgements** (conclusions) about **the nature and extent** of Western Union exposure to a **particular AML/TF threat issue** or **set of referred activity**.



Typology to Target



1

Typology Characteristics



2

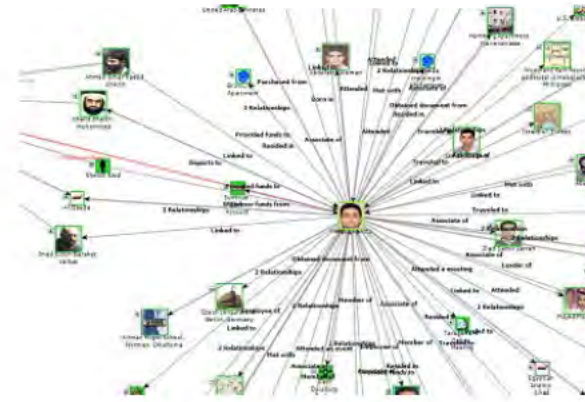


Search all WU Transactions



6

Update/Enhance Typology



Build Network



5



ID entities with Questionable Activity



4



Analyze Results



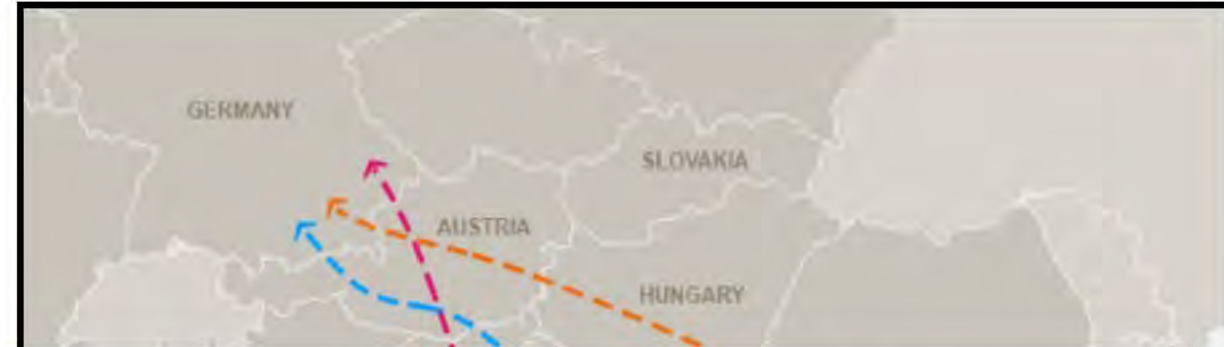
3

Strategic Analysis from Typology Characteristics

Inside Europe's people-smuggling networks: A journey from Afghanistan to Germany

NBC News met Zubair Nazeri in Serbia and tracked him for a year as he repeatedly tried to reach the West.

The recruiters or agents used by migrants outside of their home country tend to be of the same nationality, according to experts. Many are also former migrants.



██████████ said he and his companions paid \$6,000 (€5,500) each in Afghanistan for the services of smugglers who would, supposedly, get them to Germany.

“Crossing Iran we had an Iranian ‘guide’; in Turkey an Afghan, and in Bulgaria a Pakistani,” he recalls. “But in Serbia, we have no one.”

ATINA

██████████ said he and his companions paid \$6,000 (€5,500) each in Afghanistan for the services of smugglers who would, supposedly, get them to Germany.

“Crossing Iran we had an Iranian ‘guide’; in Turkey an Afghan, and in Bulgaria a Pakistani,” he recalls. “But in Serbia, we have no one.”



Strategic Analysis from Typology Characteristics

**Inside Europe's people-smuggling networks:
A journey from Afghanistan to Germany**


ATINA

CITIZENS ASSOCIATION FOR COMBATING
TRAFFICKING IN HUMAN BEINGS AND ALL FORMS
OF GENDER - BASED VIOLENCE

(23) said he and his companions paid \$6,000 (€5,500) each in Afghanistan for the services of smugglers who would, supposedly, get them to Germany.

"Crossing Iran we had an Iranian 'guide'; in Turkey an Afghan, and in Bulgaria a Pakistani," he recalls. "But in Serbia, we have no one."

EXTERNAL INTELLIGENCE

1. Payees in one or more of the following countries identified as a transit route for South Asian migrants flowing to Europe via the Balkan Route: **Albania, Bulgaria, Croatia, Greece, Hungary, Macedonia, Romania, Serbia.**
2. Payees who listed a **Country of Birth (COB)** among one of the following countries associated with significant migration via the Balkan Route: **Afghanistan, Bangladesh, Iraq, Pakistan, Syria.**



INTERNAL DATA

3. Payees matching either of the above criteria who also received transactions from **13 or more distinct counterparties** and **three or more Send countries.**



Strategic Analysis from Typology Characteristics

ENTITY TYPE + GEOGRAPHY + DIRECTION + THRESHOLD + TIMEFRAME

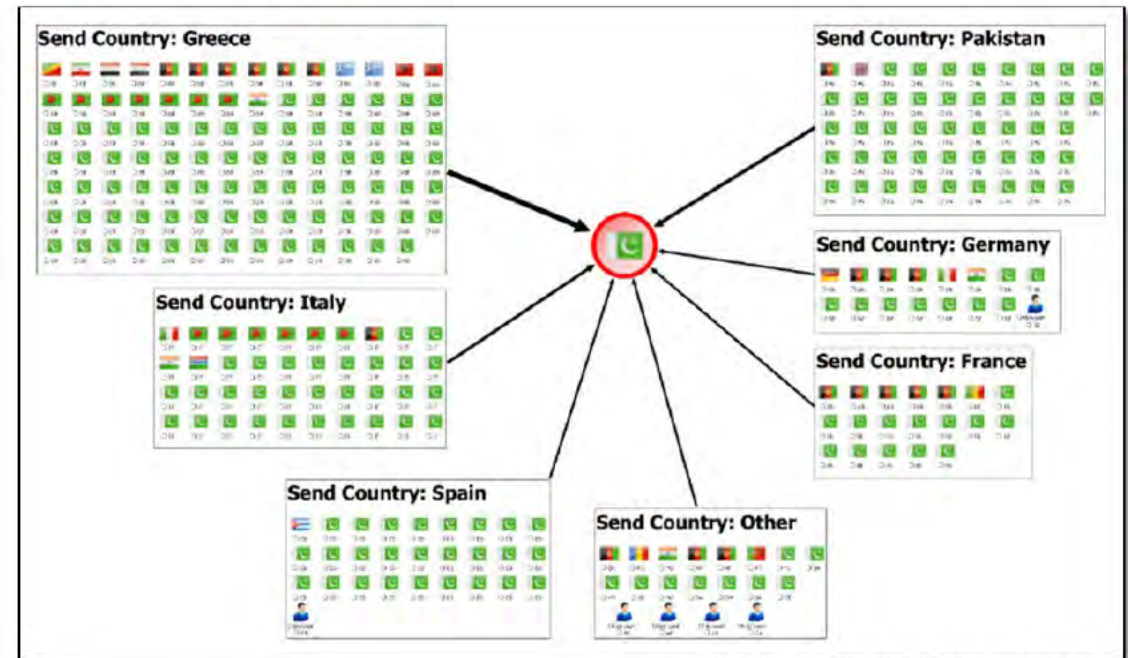
Consumers with migrant nationality (e.g., Afghanistan, Bangladesh, Pakistan, Syria, etc.) in Albania, Bulgaria, Croatia, Greece, Hungary, Macedonia, Romania, or Serbia receiving from 13 or more senders in 3 more countries in prior 65 days



Strategic Analysis from Typology Characteristics

ENTITY TYPE + GEOGRAPHY + DIRECTION + THRESHOLD + TIMEFRAME

Consumers with migrant nationality (e.g., Afghanistan, Bangladesh, Pakistan, Syria, etc.) in Albania, Bulgaria, Croatia, Greece, Hungary, Macedonia, Romania, or Serbia receiving from 13 or more senders in 3 more countries in prior 65 days



Intelligence-Driven Alerting (Tax Evasion)

- **Offshore Company Formation (OCF)** providers are firms which create legal entities, such as LLCs, on behalf of clients in a jurisdiction other than their clients' home country
- In theory, “offshore” can refer to any jurisdiction outside a client’s home country; in practice the term refers to countries which offer low or zero taxation and a degree of secrecy for foreign clients
- **It is not illegal to move money offshore or own an offshore entity** and offshore jurisdictions can be used for legitimate tax planning purposes
- However, **offshore companies are sometimes used to facilitate money laundering and tax evasion** and as such present a risk to the company
- In general, jurisdictions which market themselves on **financial secrecy** over tax advantage are considered the riskiest

Secrecy Jurisdiction: Nevis

The Caribbean island of Nevis, the autonomous partner of nearby St. Kitts, has been described in the British press as “the world’s most secretive offshore haven”. The country’s regulators keep no records of the beneficial ownership or assets of LLCs and the country requires the deposit of a \$100k bond in person to bring any legal proceedings. Nevis LLCs hold property and companies around the world and have been implicated in numerous financial scandals.

The Guardian



Intelligence-Driven Alerting (Tax Evasion)

- We identified 200 offshore company providers in high-risk jurisdictions and built a database of names, phone numbers, and email addresses.



advertised payment

made up a number

ATLANTIC INTERNATIONAL BANK

INVITES you to our **International Banking Fair**
Adding Value to Your Success!

ATLANTIC International Corp. Services Ltd.

Here's what you can expect at the fair:

- Open US Dollar Accounts
- Apply for US Dollar Loans
- Form Local & International Business Companies
- Register your Trademark
- Form a Trust
- Apply for QRP (Qualified Retired Persons) Status
- Attractive Properties for Sale
- Games & Bouncy House**
- General Information
- ...and more

Saturday, February 22nd
9 AM - 2 PM

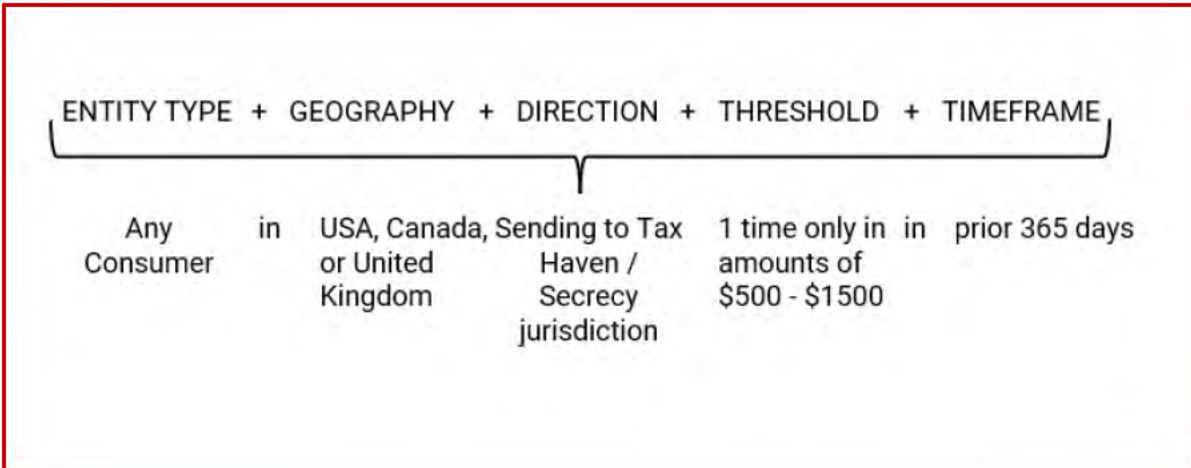
Cayo Welcome Center
San Ignacio Town

For more information call Amalia or Lovelia at 824-2634 OR 223-5318



Intelligence-Driven Alerting (Tax Evasion)

- We identified 200 offshore company providers in high-risk jurisdictions and built up a database of names, phone numbers, and addresses associated with those firms
 - The FIU identified several OFC firms that advertised Western Union as an accepted method of payment
 - Firms advertising payment by WU made up a relatively small percentage of the total number



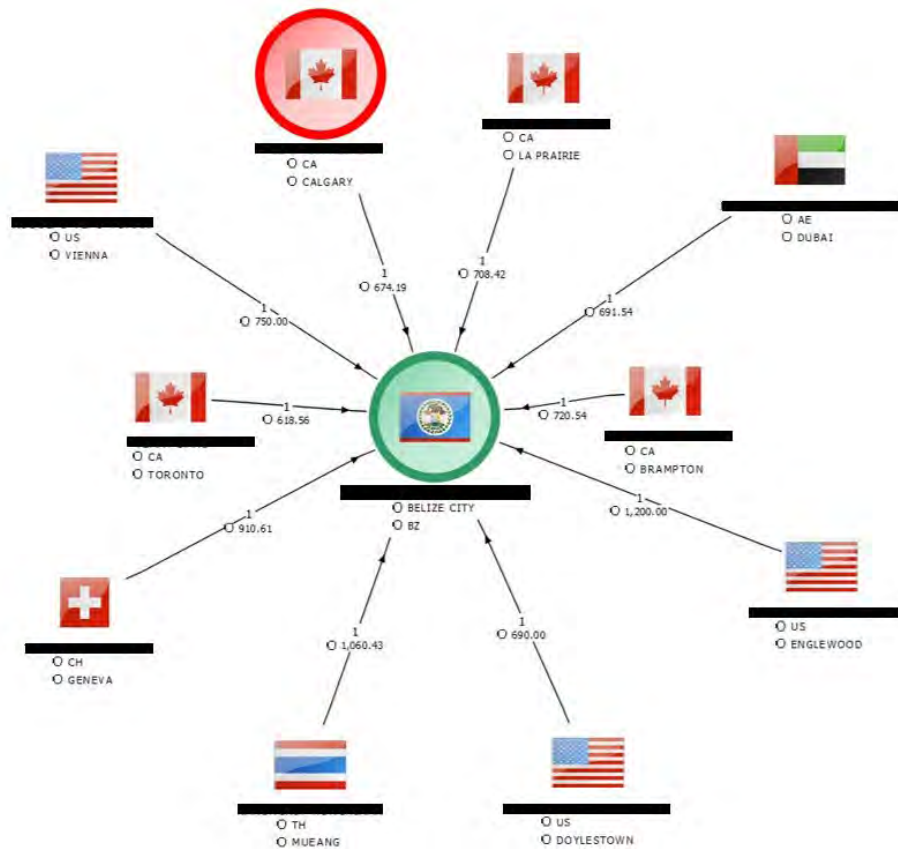
Intelligence-Driven Alerting (Tax Evasion)

- The FIU developed a pattern-based approach using a set of transaction-based criteria to target payees potentially receiving for company formation
- **We identified a few hundred US-based senders matching the pattern**
 - Globally, top send countries were the US, Russia and France
 - The most popular pay country for US-based senders was Panama
 - The average transaction amount was \$1,025





Intelligence-Driven Alerting (Tax Evasion)



When contacted by WU FIU, one sender indicated the payments were for **company formation** and pointed us to this site.

A & P INTERTRUST & CORPORATION
Makes Starting Business Easy & Convenient

Toll Free: 1.866.20.TRUST
Phone: +1.905.762.0703
Now serving over 10,000 clients

[Site Map](#) | [Contact Us](#)
[Eng](#) | [Rus](#)

HOME

CANADA INCORPORATION

US INCORPORATION

OFFSHORE COMPANY

OUR COMPANY

Innovative Way to Start Business

Belize IBC - \$650 ~~\$950~~
Courier delivery is included. Assistance with bank account available. Save \$300 Exp. Feb 9/19 [Details](#)

Canada Incorporation - \$75
Get your company incorporated and ready for business in 2 bus. hours. Order online. Over 10,000 satisfied clients. [Details](#)

Canada Company for Non-Residents
Registration of Limited Partnership. No corporate tax. Order online. In 1 day [Details](#)

A & P Intertrust Corporation forms legal entities in [Canada](#), [US](#), [Belize](#), [BVI](#), [Nevis](#) and [Panama](#). We also assist our clients with opening bank accounts in [Canada](#), [US](#), [Latvia](#), [St. Vincent](#), [Singapore](#), [Cyprus](#), [Belize](#), [Seychelles](#) and [UK](#) and merchant accounts in [Canada](#) and [Belize](#).

Company in Canada

[NUANS Report - \\$24](#)
[Incorporation - \\$75](#)
[For Non-Residents - \\$1,990](#)
[Business Name - \\$39](#)

Company in USA

[Arkansas LLC - \\$660](#)
[Colorado LLC - \\$660](#)
[Delaware LLC - \\$760](#)
[New Hampshire LLC - \\$660](#)

Offshore Company

[Belize IBC - \\$990 \\$650](#)
[BVI IBC - \\$1,350](#)
[Nevis LLC - \\$1,000 \\$900](#)
[Panama IBC - \\$1,400 \\$900](#)

As a long-term accredited business with the [Better Business Bureau](#) and a member of the [Canadian Federation of Independent Business](#) we offer highly professional and reliable service for over 10,000 clients located in more than 50 countries.

Our company is the fastest provider in the industry. We incorporate [Canadian companies](#) in one to five business hour, [US companies](#) in one business day and [offshore companies](#) usually the next

Western Union | Financial Intelligence Unit

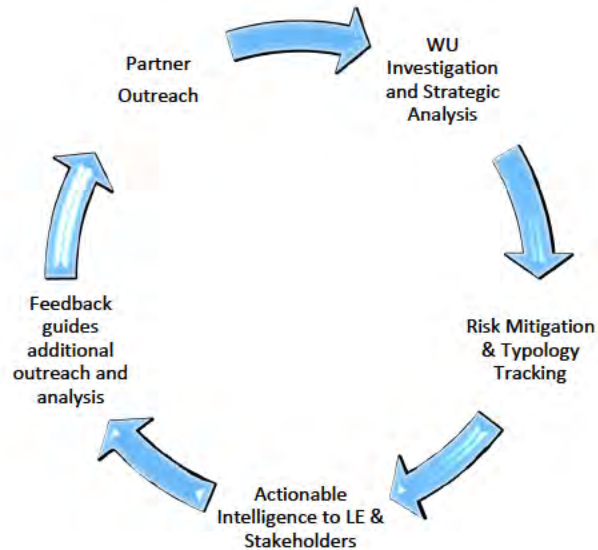
28

Western Union Confidential | ©2023 Western Union Holdings, Inc. All rights reserved

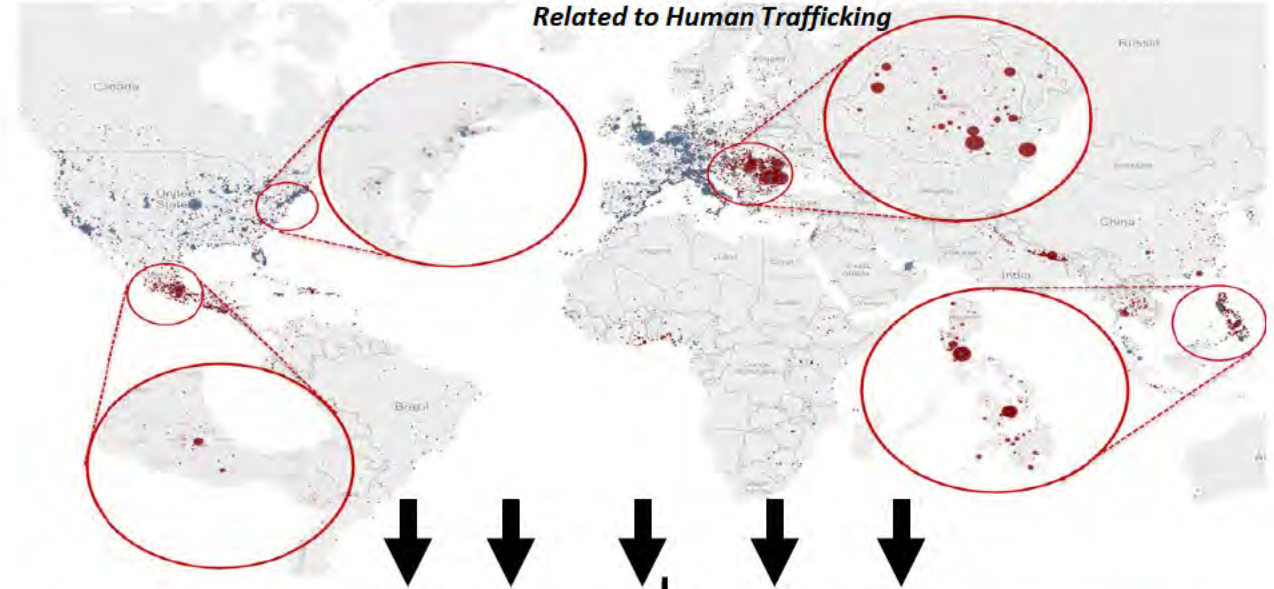
Outcomes of Intelligence Driven Work

Thousands of Compliance investigations and numerous strategic intelligence projects completed annually, providing for a comprehensive, integrated real-time view of typology risk

- Drug Trafficking
- Human Smuggling
- Human Trafficking
- Terror Finance
- Child Exploitation
- Counterfeit Goods



Example of Financial Intelligence Observations with Transactions Potentially Related to Human Trafficking



New and Enhanced Transaction Controls and other Risk Mitigations

RTRA

Training and Investigative Guidance to the Compliance Workforce

Interdictions

SAR / STR Filings (Intel Back to LE)

Inform Key Business Decisions

Outreach Opportunities

Western Union Confidential | ©2023 Western Union Holdings, Inc. All rights reserved



Thank You



From: [REDACTED]@fbi.gov]
Sent: 1/15/2021 12:40:26 PM
To: [REDACTED]@bofa.com]; [REDACTED]@bofa.com]
Subject: Re: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

As always, thanks for the very quick communication/response over the phone this morning.

To recap our morning call, we [FBI] are prepared to action **[immediately]** the following thresholds:

- CTD/SPES/SEU is interested in all financial relationships that meet the following thresholds:
 - Customers confirmed as transacting, either through bank account [debit card] or credit card, Washington D.C. purchases between 1/5/21 and 1/6/21, with the additional [identifying] targeting thresholds:
 - Purchases made for hotel/airbnb RSVPs in the DMV area [the day before and during Inauguration Day] -----since 1/6/21.
 - ANY historical purchase [going back 6 months generally, for weapons or weapons related-vendor purchases].
 - Secondly, purchases made for returns to Washington, D.C. and the surrounding DMV area:
 - With Airline travel to DMV area for Inauguration Day
 - With no identified airline purchases for the DMV.**

** - SEU intends to capture, with its FI-partner concurrence, all customers who might be more strategic in carrying out attacks related to CTD interests; travel with weapons by vehicle and [not by] air, given the current threat and aftermath of the 6 Jan Capitol building incidents. The intention by SEU is to identify all potential networks of threats vs. individual threats to Inauguration Day and beyond.

[REDACTED]

From: [REDACTED] (FBI)
Sent: Friday, January 15, 2021 9:56 AM
To: [REDACTED]@bofa.com>; [REDACTED]@bofa.com>
Subject: upcoming SAR product idea/brainstorming and check-in with you both

[REDACTED]

Ahead of next week's inauguration, I wanted to touch base on a couple things.

Message

From: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov]
Sent: 4/16/2021 9:55:51 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7 [REDACTED]; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED].unionbank.com]; [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED].unionbank.com]; [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED].unionbank.com]
Subject: [External] RE: [REDACTED] selectors provided for SAR purposes only

***** External email: Please be careful when opening attachments or clicking links. *****

[REDACTED]

This may turn into a code red, but in the interim we wanted to push you selectors we confirmed on the ops side. So yes, for now, we have not confirmed we have GJS' teed up for all results from our normal "code red" protocol --but we will take any SARs you decide to file on.

If this turns into a code red over the weekend, you will hear it from me first.

Hope this helps.

Hope you all have a safe weekend with your families.

-Pete

From: [REDACTED]@us.mufg.jp>
Sent: Friday, April 16, 2021 5:46 PM
To: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov>; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov>
Cc: [REDACTED]@unionbank.com>; [REDACTED]@unionbank.com>; [REDACTED]@unionbank.com>
Subject: [EXTERNAL EMAIL] - RE: [REDACTED] - selectors provided for SAR purposes only

Hi Pete, happy Friday. Does this mean you are not looking for a response from us except to notify you if we happen to file something based on this?

From: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov]
Sent: Friday, April 16, 2021 5:19 PM
To: [REDACTED] (CTD) (FBI)
Subject: [External] [REDACTED] - selectors provided for SAR purposes only

***** External email: Please be careful when opening attachments or clicking links. *****

Folks,

The name and selectors linked to the [REDACTED] are being provided to you below for your discretionary SAR purposes only.

At this time, this is NOT being treated as a Code RED.

-Pete

Name: [REDACTED]
DOB: [REDACTED]
SS#: [REDACTED]
Address: [REDACTED]
Driver's License: [REDACTED]

Peter Sullivan
Senior Private Sector Partner Outreach
Strategic Partner Engagement Section

[REDACTED]

This email is confidential, and your receipt of it is subject to the recipient terms appearing at: <https://www.mufgamericas.com/emailrecipientterms> . If you have received this email in error, please inform us by email reply and then delete the message. Any use of this email inconsistent with those terms is strictly prohibited.

Message

From: Peter Sullivan [REDACTED]@fbi.gov]
Sent: 26/05/2021 19:38:48
To: [REDACTED]@sc.com
Subject: [External] Fw: Equity Check - [REDACTED]
Sensitivity: Company Confidential

ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails.

[REDACTED]

Hope all is well. I wanted to revisit our conversation on your two cents if we could discuss next steps to try and get more information on name matches we would often get with yours or other multinational banking partners heavy on third party activity and name matches only. I am here until 5:30pm today as well as the rest of the week. You know you can reach out to me on my cell for this or anything else you need, always.

Thanks very much for your time.

Pete

Peter Sullivan
 Senior Private Sector Partner Outreach
 Strategic Partner Engagement Section
 [REDACTED]

From: [REDACTED]@sc.com>
Sent: Monday, May 24, 2021 4:04 PM
To: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov>; [REDACTED] (CTD) (FBI) [REDACTED]@fbi.gov>
Cc: [REDACTED]@sc.com>; [REDACTED]@sc.com>; [REDACTED]@sc.com>; MajorCase, FCCInvestigations <FCCInvestigations.MajorCase@sc.com>
Subject: [EXTERNAL EMAIL] - RE: Equity Check - [REDACTED]

CONFIDENTIAL

Hi Pete,

SC NY has conducted transactional searches based on your inquiry. We have identified transactions with an exact name match. If additional information is required, we ask that you send a subpoena.

Please do not hesitate to contact us if you have any questions.

Thank you

Best,

Strategic Partner Engagement Section



This email and any attachments are confidential and may also be privileged. If you are not the intended recipient, please delete all copies and notify the sender immediately. You may wish to refer to the incorporation details of Standard Chartered PLC, Standard Chartered Bank and their subsidiaries at <https://www.sc.com/en/our-locations>. Please refer to <https://www.sc.com/en/privacy-policy/> for Standard Chartered Bank's Privacy Policy.

Message

From: Peter Sullivan [REDACTED]@fbi.gov]
Sent: 26/05/2021 20:19:05
To: [REDACTED]@sc.com
Subject: [External] RE: Equity Check - [REDACTED]
Sensitivity: Company Confidential

ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails.

[REDACTED]

Thanks for the quick reply. Yes, would 4pm EST work? I could also do 10am EST.

And please by all means if you have compliance or someone else on the call, feel free to have a pre-call with me, I want to make sure at a minimum I am on the same page with you.

Pete

From: [REDACTED]@sc.com>
Sent: Wednesday, May 26, 2021 3:40 PM
To: Sullivan, Peter (CTD) (FBI) [REDACTED]@fbi.gov>
Subject: [EXTERNAL EMAIL] - RE: Equity Check - [REDACTED]
Sensitivity: Confidential

CONFIDENTIAL

Hi Pete,

Yes, thanks for reaching out, could I put something on the calendar for tomorrow?

[REDACTED]

From: Peter Sullivan [REDACTED]@fbi.gov>
Sent: Wednesday, May 26, 2021 3:39 PM
To: [REDACTED]@sc.com>
Subject: [External] Fw: Equity Check - [REDACTED]
Sensitivity: Confidential

ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails.

[REDACTED]

Hope all is well. I wanted to revisit our conversation on your two cents if we could discuss next steps to try and get more information on name matches we would often get with yours or other multinational banking partners heavy on third party activity and name matches only. I am here until 5:30pm today as well as the rest of the week. You know you can reach out to me on my cell for this or anything else you need, always.

Message

From: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov]
Sent: 1/22/2021 8:59:18 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8e8f841dfd2045b19f036bc5396baab7-[REDACTED]; [REDACTED]@fincen.gov]; [REDACTED]@fincen.gov]
CC: [REDACTED] [/O=BTMU/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]unionbank.com]
Subject: [External] RE: Major DC Transportation Vendor Lists.xlsx

External email: Please be careful when opening attachments or clicking links.

[REDACTED] this is terrific. Thank you both.

From: [REDACTED]@us.mufg.jp>
Sent: Friday, January 22, 2021 1:48 PM
To: [REDACTED]@fincen.gov>; [REDACTED]@fincen.gov>; Tirol, AnnaLou [SES] [REDACTED]@fincen.gov>
Cc: [REDACTED]@unionbank.com>
Subject: [EXTERNAL] Major DC Transportation Vendor Lists.xlsx

FinCEN colleagues, attached is a compilation of vendors at the 3 major DMV airports (Reagan, Dulles, BWI), Union Station (rail), and Bus Stops. Feel free to share.

This email is confidential, and your receipt of it is subject to the recipient terms appearing at: <https://hyperlink.services.treasury.gov/agency.fincen?origin=https://www.mufgamericas.com/emailrecipientterms> . If you have received this email in error, please inform us by email reply and then delete the message. Any use of this email inconsistent with those terms is strictly prohibited.

From: [REDACTED]
Sent: Friday, January 22, 2021 4:03 PM
To: [REDACTED]@keybank.com' [REDACTED]@keybank.com>; [REDACTED]@westernunion.com'
[REDACTED]@westernunion.com>; [REDACTED]@westernunion.com' [REDACTED]@westernunion.com>;
[REDACTED]@westernunion.com' [REDACTED]@westernunion.com>; [REDACTED]@us.hsbc.com'
[REDACTED]@us.hsbc.com>; [REDACTED]@us.hsbc.com' [REDACTED]@us.hsbc.com>;
[REDACTED]@bofa.com' [REDACTED]@bofa.com>; [REDACTED]@bofa.com'
[REDACTED]@bofa.com>; [REDACTED]@bofa.com' [REDACTED]@bofa.com>; [REDACTED]@santander.us'
[REDACTED]@santander.us>; [REDACTED]@santander.us' [REDACTED]@santander.us>; [REDACTED]@santander.us'
[REDACTED]@santander.us>; [REDACTED]@wellsfargo.com' [REDACTED]@wellsfargo.com>;
[REDACTED]@wellsfargo.com' [REDACTED]@wellsfargo.com>; [REDACTED]@wellsfargo.com'
[REDACTED]@wellsfargo.com>; [REDACTED]@us.mufg.jp' [REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp' [REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@unionbank.com' [REDACTED]@unionbank.com>;
[REDACTED]@unionbank.com' [REDACTED]@unionbank.com>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp' [REDACTED]@us.mufg.jp>; [REDACTED]@sc.com'
[REDACTED]@sc.com>; [REDACTED]@sc.com' [REDACTED]@sc.com>; [REDACTED]@sc.com'
[REDACTED]@sc.com>; [REDACTED]@citi.com' [REDACTED]@citi.com>; [REDACTED]@citi.com'
[REDACTED]@citi.com>; [REDACTED]@citi.com' [REDACTED]@citi.com>; [REDACTED]@paypal.com'
[REDACTED]@paypal.com>; [REDACTED]@paypal.com' [REDACTED]@paypal.com>; [REDACTED]@paypal.com'
[REDACTED]@paypal.com>; [REDACTED]@jpmorgan.com' [REDACTED]@jpmorgan.com>;
[REDACTED]@jpmchase.com' [REDACTED]@jpmchase.com>
Cc: Tirol, AnnaLou [SES] [REDACTED]@fincen.gov>; [REDACTED]@fincen.gov>; [REDACTED]
[REDACTED]@fincen.gov>; [REDACTED]@fincen.gov>
Subject: RE: Capitol Riots

All,
With thanks to our MUFG colleagues, please find attached a compilation of vendors at the three major DMV-area airports, Union Station, and various bus stops.
Regards,
[REDACTED]

From: [REDACTED]
Sent: Tuesday, January 19, 2021 5:15 PM
To: [REDACTED]@keybank.com' [REDACTED]@keybank.com>; [REDACTED]@westernunion.com'
[REDACTED]@westernunion.com>; [REDACTED]@westernunion.com' [REDACTED]@westernunion.com>;
[REDACTED]@westernunion.com' [REDACTED]@westernunion.com>; [REDACTED]@us.hsbc.com'
[REDACTED]@us.hsbc.com>; [REDACTED]@us.hsbc.com' [REDACTED]@us.hsbc.com>;
[REDACTED]@bofa.com' [REDACTED]@bofa.com>; [REDACTED]@bofa.com'
[REDACTED]@bofa.com>; [REDACTED]@bofa.com' [REDACTED]@bofa.com>; [REDACTED]@santander.us'
[REDACTED]@santander.us>; [REDACTED]@santander.us' [REDACTED]@santander.us>; [REDACTED]@santander.us'
[REDACTED]@santander.us>; [REDACTED]@wellsfargo.com' [REDACTED]@wellsfargo.com>;
[REDACTED]@wellsfargo.com' [REDACTED]@wellsfargo.com>; [REDACTED]@wellsfargo.com'
[REDACTED]@wellsfargo.com>; [REDACTED]@us.mufg.jp' [REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp' [REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@unionbank.com' [REDACTED]@unionbank.com>;
[REDACTED]@unionbank.com' [REDACTED]@unionbank.com>; [REDACTED]@us.mufg.jp'
[REDACTED]@us.mufg.jp>; [REDACTED]@us.mufg.jp' [REDACTED]@us.mufg.jp>; [REDACTED]@sc.com'
[REDACTED]@sc.com>; [REDACTED]@sc.com' [REDACTED]@sc.com>; [REDACTED]@sc.com'
[REDACTED]@sc.com>; [REDACTED]@citi.com' [REDACTED]@citi.com>; [REDACTED]@citi.com'
[REDACTED]@citi.com>; [REDACTED]@citi.com' [REDACTED]@citi.com>; [REDACTED]@paypal.com'



Financial Crimes Enforcement Network
U.S. Department of the Treasury

Office of the Director

Washington, D.C. 20220

April 13, 2021

[REDACTED]
MUFG Bank, Ltd.

Via Email: [REDACTED]

Dear [REDACTED]

I am writing to express my gratitude to MUFG Bank for its collaborative efforts in working with the Financial Crimes Enforcement Network (FinCEN) and our law enforcement partners in the aftermath of the tragic events at the U.S. Capitol on January 6, 2021.

I am truly proud of the partnership that we formed as our organizations worked together in this unprecedented time of crisis. We deeply appreciate the timely and proactive attention of your team during this period – many times on short-notice, late into evenings, or over weekends – to respond to this challenge and to share information and work with law enforcement to follow leads and identify potential threats.

I hope that this letter serves to underscore the importance of your institution's anti-money laundering efforts and reminds everyone contributing to your institution's program – particularly those staff members who work closely with FinCEN and our law enforcement partners to respond to crisis events – that their efforts truly make a difference to our national security each and every day.

Sincerely,

Michael Mosier
Acting Director

Enclosure

cc: [REDACTED]

Brick & Mortar to Bits & Bytes: Adapting the U.S. AML/CFT Regime for Digital Identity

Bank Secrecy Act Advisory Group (BSAAG)
FinTech/RegTech Working Group
Digital ID/eKYC Workstream¹

Table of Contents

- I. Introduction: what does “digital identity” mean for AML/CFT?
 - A. The Vision and the Reality

The Financial Action Task Force (FATF) *Guidance on Digital Identity* (FATF Guidance) envisions “Digital ID systems” as using “electronic means to assert and prove a person’s official identity online (digital) and/or in-person environments at various assurance levels.”² However, the FATF Guidance acknowledges that “[n]ot all elements of a digital ID system are necessarily digital. Some elements of the identity proofing and enrolment component can be either digital or physical (documentary), or a combination, but binding, credentialing, and authentication ... must be digital.”³ Written for a broad audience of government authorities, regulated entities, and digital ID service providers from jurisdictions of varying political realities and stages of development in their Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT) regimes, the FATF Guidance’s primary focus is primarily on true, end-to-end national digital ID systems.⁴

The reality is that most financial institutions⁵ currently inhabit, and will likely continue to inhabit, a world straddling the paper and plastic identification of the past and the aspirations of end-to-end digital identification systems that the FATF envisions. The range of practices used to satisfy Bank Secrecy Act (BSA) obligations in the U.S. vary widely among online banks or neobanks, fintechs, and traditional financial institutions. But overarching the financial industry and its business models is the reality that there is deep political and cultural skepticism of, or even hostility to, a national ID system in the U.S.

Therefore, this Working Group (Group) acknowledges the likelihood that a fully realized national digital ID system will face unique political challenges and structural hurdles in the U.S.

¹ This draft whitepaper was drafted for review and presentation at the May 2021 BSAAG meeting. The views expressed in this document are those of the Workstream as contributed and agreed by workstream members, and not those of their employers.

² FATF, *Guidance on Digital Identity* ¶57 (Mar. 2020).

³ *Id.* at ¶59 (emphasis added).

⁴ *Id.* at ¶58.

⁵ For purposes of this paper, “financial institution” encompasses those businesses identified in 31 CFR 1010.100(t), including banks, broker-dealers, money service businesses, casinos, and mutual funds, among others.

that it would not in many other countries⁶ and that the financial industry will likely be living in that interstitial state of paper, plastic (i.e., “analog”), and “digital ID” for the foreseeable future. “Digital ID” in the U.S. will more likely evolve to include a mosaic of tools and services offered through Federal and State governments, digital ID vendors, credit ratings agencies and other data providers, and financial institutions themselves. As the mosaic evolves and financial institutions face continued commercial pressure to provide their customers with the kind of seamless online services they are already accustomed to in other service sectors (and countries), financial institutions will only increasingly identify and verify their customers through digital means, but with AML legal and regulatory requirements that were designed for analog identification processes undertaken by financial institution in their brick-and-mortar, not online, forms.

In this context then and utilizing FATF’s terminology, this paper takes the functional view that “digital identity” or “digital ID” refers simply to:

electronic means [that can be used] to assert and prove a person’s official identity online (digital) and/or [within] in-person environments at various assurance levels.”

– FATF Guidance at ¶57.

This formulation acknowledges the realities of interstitial state between analog and digital identification our “mosaic” but allows us to chart a course for U.S. financial institutions who must continue to engage their customers in an increasingly digital world. It also encourages U.S. financial institutions to engage a key recommendation of the FATF Guidance to utilize the “anti-fraud and cyber security processes” already in common use by U.S. financial institutions, such as geolocation, IP addresses, and biometrics,⁷ “to support digital identity proofing and/or authentication for AML/CFT efforts (customer identification/verification at on-boarding and

⁶ For example, Singapore’s [myInfo/SingPass](#), Estonia’s national [ID-cards](#), or India’s [Aadhaar number](#) are all national, federated digital ID systems that may be used for CDD and digital onboarding. Others, like Sweden’s [BankID](#) have sanctioned specific digital identity services for financial services onboarding.

⁷ The FATF defines three distinct types of “biometrics”:

- biophysical biometrics: attributes, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static
- biomechanical biometrics: attributes, such as keystroke mechanics, are the product of unique interactions of an individual’s muscles, skeletal system, and nervous system.
- behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, consist of an individual’s various patterns of movement and usage in geospatial temporal data streams, and include, e.g., an individual’s email or text message patterns, file access log, mobile phone usage, and geolocation patterns.

FATF Guidance at ¶57.

ongoing due diligence and transaction monitoring)” even absent end-to-end, state-sponsored or authorized digital identity systems.⁸

B. Objectives

First, the U.S. AML regime should create the conditions for digital ID practices to take root in the U.S. financial industry by expanding and updating the existing customer identification program (CIP) rules for the different types of BSA-regulated institutions.⁹ The current CIP Rules are nearly 20 years old, were primarily designed for in-person identification in brick-and-mortar branches, and are now quickly being dated by intervening advances in technology—smartphones, biometrics, artificial intelligence, etc. While the CIP Rules wisely preserved some flexibility, they still do not provide financial institutions sufficient regulatory certainty or the permission necessary to ensure digital ID elements can be included effectively in CIP and Know-Your-Customer (KYC) processes, especially in the way that the FATF is now advocating. Therefore, this paper recommends specific regulatory action, particularly in the CIP Rules, and interpretation that can begin to create the conditions and flexibility under which financial institutions may fully utilize digital ID’s benefits, while mitigating its potential risks and better combating money laundering, terrorist financing, weapons proliferation, and other illicit transactions. For instance, the paper suggests revisiting the presumption in the CIP Rules that online identification and verification is inherently riskier, the requirement for banks to obtain the full nine digits of the Social Security Number (SSN), enhancing examiner guidance on new digital identification elements, and exploring usage of alternative identifying numbers, such as driver’s license numbers as mobile driver’s license (mDL) and state identification ecosystems mature and provide higher levels of assurance.

Second, the U.S. AML regime should incorporate more “optionality”—i.e., having more options, but not necessarily obligations—into CIP and customer due diligence (CDD) processes. Greater optionality would allow financial institutions to utilize the variety of “digital signals” inherent in a predominantly digital customer relationship—e.g., IP addresses, geolocation, biometrics, etc.—to contribute to a financial institution’s understanding of its customer for KYC purposes. In their optionality, greater utilization of digital signals would not be mandatory for financial institutions—those able to manage their AML/CFT risks with traditional CIP and KYC processes would be able to satisfy their regulatory obligations without incorporating or relying on digital signals. However, financial institutions with digital relationships would be able to incorporate and rely on those signals in addition to or in lieu of some traditional KYC elements. As discussed in more depth in section II.D, this could include substituting the traditionally required

⁸ *Id.* at Glossary, p. 101.

⁹ See 31 CFR 1020.220 (banks); 31 CFR 1023.220 (broker-dealers); 31 CFR 1024.220 (mutual funds); 31 CFR §1026.220 (futures commission merchants and introducing brokers) (together, the CIP Rules). Other BSA-regulated financial institutions, including casinos/card clubs, money service businesses, insurance companies, dealers in precious metals/stones/jewels, credit card systems, loan or finance companies, and housing government sponsored enterprises, do not have a customer identification program requirement; however, they may have requirements to either identify a customer or verify a customer’s identity for certain transactions.

CIP elements of Social Security Number (SSN) and address, either with sufficient assurance levels obtained with other digital elements or at lower risk levels, especially when considering financial inclusion policy rationales.

Third, financial institutions and regulators should continue to define the benefits of and rationales for digital identity, but especially its potential to both enhance the effectiveness of AML

[o]fficial identity that can change over time as the identified individual develops a progressively more robust digital footprint that provides an increasing number of attributes and/or authenticators that can be verified against an increasing number and range of sources.

– FATF Guidance at p. 104.

compliance and increase financial inclusion.

Fourth, this paper seeks to expand on the concept of “progressive identity” explored in the FATF Guidance. As defined by the FATF, “progressive identity” is an:

Progressive identity recognizes that digital ID is not simply a new method for static identification and verification, but can facilitate the “customer journey” through which customers increase their digital footprint and traditionally underrepresented customers can seek more and varied services as they develop a more robust digital footprint with a financial institution, all while providing financial institutions tools that could be used to better understand the nature and purpose of the customer relationship. By utilizing progressive assurance levels, financial institutions should be able to offer limited, lower-risk products and services for customers in the initial steps of that “journey” relying on simplified due diligence frameworks already sanctioned by FATF, only requiring enhanced assurance if customers wish to increase the depth and complexity of their relationships with the financial institution.

These approaches to digital ID have potentially profound policy implications and benefits. Expanding CIP elements could enhance the security of our identification ecosystem by reducing reliance on the already highly compromised SSN. Progressive identity would help financial institutions address financial inclusion, allowing and encouraging them to take on customers they have in the past overlooked or who themselves have been deterred from even seeking services from financial institutions (and make that onboarding process easier for the customer), while also focusing financial institutions on behavioral risk rather than cruder risk proxies like geography or product type. Focusing on behavioral customer risk and leveraging the digital signals that many financial institutions are already using for their fraud and cyber-security processes to mitigate operational risk would allow financial institutions to refocus the massive human resources currently allocated to KYC and train them on more effective techniques for proactively detecting financial crime.

dealers, and other financial institutions” through “the mail, electronically, or in other situations where the accountholder is not physically present at the financial institution”.¹² Those numbers have only grown since 2001 for mutual funds and broker-dealers, but also for banks for whom it was less customary to open accounts remotely in 2001. This concern led in part to the flexibility built into particularly the non-documentary verification option of the CIP Rules and informed the credit card exemption,¹³ which explicitly granted banks the ability to obtain identifying information from third-party sources prior to extending credit in large part because the credit card banks’ business model entailed opening accounts remotely by telephone or at third-party points of sale.¹⁴ Just as credit card banks’ business model in 2003 was predicated on remote, non-face-to-face onboarding, many financial institutions have had their business models disrupted by technology and are now heavily reliant on their ability to conduct non-face-to-face onboarding through smartphones and other electronic devices.

B. Clarify that that non-face-to-face identification is not always inherently riskier than face-to-face identification

The language of CIP Rules suggest that a customer opening an “account without appearing in person” is a “circumstance[] that increases the risk that the financial institution will be unable to verify the true identity of a customer through documents.”¹⁵ That presumption, and its reflection in the FFIEC’s BSA/AML Manual¹⁶ (FFIEC Manual), should be reassessed in light of the FATF’s observation that non-face-to-face identification “may be standard risk, and may even be lower risk,”¹⁷ the MOBILE Act’s Congressional sanction of digitally transmitted ID documentation, the current verification practices for many financial institutions operating online, and the state of the technology itself that has evolved well beyond what was available in 2003 when the CIP rule was promulgated.

¹² H.R. Rep. No. 107-250, pt. 1, at 63 (2001) (discussing the Financial Anti-Terrorism Act of 2001, which was later consolidated in the USA PATRIOT Act).

¹³ 31 CFR §1020.220(a)(2)(i)(C) (“In connection with a customer who opens a credit card account, a bank may obtain the identifying information about a customer required under paragraph (a)(2)(i)(A) by acquiring it from a third-party source prior to extending credit to the customer”).

¹⁴ Final Rule, *Customer Identification Programs for Banks, et al.*, 68 FR 25089, 25097 (2003) (citing H.R. Rep. No. 107-250).

¹⁵ 31 CFR §1020.220(a)(2)(ii)(B)(2) (bank); 31 CFR §1023.220(a)(2)(ii)(B)(2) (broker-dealers); 31 CFR 1024.220(a)(2)(ii)(B)(2) (mutual funds); 31 CFR §1026.220(a)(2)(ii)(B)(2) (futures commission merchants and introducing brokers).

¹⁶ Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual, Customer Identification Program* at 5 (2021).

¹⁷ FATF Guidance at ¶13; see also id. at ¶125 (“If, as a matter of internal policy or practice, non-face-to-face business relationships or transactions are always classified as high-risk, [regulated entities should] consider reviewing and revising those policies to take into account that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower-risk”).

Where in 2003 a financial institution might have only the identification documentation and their impressions of an in-person account opening, it now may have more identification and verification data points from a customer relationship initiated online than in-person. In addition to non-documentary verification methods contemplated at the time of the CIP Rules' adoption, facial recognition techniques can now compare the government-issued photo ID document with real-time video calls or video-selfies, effectively replacing human vision with a computer's and establishing confidence that the individual behind the device during onboarding is in fact the onboarded personality.¹⁸ In real-time, financial institutions are now capable of: verifying that the information provided by the prospective customer matches the government-issued photo ID document scanned by the device; validating the authenticity of the document and device via third-party software and mobile applications; and confirming that the photo on the document matches the individual's facial biometric as presented through the device which can be recorded in the customer's KYC file.

Though the ID document may be transmitted digitally and the account opening conducted "without appearing in person," today's remote digital verification of ID documents may in fact pose fewer risks than an in-person identification and verification that does not also use these techniques. The use of the biometric checks and specially trained screeners for inconclusive digital results adds an additional layer of protection against stolen IDs and impersonation attacks that can meet or exceed the reliability of traditional face-to-face verification. Even setting aside the potential foibles of human judgment in an in-person visual identification, an online onboarding simply captures more data by which to understand the customer, such as email address, device information, IP address, and geo-location, and allows the financial institution to cross-reference those data points to existing databases and form a more holistic view of the customer.

As larger scale reform for the CIP Rules is worked through, regulators could also address this point for examiners in the FFIEC Manual and/or for financial institutions through FAQs clarifying that the CIP Rules' presumption here is limited to situations where, at the time the rules were crafted, there would have been no reliable way to digitally convey documentary identification such as a driver's license and acknowledge that, today, there are viable and secure ways to convey and verify that documentation remotely.

- C. In the near-term, explicitly permit banks and other financial institutions to collect the "last-four" of the SSN with adequate verification and retention of the "full-nine"

Truncation of the SSN has become a standard information security practice in different areas of society.¹⁹ However, the bank CIP Rule alone explicitly requires that the four elements of

¹⁸ Importantly and as discussed below, we must be critical of and continue to assess and improve technologies like facial recognition, which have thus far proven less effective at recognizing, for instance, darker skin tones.

¹⁹ See, e.g., Internal Revenue Service, *Use of Truncated Taxpayer Identification Numbers on Forms W-2, Wage and Tax Statement, Furnished to Employees*, 84 F.R. 31717 (2019) (permitting employers to print only the last four

II. Modernize the CIP Rules to Adapt to Evolving Digital Identification Practices

As public and private stakeholders provide new tools for digital identification and verification, the U.S. AML regime should be prepared to ingest them and acknowledge the changed landscape and expectations of cybersecurity.

- A. The Customer Identification Program rules were built to last and adapt but were still created primarily for brick-and-mortar relationships.

The different iterations of the BSA's CIP Rules provide inherent flexibility, both in their fundamental requirement simply to have procedures that "enable [the formation of] a reasonable belief that [the financial institution] knows the true identity of each customer" and the ability to obtain "documentary" or "non-documentary" verification—itself a version of the "optionality" concept that this paper advocates expanding. The rules do not absolutely require the presentation of government-issued identification, mandate in-person presentation of documentation, or even require an identification photograph.¹⁰

For example, the CIP Rules arguably provide sufficient flexibility for the growing practice of accepting a digitized transmission of a driver's license, which is further supported by 2018's MOBILE Act.¹¹ That Act allows financial institutions to accept and record information from a scanned driver's license or personal identification card to verify the authenticity of the identification and the identity of an individual requesting to open an account or obtain a financial product or service. However, other aspects of the CIP Rules, such as requiring banks to collect identification data "from the customer" or the apparent presumption that non-face-to-face identification is inherently riskier than in-person identification, undermine some of that flexibility. These limitations are inconsistent with the MOBILE Act's intent to encourage the digital delivery of financial services to address increasing mobility and lack of fixed addresses in the population, consumer expectations for digital products and services, and the unfortunate reality that face-to-face identification requirements also may raise health and safety risks as during the COVID-19 pandemic.

Though the CIP Rules were prescient in utilizing both documentary and non-documentary verification methods, it is worth considering whether they can be updated or clarified to reflect the reality that online relationships and the technologies that manage those relationships have only become more prevalent across all BSA-regulated financial institution types and forced many to rely increasingly on non-documentary identification and verification. Even in 2001, Congress recognized that the fact that "[m]illions of Americans open accounts at mutual funds, broker-

¹⁰ See, e.g., 31 CFR 1020.220 ("documents may include... [f]or an individual, an unexpired government-issued identification").

¹¹ The Making Online Banking Initiation Legal and Easy [MOBILE] Act (enacted as Section 213 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018).

CIP, including the SSN, be collected “from the customer,” which banks and their examiners commonly read as collecting the full-nine digits directly “from the customer.” Though this requirement is only explicitly present in the bank CIP Rule, this group understands anecdotally that other financial institutions commonly understand it to be a requirement in their respective industries.²⁰ In any event, however, it is now common practice for some traditional financial institutions and certainly for fintechs typically regulated as MSBs to collect only the “last four” digits of the TIN/SSN “from the customer” when establishing a business relationship online and then verify and/or collect the remainder from a credit rating agency or other authorized third-party that can match the customer to the partial TIN/SSN (in which case, the full-nine digit SSN is never transmitted). Allowing the collection of the last-four digits of the SSN, which are its most unique numbers, while ensuring collection of the full- nine from a third party would comport not only with better information security practices, but also with consumer expectations and wariness in using the SSN at all.

Even though obtaining the last-four digits is still susceptible to identity theft because SSNs are so widely available and because the last-four digits are the most unique, the use of the last-four digits reduces the data security and privacy risks in acquiring and transmitting the full-nine digits. As a matter of industry practice, many financial institutions that collect the full-nine digits now send them to a credit reporting agency for verification purposes in any event. Sending only the last-four digits would therefore reduce data security and privacy risks while also being sufficient in most circumstances for identification and verification purposes—utilizing valid name, address, date of birth, and verifying the last-four digits against the full-nine presents low risk of misidentification. Banks or other financial institutions who may still collect the full-nine will also need to consider any other potential risks in larger scale adoption of last-four and establish clear guardrails for requiring the full-nine where a last-four method has failed. Fortunately, there is already a wealth of best practices and techniques from the large number of other financial institutions and vendors that have utilized these practices for some time already. Perhaps more important than the identity theft, data security, and privacy risks, is the possibility that requiring the full-nine in an online setting will likely discourage potential customers from opening bank accounts online because widely accepted and promoted data security practices suggest that provide the last-four whenever possible.²¹ Utilizing last-four would also have the knock-on effect

digits of the SSN on W-2 statements and noting the ability to identify individuals with last-four together with name and address).

²⁰ While the bank CIP Rule specifies that the four CIP elements must be collected “from *the* customer”, all the CIP Rules require their covered FIs’ CIP contain procedures that specify what identifying information must be obtained “from each customer”, followed in close proximity by the four CIP elements. This proximity may have led to a reading that the four element themselves must be “obtained from each customer.” The non-bank CIP Rules, however, only require the CIP to determine which elements must be collected “from each customer”, not that each element must be collected “from the customer,” and therefore may be more susceptible to clarification by FAQ.

²¹ See, e.g., Federal Trade Commission, [What to Know About Identity Theft](#) (suggesting consumers ask if they can only provide the last-four digits when asked for their SSN); American Association of Retired Persons, [Guard Your](#)

of streamlining collection of CIP information from beneficial owners and especially from corporate controls persons, who are sometimes reluctant to potentially compromise their own identity in service of their employer.

The OCC's recent Interpretive Letter 1175,²² permitting the requesting bank to use the last-four digits in a specific circumstance, may pave the way by confirming that "collecting partial TINs from customers does not present any additional risk of money laundering since [the requestor's operating subsidiary] will obtain the full TIN from a reliable third party source that will enable it to form a reasonable belief that it knows the true identify of its customer." Though the Interpretive Letter is limited to the facts presented by the requestor, its rationale should be more broadly accepted, if not encouraged, across the financial industry.

Wide-scale adoption of last-four may also be a relatively easy regulatory change to make outside of full-scale revision of the CIP Rules. First, regulators could issue a Frequently Asked Question (FAQ) clarifying that a customer providing their last-four digits and consent to collect their full-nine digits from an authorized third party is the equivalent of obtaining the full-nine digits directly "from the customer." Second, the "from the customer" language may be susceptible to carve out from the CIP Rules' exemptive relief provisions. Since the practice of collecting full-nine originates with the "from the customer" language of the Bank CIP Rule alone, it would not require a regulatory and AML risk analysis for all BSA-covered financial institutions. Third, the CIP Rule's exemptive relief provision authorizes the "appropriate Federal functional regulator, with the concurrence of the [Treasury] Secretary" to "exempt any bank or type of account from the requirements of this section" by simple order, provided that exemption is consistent with the purposes of the BSA, safe and sound banking, and other appropriate factors.²³ Though the credit card exemption was written into the regulation itself, the logic of its flexibility to account for the nuances of the commercial context and privacy expectations of customers at the time may also provide a guidepost for the rationale for a last-four exemption.

D. Look beyond the CIP Rules' "Core Four" as identifiers

The only identification elements that the USA PATRIOT Act (in amending the BSA) explicitly required for the identification and verification of accountholders were name and address²⁴—it did not explicitly mandate collecting or maintaining the SSN or date of birth. The USA PATRIOT Act also required the Secretary of the Treasury to "take into consideration the various types of accounts maintained by various types of financial institutions, the various methods of opening

Social Security Number (suggesting the protection of even the last-four by asking if a company can accept an alternative identifier).

²² Office of the Comptroller of the Currency, *Interpretive Letter #1175 re: Customer Identification Program Rule Exemption Request* (Nov. 16, 2020, published Dec. 2020).

²³ 31 CFR §1020.220(b).

²⁴ 31 U.S.C. §5318(l)(2)(B) ("maintaining records of the information used to verify a person's identity, including name, address, and other identifying information").

accounts, and the various types of identifying information available.”²⁵ Since there are now many more methods of opening accounts and types of identifying information available than there were in 2001 at the time of the USA PATRIOT Act’s passage and the implementing regulations for the CIP requirement in 2003, and the Anti-Money Laundering Act of 2020²⁶ (AML Act) is causing a broader reconsideration of the U.S. AML regime, this is an appropriate inflection point for Treasury to reconsider its CIP Rules. Assuming, however, that “name” is a fundamental requirement for identification and as a practical matter “date of birth” (or at least month and year of birth) may be a necessary identification element for OFAC screening purposes and possibly ensuring true matches in 314a or 314b requests, we should at least reconsider the SSN and address as absolutely required CIP elements and assess potential alternatives at this moment in the evolution of the BSA/AML regime. As discussed in more depth below, reconsidering whether alternative identification elements could substitute for identifying number and address could have important implications for the ability of financial institutions to utilize digital identity systems at the state level and address increasing concerns over financial inclusion for those who may lack fixed addresses or SSNs.

In addition, we should clarify and distinguish that identifiers may and sometimes should be different than the record-keeping requirements for customers. For instance, even if the SSN is not required as an identifier it is sometimes required for other regulatory purposes, such as tax reporting, and is often a helpful data point for law enforcement. Financial institutions could, however, still collect the SSN from credit reporting agencies for regulatory, tax, and record-keeping purposes, as well as assisting law enforcement.

1. Reduce the dependence on the SSN as an identifier and open the door to alternative identifying numbers

The deficiencies of the SSN from an identification, verification, authentication, and general cybersecurity perspective are well-documented. Requiring a new customer to provide an SSN in 2003 was much more valuable in authenticating that the customer was who s/he claimed to be because knowledge of one’s SSN was generally more private then and the numbers themselves had not been compromised the way many of them have been today.²⁷ Today, however, after so many large-scale data breaches and ready accessibility of SSNs from illicit brokers, the SSN is no longer as valuable particularly as an authenticator and, as discussed above, customers are increasingly wary of sharing it. Moving away from it as a required element of CIP and allowing other identification numbers in its place as long as they provide financial institutions that “reasonable belief” in the “true identity” of their customers would likely be beneficial not only for financial institutions’ identification purposes and fraud reduction, but also for customer privacy,

²⁵ *Id.*

²⁶ AML Act of 2020, H.R. 6395 (2021).

²⁷ See, e.g., The Better Identity Coalition, *Better Identity in America: A Blueprint for Policymakers* (July 2018) (advocating the cessation of using the SSN as an authenticator and limiting its use as an identifier).

information security, financial inclusion, and the health of the country's identity ecosystem.²⁸ Moreover, as discussed below, the Anti-Money Laundering Act of 2020 allows for the use of other potential identifying numbers in identifying beneficial owners of legal entities and even creates a new form of identifier to be issued by FinCEN, both of which may expand the identification landscape to broader sets of identifying numbers.

As the most common documentary identification and verification source for natural persons, driver's licenses and state-issued identification and their identification numbers are the prime candidate for expanding the "optionality" for identification number. Driver's license and state identification card numbers are themselves readily verifiable with credit ratings agencies and other providers, just as SSNs are. The widespread adoption of the more reliable REAL ID standard for driver's licenses and identification cards, which requires a thorough verification of the "Core Four" including the SSN itself by state government issuers,²⁹ will also make driver's licenses and identification card numbers more reliable identifiers generally. In addition, state mobile driver's licenses (mDLs) may be showing the most promise and progress as end-to-end digital identification systems—and may ultimately get more traction with a general public that has viewed Federal identification systems with skepticism and suspicion since the advent of the SSN itself.³⁰

Apple has been actively advancing the possibility of greater adoption and consistency of mDLs by announcing in June 2021 that iOS 15 would allow customers in participating states to add their drivers licenses or state IDs to its Wallet App.³¹ More recently, Apple has announced the initial wave of participating states and that the Transportation Security Administration (TSA) will enable their use at certain airport checkpoints.³² While Apple has promised privacy, concerns about the issue and potential inconsistencies across states and by government actors may

²⁸ National Institute of Standards and Technology, *Special Publication 800-63A Digital Identity Guidelines* §8.1.1 (June 2017) (noting that "[o]verreliance on the SSN can contribute to misuse and place the applicant at risk of harm, such as through identity theft", that "operational necessity" for use of the SSN can only be demonstrated by an inability to alter systems, processes, or forms due to cost or unacceptable levels of risk", and the federal agencies are required to "review any decision to collect SSN relative to their *obligation to reduce the collection and unnecessary use of the SSN as necessary*") (emphasis added).

²⁹ In this sense, REAL ID driver's licenses will essentially become derivative of SSN-based identification. However, to the extent that it may be carried out at more stringent assurance levels by state government actors, REAL IDs may help limit the use of the SSN in private-sector relationships.

³⁰ See, e.g., Thales Group, *Digital Driver's license-your ID in your smartphone* (detailing pilots in Idaho, Colorado, Maryland, and Washington, DC); Idemia & Arizona Department of Motor Vehicles, Treasury Department Virtual Policy Forum, *Spotlight Session: Mobile Driver's Licenses* (Feb. 2021).

³¹ Apple Inc., *Press Release: iOS 15 brings new ways to stay connected and powerful features* (June 7, 2021);

³² Apple Inc., *Press Release: Apple announces first states signed up to adopt driver's licenses and state IDs in Apple Wallet* (Sept. 1, 2021) (announcing Arizona, Connecticut, Georgia, Iowa, Kentucky, Maryland, Oklahoma, and Utah as among the first states to allow their mDLs in Apple Wallet).

“acceptable identification documents,” while collecting the TIN for recordkeeping purposes from third-party services and eventually via APIs with the government issuing authorities.

To further promote financial inclusion, financial institutions, regulators, and law enforcement should also consider whether alternative identifying numbers could be used at lower assurance levels for correspondingly lower dollar, limited service accounts even without a record-keeping requirement for an SSN.³⁶ As discussed in more depth below, in digital or predominantly digital relationships, the digital signals from a customer that a financial institution collects during the customer lifecycle may themselves add to the level of identity assurance over time, or conversely, customer account activity and/or additional product usage may trigger the need for increased assurances. In addition to promoting financial inclusion and equity, such an approach could increase “SSN-shy” customers’ access to financial services instead of use of less transparent, informal value transfer systems, which could benefit law enforcement.

2. Expand the Scope of the BSA’s Requirement for “Address”

Though “address,” unlike “identification number,” is specifically mentioned in the BSA as an identification element, it has a history of broader interpretation than the “residential or business street address” required by the CIP Rules. The CIP Rules themselves make allowances for individuals without fixed residential or business addresses to provide Army or Fleet P.O. boxes or the residential or business address of a “next of kin or of another contact individual.”³⁷ In 2004, FinCEN issued an FAQ indicating that rural route numbers are acceptable as addresses and that in the absence of such a number or address for next of kin or another contact individual, even a “description of the customer’s physical location” would suffice.³⁸ Similarly, in 2010, FinCEN issued a ruling on the CIP requirements allowing victims of domestic violence in state-sponsored address confidentiality programs to use the P.O. boxes assigned by their state programs.³⁹ While this guidance is helpful, FinCEN could advance financial inclusion in both analog and digital identification by expanding upon the “next of kin or of another contact individual” option in the CIP Rules by utilizing the FATF’s suggestion of allowing “trusted referees”, including for example local government authorities, employers, or school administrators, to vouch for an applicant.⁴⁰ In the digital identity context, the National Institute of Standards and Technology (NIST) makes allowance for the use of trusted referees in its *Digital Identity Guidelines*, which provide digital ID

³⁶ For example, alternative identifiers may be needed to assist victims of human trafficking recover when their original identities have been compromised as a result of their victimization.

³⁷ See, e.g., 31 CFR 1020.220(a)(2)(ii).

³⁸ FinCEN, *Guidance on Customer Identification Regulations—FAQs: Final CIP Rule* (Jan. 2004).

³⁹ FinCEN, *Ruling FIN-2009-R003: Customer Identification Program Rule - Address Confidentiality Programs* (Nov. 3, 2009).

⁴⁰ FATF Guidance at ¶¶169-71.

inevitably linger and remain a barrier to use.³³ There may also be drawbacks for verifying financial institutions such as the fact that drivers' licenses may be revoked or expire, or individuals may carry driver's licenses from multiple states. The fact that physical driver's licenses are easily stolen and presented in full in a variety of settings, could make their identification numbers more vulnerable to fraud and identity theft.

While these are certainly concerns, there may also be advantages to mDLs that protect them from some of these potential weaknesses. If an iPhone is stolen or lost, bad actors will have a much more difficult time extracting mDL information from the iPhone than the face of a plastic license. mDL proponents, including Apple, tout the possibility of a "Privacy View", limiting access to those information elements required by the verifying requestor, confirming for example to a liquor store only that the bearer is over 21 without revealing even their birth date, identification number, or any other identifying information while revealing more to a TSA or law enforcement officer.³⁴ Most tantalizingly, perhaps, mDLs offer a clear path to linking verification systems directly to state agencies as official, authoritative "sources of truth" for identity—the end-to-end digital ID system. The decentralized and dispersed efforts of different states as our "laboratories of democracy" may even be a strength in this context. While Apple's early efforts are currently limited to proving identity in the physical world to law enforcement and the TSA, their broader adoption and potential linkages to DMVs and other state sources as verifiers make them strong candidates both for greater use and inclusion in the mosaic of our digital identity ecosystem, proving identity online, and for use of their identifying numbers by financial institutions for CIP purposes. In time, financial institutions and third-party identity providers should be able to establish Application Programming Interfaces (APIs) with DMVs and state identification providers directly, or even blockchain authenticated identity tokens.

The Corporate Transparency Act (CTA), as part of the AML Act, has also recently opened the door for alternatives to the SSN by not requiring the provision of an SSN for beneficial owners but rather only a "unique identifying number from an acceptable identification document," and indicating that the "acceptable identification document" may be a nonexpired driver's license, state identification card, or domestic or foreign passport.³⁵ Opening the door even a little more, perhaps, the CTA also authorized the use of a unique "FinCEN identifier," which the agency will be required to issue to both entities and individuals that otherwise provide the required identifying information. While much remains to be determined with respect to the CTA, the CIP Rules' requirement to collect Taxpayer Identification Number (TIN) (i.e., SSN for individuals and EIN for legal entities) for identification and verification purposes should be opened up to a risk-based approach that would allow for the collection of other "unique identifying numbers" from

³³ See, e.g., American Civil Liberties Union, *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom* (citing possibilities of police access and tracking without adequate safeguards).

³⁴ See, Wash. Post, *Your driver's license could soon live on your phone. Here's what you should know.* (Oct. 11, 2021).

³⁵ Corporate Transparency Act (AML Act of 2020), H.R. 6395, Div. F, §6403 (2021).

assurance frameworks and standards in the U.S. and are widely considered authoritative elsewhere.⁴¹

While expansion of the “trusted referee” concept could enhance financial inclusion, the nature of digital identification and relationships themselves may provide even greater flexibility in banking those in underserved communities without a fixed residential or business address. Signals and data points available in a digital relationship may allow financial institutions to conduct the appropriate level of transaction monitoring for customers who are unable to provide a fixed address. For instance, a customer with no fixed address but an identified and authenticated electronic device bound at an acceptable assurance level who consents to geo-location may provide a better “description of the customer’s physical location” than the potential uncertainties of locating that customer through “next of kin” or “another contact individual”—potentially allowing financial institutions to consider banking persons they might not have previously, even if at more restrictive, risk-based service levels. The FATF’s 2017 supplement on CDD to its 2013 Guidance on financial inclusion acknowledges this possibility and the likelihood that the sustainability of financially inclusive business models may be dependent on leveraging technological solutions like these.⁴² The intent behind requiring a physical address was to ensure that banks and law enforcement be able to locate a particular customer. Where digital identification information allows for a similar or perhaps even greater degree of certainty of customer location as physical address, it should be treated equivalently if not with greater certainty.

- E. Ensure the CIP Rules’ documentary verification examples and/or related examiner guidance are adaptable to a digital identification environment

The CIP Rules provide only one example for documentary verification of individual customers: “unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport.”⁴³ While there is built-in optionality for financial institutions to take a risk-based approach as to acceptable identification documentation, the example could potentially be enhanced to accommodate changes in the way digital identity may be provided. As it stands, the example suggests

⁴¹ NIST, *Special Publication 800-63A Digital Identity Guidelines* §5.3.4. Note that NIST issued a call for comment on its current guidelines in June 2020.

⁴² FATF, *Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence* at 25 (2013, updated Nov. 2017) (“FATF Financial Inclusion Guidance”) (“Increasingly, digital financial inclusion also includes the use of digital identity products and services to provide individuals with proof of identity for CDD purposes (though conventional and other alternative means of identifying customers and verifying identity may also be used). It also increasingly involves technological solutions used by financial institutions to fulfil their compliance obligations, for instance using big data collected through mobile phone usage, to monitor customers’ transactions in a cost-effective manner. This is an important factor regarding the sustainability of the business models developed by financial institutions to reach out to low-income, unserved and underserved groups”).

⁴³ See, e.g., 31 CFR 1020.220(a)(2)(ii)(A)(2).

“government-issued” identification, when in many jurisdictions “government-authorized” digital identity service providers could potentially provide greater assurance levels in identification.⁴⁴ The flexibility built into “photograph or similar safeguard” is also helpful but, even in the context of physical identification, is now dated when “safeguards” may include a range of technical advances, including holograms, UV printing, microprinting, laser perforation, etc.⁴⁵ For advancing the acceptance of, and best practices for, digital identification, it may be helpful for the CIP Rules themselves, examiner guidance like the FFIEC manual, or FAQs to clarify that, while the photograph may still be the gold standard, the range of safeguards has expanded dramatically since the CIP Rules’ issuance and that, in addition to photographic evidence, it may be helpful to financial institutions to have reference to the new range of photographic tools (selfies, liveness, biometrics, e.g.) and assurance levels set forth by an authoritative standard setting body like NIST.

F. Ensure the CIP’s rules’ non-documentary verification element and/or related guidance for examiners are fit for a digital environment

While the CIP Rules’ current examples for non-documentary verification have a helpful degree of flexibility, as discussed previously, they were crafted primarily for an analog identification environment and before many of the digital signals referenced above existed or were commonplace. Regulators should therefore also consider whether the CIP Rules’ specification of non-documentary verification methods is sufficient for the digital identification environment. The current examples specified in the CIP mostly remain useful today: “contacting a customer; independently verifying the customer’s identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.” The “comparison of information” to “a consumer reporting agency, public database, or other source”, in particular, is increasingly utilized over the other non-documentary and documentary verification methods in online customer relationships. However, additional examples that are both technology-neutral and principles-based could attune and encourage financial institutions and examiners to the possibilities of digital non-documentary verification. For instance, the rules could simply add a category that suggests “assessing data and assurance levels relevant to the delivery channel.”

⁴⁴ See, e.g., *FATF Guidance* at ¶155 (“Typically, proof of official identity has been provided by—or on behalf of—governments. In the digital era, we have begun to see new models, with digital credentials provided by, or in partnership with, the private sector being recognized by the government as official proof of identity in an online environment (e.g., NemID in Denmark), alongside more traditional government-issued digital credentials (e.g., electronic national IDs).”).

⁴⁵ See, e.g., Dep’t of Homeland Sec., Request for Information: *Minimum Standards for Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver’s Licenses*, 86 FR 20320, 20322 (Apr. 19, 2021) (distinguishing physical security features from electronic security features of mobile driver’s licenses).

Though amending the CIP Rules would be the most effective way to ensure effective adaptation to digital identification, training examiners to consider a financial institution's usage of digital signals as a valid part of identifying, verifying, and even enhancing ongoing CDD obligations, as discussed below, would also be helpful. Accordingly, the FFIEC could consider amending the FFIEC Manual's CIP section to reflect even that the "comparison of information" element could include an assessment of assurance levels, particularly through digital signals that could impact onboarding, such as MAC/IP address, geolocation, email age, and website interaction. Although the FFIEC Manual's CIP section was only recently updated, the principles reflected here and in the FATF Guidance could also be reflected in the Manual's "Electronic Banking" (2014) section or even in a standalone section on AML in the FFIEC's booklet on E-Banking, which was issued in 2003. The utilization of some of these digital signals is, of course, also predicated on having access to them—if customers are unwilling to provide access to them either at onboarding or during the course of the customer relationship, customers could choose to be subject to more manual monitoring, KYC refreshes, and their attendant inconveniences. For their part, financial institutions may choose to assess the feasibility or risks of the relationship in those circumstances and limit them accordingly.

Case study in optionality to the north: Canada

FINTRAC's recent publication of guidance for Canadian financial institutions on identifying and verifying customers explicitly adopts an "optionality" approach that may be instructive for the U.S. FINTRAC offers five different ways to identify and verify a person, including the more recognizable government-issued photo identification and "credit file" method (i.e., utilizing a credit bureau similar to U.S. financial institutions). FINTRAC provides guidance for digitally provided government-issued photo ID, requiring that FIs have a process in place to authenticate the ID, and walking through examples of how this may be accomplished with digital photographs of the ID, selfies, and live video chat. However, FINTRAC also offers financial institutions a "dual process" method by performing any two of the following three elements:

1. refer to and confirm information from a reliable source that includes the person's name and address;
2. refer to and confirm information from a reliable source that includes the person's name and date of birth; or
3. refer to information that includes the person's name and confirms that they have a deposit account, a prepaid payment product account, or a credit card or other loan account with a financial entity, and confirm that information.

The information may come from "statements, letters, certificates, forms or other information sources" either in the original or in paper or digital copy. However, the sources of any two elements used may not be the same. The dual process method would allow a customer to obtain financial services who may both lack government-issued identification and a credit file, although a credit bureau may be used to prove on the two elements.

by Congress in the passage of the AML Act of 2020,⁴⁹ and echoed by industry bodies like the Wolfsberg Group,⁵⁰ consultants and trade groups,⁵¹ and thinktanks.⁵² As the FATF suggests, encouraging and supporting digital identity systems and the effective use of digital identification techniques are exactly the kind of regulatory initiative that can allow financial institutions to refocus their AML/CFT programs on those more effective techniques. The effective use of digital identity in AML/CFT programs will not only allow the reallocation of cost savings, but itself will also produce more and more valuable information in the detection and prevention of ML/TF, as financial institutions leverage those digital signals that are increasingly defining their customer relationships. For example, one major investigative firm has related the effectiveness of utilizing digital signals and “following their data” by analyzing IP address data that revealed connections across a large number of purportedly unrelated customers, exposing a complex fraud and money laundering network.⁵³

2. Digital Identity and Financial Inclusion

Though the FATF’s March 2020 Guidance made a strong case for advancing financial inclusion particularly in developing countries by harnessing digital identity in AML/CFT programs, its authors likely could not have foreseen the outsized imperative financial inclusion would take in the ensuing year as governments even (perhaps especially) in developed economies like our own struggled to distribute funds at unprecedented speeds to the public to counteract the economic effects of the COVID-19 pandemic.⁵⁴ An effective system of digital identification not only would have hastened the stimulus and unemployment programs, but would also have helped the programs actually reach their intended recipients with less fraud and error.⁵⁵ Even more important, an effective digital identification system that fostered financial inclusion, could have helped the government reach more of those that have been most marginalized and vulnerable. As reported by *The New York Times* earlier this year, many homeless people lacking fixed addresses, identification, and resources were reportedly unable to receive the stimulus funds to which they

⁴⁹ See AML Act, §6002.

⁵⁰ Wolfsberg Group, *Statement on Effectiveness* (2019).

⁵¹ See, e.g., Deloitte & IIF, *The Global Framework for Fighting Financial Crime: Enhancing Effectiveness & Improving Outcomes* (2019).

⁵² See, e.g., RUSI, *Financial Crime 2.0*; Brookings Institution, *3 steps to improve anti-money laundering regulation* (2020).

⁵³ Tax Justice Network, *The role of banks and digitalised beneficial ownership registries* (July 2020) (describing analyses performed by Kroll in identifying the relationships of beneficial owners).

⁵⁴ See FATF Guidance at ¶109.

⁵⁵ See Center for Strategic & Int’l Studies, *The United States Has an Opportunity to Lead in Digital Development* (Mar. 30, 2021) (noting how “[t]he unforeseen devastation caused by the COVID-19 pandemic has highlighted the importance of digital payments and digital ID infrastructure for mitigating socioeconomic challenges” and citing the success of India’s universal digital identification system—the Aadhaar—to effect cash transfers).

were entitled.⁵⁶ There are of course many more prosaic but still vitally important use cases for utilizing digital identity to ensure that more routine social safety net payments are made to their intended recipients safe from fraud and abuse.

The use of digital identification to reach underserved populations may not be a panacea, as there are well-known barriers to access to technology that will inevitably affect some in those populations.⁵⁷ Sometimes referred to as the “digital divide”, lower income populations simply have less or less reliable access to the technologies that would facilitate digital identification. There is some reason for optimism on this front, however, as recent studies have found that 93% of the U.S. adult population use the internet, 97% use cell phones of some kind, and 85% use smart phones—and the percentages are regularly increasing.⁵⁸ In a potential silver lining, the pandemic laid bare the deficiencies of digital access particularly in education and concerted efforts by the government to facilitate access to underserved populations appear to be following.⁵⁹

Case study in financial inclusion to the south: Mexico

Mexico has, since 2011, utilized a four-tier system of account opening at increasing risk levels to enhance financial inclusion:

- Tier 1 accounts are anonymous, may be opened electronically or in retail stores, and require no account opening data. Monthly deposits, however, cannot exceed \$291, the balance may not exceed \$388, and funds may not be transferred to other accounts. Cash may be deposited only through physical channels.
- Tier 2 accounts require some basic personal information—name, DOB, gender, address, and Mexican state of origin—but also may be opened electronically. Monthly deposits may not exceed \$583 and the balance may not exceed \$1,165. Electronic banking and mobile transfers may be used.
- Tier 3 accounts require still more personal information—including occupation, phone number, email, and national identity and tax numbers—and may also be opened electronically. The monthly deposits are capped at \$3,885, but there is no balance limit.
- Tier 4 accounts are full featured, traditional bank accounts with checking and no deposit or balance limits. Physical presence is required for opening and the financial institution must keep copies of the identification information for a full KYC file.

Though Mexico’s financial inclusion numbers have not been buoyed as much as hoped by

⁵⁶ A. Newman, *No Address, No ID, and Struggling to Get Their Stimulus Checks*, The New York Times (Apr. 5, 2021).

⁵⁷ FATF Guidance at ¶137.

⁵⁸ See Pew Research Center, *Internet/Broadband Fact Sheet* (Apr. 7 2021); *Mobile Fact Sheet* (Apr. 7, 2021).

⁵⁹ See, e.g., USA Today, *Broadband for all: Inside President Biden’s \$100 billion plan to improve internet access* (Apr. 5, 2021).

III. Clearly define the benefits of digital ID for AML/CFT purposes, including for AML Effectiveness and Financial Inclusion

Though the FATF Guidance has effectively started cataloging many of the benefits of digital ID for AML/CFT,⁴⁶ financial institutions and regulators should continue to explore and define them but pay special attention to two key rationales: (1) effectiveness and (2) financial inclusion. These two rationales have now taken on greater significance in the context of recent world events of the COVID-19 pandemic and its economic fallout, as well as AML reform efforts emphasizing the “effectiveness” of AML programs. The FATF Guidance recognizes the importance and interrelatedness of both, suggesting that digital ID systems could not only “generate cost savings” and “help lower onboarding costs” for financial institutions, but also that “[t]hese cost savings could enable regulated entities to allocate compliance resources to other AML/CFT compliance functions, and also facilitate financial inclusion for otherwise excluded or under-served individuals by reducing on-boarding costs.”⁴⁷

1. Digital Identity and AML “Effectiveness”

As adopted at the October 2019 BSAAG Plenary and subsequently disseminated by FinCEN’s advance notice of proposed rulemaking on AML Program Effectiveness, the BSAAG’s AML Effectiveness Working Group identified regulatory initiatives that would allow financial institutions to reallocate resources in order to refocus their AML/CFT programs on more effective and efficient methods of detecting and preventing money laundering.⁴⁸ This theme has since been reinforced

⁴⁶ FATF Guidance at ¶¶104-11 (e.g., minimizing human error, improving customer experience, and enhancing transaction monitoring). Though better defining the risks, their mitigants, and best practices will also of course be critical to the effective use of digital identity in AML/CFT programs, they deserve more extensive consideration and expertise than we can give them here without consultation with broader group of stakeholders, such as cyber and fraud departments from FIs, law enforcement, and digital identity providers. The FATF Guidance effectively catalogs the risks, and their mitigants, of digital identity including the following (many of which may be overlapping): data loss; data corruption; misuse of data due to unauthorized access; cyberattack; impersonation risks; synthetic IDs; authentication and life cycle management risks, including credential stuffing, phishing, man-in-the-middle or credential interception, and PIN code capture and reply; multi-factor authentication vulnerabilities; and bio-metric authenticator spoofing and lower reliability of facial recognition with darker pigmentation or certain types of facial features. Members of this group have reported that their institutions are encountering many variations of these issues already in their fraud prevention efforts, including SIM swapping, IP/geolocation spoofing, cookie copying, browser version and screen resolution emulation. While FATF identifies some mitigants for these risks, technical standard setting bodies like NIST may be best suited to helping FIs control for these risks in the AML context going forward. Of course, many FIs already control for these risks in their fraud and cyber programs and may be well-prepared to understand the risks of incorporating these digital signals in their AML programs. In any event, since risks like these persist both online and in-person and increased digitization of customer relationships is a certainty, the real question for FIs may not be “whether” to consider these digital signals for AML/KYC purposes, but “how”.

⁴⁷ FATF Guidance at ¶107.

⁴⁸ FinCEN, *Advance Notice of Proposed Rulemaking: AML Program Effectiveness*, 85 FR 58023, 58025 (Sept. 2019).

IV. Progressive Identity and the Customer Journey

- A. Encourage the use of information associated with digital identification for broader KYC and transaction monitoring purposes

Financial institutions (and their examiners) should take the FATF's cue and expand their view of traditional KYC information to include those "anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts [like] customer identification/verification at onboarding *and ongoing due diligence and transaction monitoring.*"⁶⁰ Depending on the purpose and stage of the relationship, these "digital signals" may include: geolocation, MAC and IP addresses, biophysical biometric attributes (e.g., fingerprints, iris patterns, voiceprints, facial recognition), biomechanical patterns (e.g., keystroke mechanics, typing cadence, or device angle compared with known patterns), behavioral attributes (e.g., expected log-in channels, email/text message patterns, file access log, time of log-in, etc. compared with historical behavior), email age, patterns of website interaction (e.g., expected progression through product offering and account opening), frequency and type of usage, among others.

Without engaging in the extensive and necessary analyses of the specific use cases and best practices necessary for these digital signals in AML/KYC processes here, the basic use case for digital signals in AML/KYC processes is clear: as customer relationships become increasingly digital, and decreasingly in-person, a customer's behavior online becomes increasingly important to the fundamental CDD undertakings of "understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile [and c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."⁶¹ The strength of the binding event at onboarding that pairs the registered/identified and verified customer with his/her device(s) can help the financial institution establish the initial level of confidence in the identity and risk of the customer and inform the risk appetite for product and service levels for the customer. Ongoing authentication, "progressive binding" of new devices authenticated by the customer, behavioral trends, and events across the duration of the customer lifecycle may then all contribute to a customer's dynamic KYC profile. By expanding the initial profile of the customer necessary for onboarding, over time the financial institution develops a better understanding of the customer and its risk profile, which in turn allows the financial institution to expand the level or products and services. Merging these digital signals with traditional and evolving transaction monitoring scenarios and techniques will allow

⁶⁰ FATF Guidance at ¶126 (emphasis added).

⁶¹ See, e.g., 31 CFR §1020.210(a)(v) (CDD procedures requirement for banks).

financial institutions to better “follow their data” in discerning patterns of suspicious activity, in addition to fraud.

- B. Identification and verification are only the beginning—digital identity elements should inform the ongoing CDD obligations to understand the nature and purpose of the customer relationship.

To reap these benefits most effectively, however, financial institutions and regulators should—or at least should have the option to depending on the financial institution’s scale and resources—treat digital identification as a dynamic and progressive process of understanding customer identity over time as more data attributes are gathered and/or customer risk changes. Instead of treating identification and verification as a periodic, static, “point in time” check like onboarding followed by KYC refresh intervals, financial institutions, regulators, and examiners should recognize possibility that the continuous process of ongoing and dynamic identity proofing inherent in digital customer relationships may help facilitate different kinds of customer relationships, including more financially inclusive relationships. A dynamic, progressive view of identification would implement trigger-based thresholds in the KYC process that would prompt additional levels of assurance and verification and utilize that data to continuously rescore the overall confidence in the customer identity and, in turn, determine the scope of customer activity. In this KYC paradigm, a customer would progress on their “customer journey” from lower-risk, limited activity, but financially inclusive accounts to increasingly sophisticated products as that confidence increases—a process not dissimilar to today’s credit card business models, which raise credit limits as the financial institution’s confidence in their customer increases.

But this new paradigm will require reimagination of the customer lifecycle for AML/KYC purposes. Today, traditional customer risk assessment methodologies identify four general categories of “risk factors” that inform the overall profile: (1) intrinsic customer-related factors like professional activity; (2) geographical factors; (3) product, service and transactional behavior like inherent product risk or associated source/destination of funds; and (4) delivery channel such as in person or digital. In a progressive digital identity environment, however, “delivery channel” becomes its own distinct taxonomic rank. Instead of a “factor among many” at onboarding, it becomes the ordering principle for how financial institutions manage the customer across their lifecycle and puts a premium on the financial institution’s own technical capabilities and digital transparency between the financial institution and customer, which will likely be determined in some measure by the customer. Thus, if a customer uses a VPN or blocks location permissions—both legitimate privacy-based decisions—the progressive identity of the customer will be hampered (as will the frictionless service) as the financial institution may likely have to resort to more traditional KYC techniques or limit the customer’s access to its services.

For progressive identity concepts to be most effective, however, financial institutions should increasingly be able to treat significant deviations in risk factors as triggers for increased levels of assurance. To begin operationalizing those triggers, financial institutions should consider de-constructing each broad risk factor into a series of variables, or data elements, and mapping

those elements to the internal or external digital signals capable of indicating a deviation from the existing value (e.g., as collected at onboarding). Established thresholds against the variable's behavior would then determine whether or not the deviation reflects a material change in the overall risk factor and/or if a specific action is necessary to gain further confidence that the risk profile has actually changed (i.e., the trigger). Initially these thresholds may be theoretical (or vendor-driven based on industry experience), but over time, insights into the digital customer lifecycle management program would facilitate the financial institution's ability to "follow their data" and decrease or increase the need to trigger a specific action. For example, if the IP address login activity for the main account contact changes to be outside of the country(ies) stated at onboarding, the risk profile should be reassessed and updated to reflect this new country of operation.

In this vision of progressive identity, financial institutions should be better equipped to fulfill their fundamental obligation to understand the nature and purpose of their customer relationships on an ongoing basis. Combined with traditional transaction monitoring, financial institutions should be able to identify a more holistic picture of customer risk by focusing less on cruder proxies of customer risk assessed at arbitrary intervals and more on customer behaviors and intent.

- C. An explicit provision for simplified due diligence would increase adoption of progressive identity and encourage financial inclusion.

In order to enhance the potential of progressive identity and take full advantage of its potential for financial inclusion, however, U.S. regulators should consider adopting regulations that would encourage a true simplified due diligence (SDD)—a concept that has long been part of the FATF's Recommendations,⁶² but currently does not exist in the BSA/AML regime. Though a part of its initial 2012 Recommendations, the FATF more explicitly highlighted the importance of SDD to financial inclusion in its 2017 *Financial Inclusion Guidance*, which encouraged the reliance on a broader range of identification criteria as a part of SDD measures.⁶³ While the CIP Rules do, as discussed, provide some flexibility in the information collected from customers, they do not clearly tie the possibility of a simplified due diligence in connection with lower risk customers or relationships, products, or services. Regulatory sanction of this concept in the U.S., would encourage financial institutions to take the regulatory risk of "doing less," even if it is proportionate to the lower risks of the customer, for the laudable policy goal of financial inclusion.

V. Next Steps

Without a national government-issued form of digital ID in the U.S., financial institutions and their regulators will need time and flexibility to test new methods to fully realize the potential

⁶² FATF, *The FATF Recommendations* ¶11, Interp. Note. to Rec. 10 (2012).

⁶³ FATF, *FATF Financial Inclusion Guidance* at 20 (2017).

of our digital ID mosaic for AML/CFT purposes. However, this Group believes there are a few key next steps that would accelerate these efforts.

A multi-stakeholder approach. To fully understand and leverage digital ID for AML/CFT, financial institutions, regulators, and law enforcement should include technology and digital identity firms that are actively working on digital identity solutions—either for governments or financial institutions—in the conversation about how to develop and operationalize ideas like progressive identity. Since most digital identification software and systems for financial institutions are currently developed by specialized vendors, financial institutions, regulators, and law enforcement would benefit from greater understanding of the increasingly specialized techniques used by digital identity firms and their application to KYC. Similarly, different government agencies at both the federal and state level that deal with identifying information should be a part of the conversation to identify synergies and areas of collaboration between the public and private stakeholders that share the same goals for digital identification. To fully capture the range of views from these stakeholders, FinCEN should consider issuing a Request for Information (RFI) or an advanced notice of proposed rulemaking (ANPRM) on potential amendments to the CIP Rules, including those discussed above. To facilitate an effective and probing RFI or ANPRM, FinCEN could consider commissioning additional inquiry under the AML Act-mandated BSAAG Subcommittee on Innovation & Technology, possibly in tandem with the Subcommittee on Information Security & Confidentiality, to better define the scope of issues under digital identity and reform of the CIP Rules and better inform an effective RFI or ANPRM on CIP in the future. In addition, FinCEN could consider devoting some portion of the AML Act-mandated Financial Crimes Tech Symposium to the topics of Digital ID and financial inclusion, especially since the AML Act specifically requires the inclusion of international participants, many of whom have addressed these issues more squarely in recent enhancements to their AML/CFT regimes.

Legal entities. While this paper has focused primarily on digital ID in the context of natural persons, digital ID should also be leveraged for legal entities. Certainly, the identification of beneficial owners, control persons, and representatives of legal entities will benefit from advances in the digital identification of natural persons. However, digital identity solutions for entities themselves could also benefit from digital identification. Indeed, the forthcoming beneficial ownership registry required by the CTA could be seen as the foundational data point in the digital identification of legal entities.

Portability. As noted by the FATF, the portability of digital identification—the ability for a customer to utilize their proofed digital identity between different financial institutions—would make it far more valuable.⁶⁴ Where a digital identity can travel with a customer between financial institutions, it can allow the customer to continue that “customer journey” of progressive identity uninterrupted through their relationships with different financial institutions without having to

⁶⁴ See [FATF Guidance](#) at ¶168.

start from the beginning, building digital trust with each successive financial institution. Financial institutions would benefit not only from not having to redo a customer's KYC profile at each financial institution of their choice, but also from the accumulated risk information that comes with portability. Portability could also help reduce the constant re-exposure of a customer's personal identifying information (PII) in their onboarding at every financial institution. Again, without a national digital identity platform, the U.S. may be at a structural disadvantage on issues like portability. However, this Group strongly believes in pursuing portable digital identity solutions, and how financial institutions, digital identity providers, and government may be best be incentivized in that pursuit.

Government's Role and Partnership. Composed primarily of industry participants, this Group focused more on what financial institutions themselves can do or how AML/CFT regulations may be changed to enhance and promote the use of digital ID. However, even if a national identification system will always remain the "third rail" of the identification problem, there is unquestionably a greater role for governments to play in an effective digital identification system. While this paper explored the potential for mDLs and the use of their identification numbers above, the possibilities for federal government's role in digital identification should also be more deeply explored. Perhaps because of the national identity debate, the federal government has been viewed more as a technical standard setter—as with NIST's global leadership on the issue—or as a regulator—as with the CIP Rules. However, the federal government has recently taken an important step towards utilizing its powerful imprimatur as an authoritative "source of truth" in the digital ID ecosystem with the introduction and scaling of the Social Security Administration's (SSA) electronic Consent Based Social Security Number Verification (eCBSV) Service.⁶⁵ Required by 2018's Economic Growth, Regulatory Relief, and Consumer Protection Act, the eCBSV allows authorized entities, including financial institutions with customer consent, to query the SSA's database and verify if an individual's SSN, name, and date of birth combination matches the SSA's records. While there is of course room for improvement, the rollout of eCBSV is a welcome addition to the suite of digital identity tools for financial institutions and others. We should, however, continue to explore further roles for the unique authority of federal (and state) government in validating identity attributes while ensuring the privacy and control of consumer data.

⁶⁵ Social Security Administration, [electronic Consent Based Social Security Number Verification \(eCBSV\) Service](#).

BSAAG Document—Do Not Distribute beyond the BSAAG Membership Base



Financial Crimes Enforcement Network
U.S. Department of the Treasury

Washington, D.C. 20220

BSAAG Innovation and Technology Subcommittee Meeting

June 23, 2022

2:00 pm ET

Agenda

- 1.) Co-chair Opening Remarks
- 2.) BSAAG Plenary Read-out
- 3.) AI/Machine Learning—new focus area
- 4.) New Business/Open Discussion
 - a. Future ad hoc discussion on barriers to innovation
 - b. Future ad hoc discussion on DeFi lending and stablecoins

From: [REDACTED]@fincen.gov]
Sent: 8/18/2022 6:04:21 PM
To: [REDACTED]@promontory.com]; BSAAG [REDACTED]@fincen.gov]; [REDACTED]@us.hsbc.com;
[REDACTED]@fdic.gov]; [REDACTED]@barclays.com
Subject: EXTERNAL: RE: BSAAG: AI/Machine Learning Working Group

Hi [REDACTED]

Thanks for participating today! And thanks for sharing the link with us.

From: [REDACTED]@promontory.com>
Sent: Thursday, August 18, 2022 1:58 PM
To: BSAAG <[REDACTED]@fincen.gov>; [REDACTED]@us.hsbc.com; [REDACTED]@fdic.gov>;
[REDACTED]@barclays.com; [REDACTED]@fincen.gov>
Subject: [EXTERNAL] RE: BSAAG: AI/Machine Learning Working Group

Hello [REDACTED]

Great call, and really enjoyed the exchange of ideas.

As promised, sharing the link of an example of the educational articles that HKMA is producing:

[https://hyperlink.s\[REDACTED\]](https://hyperlink.s[REDACTED])
[REDACTED]

Warm regards,
[REDACTED]



[REDACTED]
Managing Director, Promontory Financial Group, a business unit of IBM Consulting
IBM Industry Academy Member

[REDACTED]

-----Original Appointment-----

From: BSAAG <[REDACTED]@fincen.gov>
Sent: Wednesday, August 10, 2022 1:34 PM

CONFIDENTIALITY NOTICE

Call for volunteers: AI/ML Working Group White Paper

From: [REDACTED]@fincen.gov>
To: BSAAG [REDACTED]@fincen.gov>
Date: Tue, 19 Sep 2023 14:24:59 -0500
Attachments: Third Party BSA Data Sharing Clean Draft Aug 2023 v5.docx (80.55 kB)

Hello BSAAG AI/ML Working Group Members,

(BSAAG communication: Not for further dissemination)

As mentioned during today's call, we are seeking 2-4 (or more) volunteers to work on drafting content for each section of the white paper. If you're personally unable to volunteer, you may submit the name of another representative from your organization who would like to participate in this effort. Here are the four sections of the white paper:

- a. 1. Definition of AI/ML for purposes of the white paper
- b. 2. Use Cases
- c. 3. Summary of risks/benefits/consideration
- d. 4. Appendix: Regulatory statements or guidance

Please respond by COB this Friday (September 22nd) and I'll then coordinate with the co-chairs.

I'm also attaching the Third Party Vendors Working Group draft white paper. This group has been working on this paper for about a 1 ½ and is now ready to deliver it to the full BSAAG plenary. With the permission of the co-chair, I'm attaching it to provide you with an example of what a BSAAG white paper might look like. Please do not share it any further.

[REDACTED]

BSAAG INNOVATION AND ADOPTION WORKING GROUP RECOMMENDATIONS

I. PROBLEM STATEMENT, GOALS AND DELIVERABLES

As technology evolves in the RegTech/FinTech ecosystem, financial institutions may be reluctant to test/adopt new technologies without the technologies regulatory track record or known reaction from regulators. Encouraging the adoption of innovative technologies is a priority for industry, law enforcement and regulators to increase the efficiency and effectiveness of AML/CFT programs and enhance our collective abilities to detect and deter financial crime. The goal of the Innovation and Adoption Working Group (the "Innovation Working Group") was to identify ways in which FinCEN can promote the adoption of new technologies for AML/CFT programs via pilots and increased regulatory feedback mechanisms (e.g., no action letters), in coordination with law enforcement.

During discussions regarding what actions FinCEN should consider as it looks to encourage more widespread adoption of new advanced technologies, the Innovation Working Group explored technologies currently being used or explored by stakeholders, the perceived challenges and opportunities in the adoption of new technologies, impacts to financial inclusion, and ways in which work being performed to implement the AML Act ("AML") could be leveraged.

II. TECHNOLOGY EXAMPLES AND CHALLENGES TO ADOPTION

Technologies either being used or developed/contemplated by financial institutions or vendors include:

- Suspicious activity detection and reporting programs that leverage machine learning, robotic process automation or artificial intelligence.
- Technologies that extract, capture, and analyze structured and unstructured data (e.g., text, speech, voice, image, video, metadata) to identify unusual or suspicious patterns.
- Technologies which review, digitize, and interpret new and existing regulatory intelligence (e.g., rules, regulations, enforcement actions, no-action letters, advisories).
- Big data infrastructures (e.g., cloud computing, data lakes, knowledge graphs) that can enable financial institutions to ingest, store, index, and analyze information within their organizations more quickly and make faster data connections.
- e-Know Your Customer ("KYC") and Know Your Business ("KYB") utilities that leverage distributed ledgers and cryptography to create trusted networks managed by a central provider that stores data that is made available to a larger group via personalizing access per user.
- Use of automated verification tools (e.g., using biometrics, computer vision, deep learning) that speeds up and increases security during remote onboarding.
- Use of distributive ledger platforms to enhance transaction monitoring and enable comprehensive investigations across financial institutions and jurisdiction (e.g., enclave-supporting data sharing).

Potential impediments to the adoption of technologies include the following:

- Inconsistent rules and regulatory expectations across the financial industry (e.g., application of risk-based approach differs across and within regulators, and across different jurisdictions), and inconsistent experience and awareness of new technologies across and within regulators, and across different jurisdictions.
- Past AML/CFT guidance and definitions may not align with new and emerging technologies and may not provide clear and relevant information for today's environment, including the material operational differences of new financial ecosystems (e.g. cryptocurrency, blockchain networks).

Confidential Draft

BSAAG Document: Do not further disseminate.

- Infrequent communication from regulators and law enforcement encouraging change/innovation and a lack of guidance providing a roadmap for effective implementation.
- The cost of new technologies is high (e.g., vendor license and implementation costs) and has not yet reached acceptable return on investment levels, especially for small and medium sized financial institutions as well as nonbank financial institutions, fintech companies and virtual asset service providers (“VASP”).
- Hesitancy to shift resources from surveillances viewed as inefficient (e.g., surveillances with high false positive rates, surveillances that produce SARs considered to be low value for law enforcement) to more in-depth surveillances due to uncertain regulatory reactions.
- Data privacy considerations and data quality limitations inhibit vendor solutions from being optimally deployed across multiple financial institutions and jurisdictions.
- Perception that new approaches will need to run alongside existing approaches.
- AML/CFT risk is constantly evolving and as markets, technology, and practices change, bad actors will look to exploit these new environments (e.g., synthetic identification fraud).

III. RECOMMENDATIONS

a. Facilitate open and frequent dialogue

Financial institutions look to the perceptions of regulators when considering whether to make changes to their AML/CFT programs and/or to utilize new technologies. In this way, a significant component to facilitating the adoption of new technologies is frequent and open communication between law enforcement, regulators, financial institutions, and technology providers.

Sections 6208 and 6207 of AMLA can drive these communications. Specifically, Section 6208 mandates that FinCEN and each federal functional regulator appoint an Innovation Officer to provide outreach on new innovative methods, processes and technologies that may assist in BSA compliance and provide technical assistance or guidance on the implementation of technologies by financial institutions, related persons, service providers/vendors and technology companies. Section 6207 establishes a BSAAG Subcommittee on Innovation and Technology (the “Innovation Subcommittee”) to advise on means to support technological innovation in AML/CFT and reduce obstacles to innovation from existing rules, guidance, and exam practices.

We recommend that Innovations Officers and the Innovation Subcommittee coordinate periodic roundtables with law enforcement, regulators, financial service providers, vendors, and technology companies. Initial focus areas to consider for roundtables include:

- Innovative tools in use or under development, corresponding regulatory expectations, and effective use cases and success stories.
- Best practices and success stories during pre- and postimplementation of new technologies.
- Rules, regulations, and guidance that may be impediments to the adoption of new technologies.
- Terms and definitions in rules, regulations, and guidance that may need to be modernized.
- Emerging AML/CFT risks, particularly those attempting to evade or exploit new technologies.
- How new technologies and innovations can advance BSA/CFT modernization and broader financial inclusion in tandem.
- Effective data sharing between financial institutions to detect illicit activity more comprehensively.
- Challenges specific to smaller financial institutions in adopting innovative solutions.

Confidential Draft

BSAAG Document: Do not further disseminate.

After completion of each roundtable, consideration should be given to what information can be released publicly (e.g., joint statements, white papers, guidance) to ensure the broader financial industry benefits from the discussions. Innovation Officers should also share this information within their respective organizations to increase awareness of technologies and level set regulatory expectations.

b. Comprehensive review of rules, regulations, and guidance

Innovation Officers and the Innovation Subcommittee should consider periodically assessing what rules, regulations, and guidance may be inhibiting the adoption of new technologies or otherwise may require modernization to adapt to new financial transaction types (e.g., cryptocurrencies and non-fungible tokens). Where necessary, Innovation Officers and the Innovation Subcommittee should recommend the issuance of updated guidance that seeks to achieve consistency across the financial industry and redefines terms for the modern age. Innovation Working Group discussions in this space focused on areas that may benefit from modernized definitions (e.g., definitions and guidance related to “reasonable” CIP verification in the modern age and “reasonable” reliance on third parties for CIP/CDD) and broader concepts that may warrant consideration given the evolution of financial activity (e.g., moving away from a definition of covered financial institution to a definition of covered financial activities).

Results of periodic reviews can be leveraged to inform work under Sections 6305, 6209 and 6211 of AMLA. For example, Section 6305 of AMLA requires the FinCEN Director (in consultation with other stakeholders) to determine whether to establish a process for the issuance of no-action letters in response to inquiries from financial institutions regarding interpretations of the Bank Secrecy Act (“BSA”) and USA PATRIOT Act. If such a process is formalized, reviews performed by Innovation Officers and the Innovation Subcommittee of rules, regulations, and guidance (as well as periodic roundtables) can be leveraged to identify areas where new no-action letters may be warranted. Examples of potential no-action letters discussed by the Innovation Working Group that may warrant consideration include:

- Fact patterns where no action would be taken on financial institutions that shift resources from less productive surveillances to more advanced technologies.
- Fact patterns where no action would be taken on financial institutions related to suspicious activity that occurred before a new technology was deployed which may have been detected had the technology been deployed at an earlier date.

While the December 2018 joint statement by FinCEN and its regulatory partners noted “innovative pilot programs in and of themselves should not subject banks to supervisory criticism, even if the pilot programs ultimately prove unsuccessful. Likewise, pilot programs that expose gaps in a BSA/AML compliance program will not necessarily result in supervisory action with respect to that program” a no-action letter should be considered to further encourage financial institutions to adopt innovative steps to enhance AML/CFT programs and provide clarity around specific regulatory expectations.

The Innovation Working Group also discussed how model risk management (“MRM”) and its application to AML/CFT programs is unclear (with many financial institutions believing that AML/CFT and sanctions tools are not models) and may be hindering the adoption of advanced technologies due to the perceived incompatibility of this framework to these technologies (e.g., machine learning, artificial intelligence, robotic processing) and the lack of guidance around the testing of these technologies. Work being done under Section 6209 of AMLA, which requires Treasury to issue a rule specifying standards by which financial institutions are to test technology and related internal processes, should consider feedback in these areas provided during roundtables, and the results of reviews performed over existing regulations, rules, and guidance. Partnering the results of work completed under Section 6209 of AMLA with a no action letter process that focuses on regulatory expectations associated with the transition to new technologies will provide a clear roadmap moving into new and innovative technological solutions.

We also recommend FinCEN consider joining, coordinating, and hosting “tech sprints,” “hackathons,” and other similar events with its partners from law enforcement, regulators, and financial and technology service providers. Section 6211 of AMLA requires the Secretary of the Treasury, in coordination with the

Confidential Draft

BSAAG Document: Do not further disseminate.

Innovation Subcommittee, to hold periodic global symposiums to promote international collaboration on the use of new technologies to prevent, detect, and investigate financial crime and other illicit activity. These symposiums can streamline efforts to approve new technologies and/or no-action letters, on a case by case basis, to clarify expectations and permitted activities. Innovation Working Group discussions in this space focused on similar events attended by members of the Innovation Working Group to understand what made these events successful (or unsuccessful). Based on these discussions, consideration should be given to establishing a theme for each symposium that addresses an area of need (e.g., using privacy enhancing software to monitor cross border transactions). Themes can be discussed and evaluated through roundtables and be further influenced by periodic reviews of rules, regulations and guidance performed by Innovations Officers and Innovation Subcommittee.

c. Enhance intelligence-sharing between law enforcement, regulators, and industry

FinCEN and other law enforcement and regulatory agencies regularly share intelligence and advisories. To increase the use and effectiveness of these materials and facilitate the adoption of new technologies, FinCEN should consider enhancing the mechanisms intelligence is made available and coordinating collaborative efforts between law enforcement, regulators, and financial institutions.

Supplementing public intelligence assessments with technical advisories shared privately with financial service providers (e.g., December 2020 Technical Bulletin on identifying cryptocurrency addresses, periodic release of Cyber Threat Indicators) can assist in enhancing suspicious activity detection efforts and protecting the financial industry from threats. FinCEN can also consider improving and standardizing formats that intelligence and advisories are distributed in and fostering digital reporting and information sharing. This includes transitioning rules, regulations, guidance, and intelligence advisories into machine-readable formats (e.g., XML) and establishing secure Application Programming Interfaces ("API") to enable financial institutions to factor new intelligence into AML/CFT programs more efficiently.

Including specific and contextualized intelligence on risks and red flags associated with different typologies and enabling these to be easily analyzed by AML/CFT systems will also assist financial institutions differentiate between actual versus perceived risks. While ensuring this differentiation is clear is critical to the AML/CFT priorities, it also plays a significant role in broadening financial inclusion by limiting overly broad de-risking that impacts low risk customers who fall within a broad risk category (e.g., customers located in a high risk jurisdiction with a de minimis nexus to the risk drivers of that jurisdiction).

We recommend FinCEN also consider coordinating collaborative efforts between law enforcement, regulators, and industry and establishing feedback loops on effective SAR filings. Previous efforts to collaboratively investigate money launderers and other illicit actors have occurred within a money laundering working group (sub-set of the five-eye working group) that leveraged 314(a) and 314(b). Increasing such efforts, particularly where law enforcement or national security focus areas have been identified, should be considered. Similarly, establishing mechanisms to provide feedback on SAR effectiveness would provide clarity on SARs considered to have provided high value intelligence would further assist the industry in their efforts to implement effective AML/CFT programs.

d. Areas for further study and consideration

Consider what role FinCEN/Treasury can play in creating, or coordinating efforts to create, technology utilities (e.g., distributive ledger or trusted network to support e-KYC and KYB efforts, or to protect and track sensitive or confidential information/BSA materials). Creation of such utilities may permit advanced data collection and sharing amongst FinCEN, law enforcement and other regulators and help to limit the barriers to entry in adopting new technologies associated with smaller financial institutions.

Consider how to assess the impact on financial inclusion as AML/CFT requirements evolve and new financial technologies, payment services, and digital asset services are increasingly used by previously undeserved constituencies. This can include assessments of the intelligence shared regarding AML/CFT risks and whether opportunities exist to provide further context and guidance around risks that better

Confidential Draft

BSAAG Document: Do not further disseminate.

informs the industry on critical risks and red flags and reduces the perceived binary choice financial institutions face when broad categories of customers or activities are labeled as high risk.

Bank Secrecy Act Advisory Group (BSAAG)**FinTech/RegTech Working Group****Payment Processor Exemption Workstream****Recommendations for the BSAAG May 2021 Plenary****Summary**

This white paper outlines for the consideration of the FinCEN Acting-Director, the three recommendations of the Payment Processor Exemption Workstream of the BSAAG FinTech & RegTech Work Group. These recommendations are the culmination of a multi-year effort by members of the Workstream to identify opportunities to further the US anti-money laundering (AML) regime by ensuring the Bank Secrecy Act (BSA) and its implementing regulations are appropriate across emerging entrants/technologies relative to their respective business models and risk profiles, including FinTech and RegTech firms.¹ More specifically, the Workstream focused on 31 CFR 1010.100(ff)(5)(ii), commonly referred as the “payment processor exemption” (PPE), which exempts persons engaging in certain activities from the AML regulatory obligations of the BSA.

Summary of the PPE Workstream Recommendations**Recommendation 1**

FinCEN should engage in a comprehensive regulatory review and update of the Payment Processor Exemption to account for new business models emerging from technological innovations in the financial services sector. As part of its regulatory update, FinCEN should exclude from the PPE entities that maintain accounts/relationships with the public, or process payments for goods and services where the entry or exit point is not a BSA-regulated entity.

Recommendation 2

Extend the BSA’s suspicious activity reporting safe harbor protections to any person operating under the PPE that chooses to file a Suspicious Activity Report (SAR).

Recommendation 3

¹ The Workstream defined:

- FinTech Firms as non-bank financial institutions, primarily third-party payment processors, that offer alternative methods of payment for local and/or cross-border payments or storage of monetary value in support of specific commercial activity, by processing transactions or holding value on behalf of other parties (i.e., online marketplaces, merchant processors, payment facilitators). FinTech Firms can also be money transmitters who enable customers to make money transfers online through the web and/or mobile applications.
- RegTech Firms as entities that use technologies to solve regulatory and compliance requirements and expectations more effectively and efficiently.

Require any person operating under the PPE to be registered with FinCEN.

Background and Overview

The BSA requires that Money Services Businesses (MSBs) comply with certain registration, AML program, customer identification, transaction monitoring, reporting, and recordkeeping requirements. The BSA defines an MSB to include money transmitters and defines “money transmission services” as the acceptance of funds from one person and the transmission of those funds to another location or person by any means.² However, whether a person is a money transmitter as defined by the BSA and therefore subject to regulation as an MSB is a matter of “facts and circumstances.”³ One of the exemptions from the BSA definition of money transmission is for a person that only “[a]cts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller”⁴ (i.e., the PPE). Accordingly, a person that is acting consistent with this exemption would not be an MSB (at least with respect to the transactions handled as a payment processor) and therefore not subject to the requirements of the BSA.

Through interpretive guidance, FinCEN has indicated that the following criteria must be met for the PPE to apply:

- (1) The entity providing the service must facilitate the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself);
- (2) The entity must operate through clearance and settlement systems that admit only BSA-regulated financial institutions (e.g., the Automated Clearing House);
- (3) The entity must provide the service pursuant to a formal agreement; and
- (4) The entity’s agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds from the entity.⁵

The below recommendations are intended to address three considerations with respect to the PPE as it applies to payments services companies today: (1) whether certain entities that come within the scope of the PPE should nonetheless be subject to BSA requirements, either by narrowing the scope of the exemption or by imposing requirements on exempt entities; (2) clarifying the scope of the PPE today to affirm that certain activities are outside the scope of the exemption (and therefore that companies that may be inappropriately relying on it are on notice that they may be MSBs); and (3) whether persons operating under the PPE have information on transactions that are of high degree of usefulness to law enforcement.

Recommendation 1

Problem Statement

² 31 CFR 1010.100(ff)(5).

³ *Id.*

⁴ 31 CFR 1010.100(ff)(5)(ii)(B).

⁵ See FinCEN guidance FIN-2014-R009 “[HYPERLINK "https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/application-money-services-business"]” (August, 2014).

Currently, there is limited regulatory oversight/accountability of payment processors, which extend to the consumer protection, fraud, cybersecurity, and AML areas. For instance, the BSA does not require payment processors to maintain the same level of financial crime transparency that AML-examined entities are subject to, and it is unclear what are, if any, the AML obligations of foreign located entities that process US transactions under the PPE. These issues have been exacerbated by the emergence of new business models in the financial services sector as the result of recent innovation and technological advances.

Furthermore, this landscape has prompted banks to generally require by contract that payment processors implement an AML program to mitigate risks, and for banks to be subject to examination and oversight with respect to their management of risk associated with payment processing relationships. This ultimately has placed banks in the position of de facto regulator of payment processors.

The confluence of these circumstances has (1) potentially created a gap in the US AML framework, (2) led law enforcement to have little to no visibility into the transactions that payment processors facilitate, and (3) for other financial firms (i.e., banks) to effectively supervise payment processors(perhaps unevenly).

Recommendation

FinCEN should engage in a comprehensive regulatory review and update of the Payment Processor Exemption to account for new business models emerging from technological innovations in the financial services sector. As part of its regulatory update, FinCEN should, as further detailed below, exclude from the PPE persons that maintain accounts/relationships with the public or process payments for goods and services, where the entry point is not a BSA-regulated entity.

More specifically, based on the analysis of the Workstream of associated AML risks, FinCEN should revise the scope of the payment processor exemption so that the PPE does not apply to the below payment processor business models (and businesses that may engage in activities under a combination of these models) and therefore are subject to the BSA requirements for MSBs. The following business models should not qualify for the PPE:⁶

- *Payment processors facilitating non-face-to-face payments for goods and services, where such processors are not operating solely through clearance and settlement systems that admit only BSA-regulated institutions, both with respect to pay-ins and pay-outs.*

This recommendation would definitionally include the following business models as MSBs: payments for goods and services, where the funds originate from or settle to

⁶ The PPE workstream considered the application of suspicious activity reporting as a standalone requirement for certain payment processors but concluded that, a SAR filing regime without the accompanying transaction monitoring, customer identification and due diligence and record keeping requirements would not be sustainable. Furthermore, the PPE workstream concluded that it would be very difficult for partner banks, other financial institutions, law enforcement and even regulators to keep track of which requirements apply to which types of payment processors.

Confidential Draft

BSAAG Document: Do not further disseminate.

unhosted wallets, foreign financial institutions, or other non BSA-regulated entities. The Workstream concluded that payments for goods and services involving unhosted wallets, foreign financial institutions, or other non BSA-regulated entities are of inherent higher risk, have limited financial transparency, and include entry or exit points that do not have the same oversight that BSA-regulated entities have.

Due to the low-risk nature of utility payments, payment processors facilitating only these transactions, despite from/to where funds originate/settle, could remain operating under the PPE.⁷

- *Payment processors that maintain and allow the public to create profiles or accounts in order to transact, even if such payment processors operate solely through clearance and settlement systems that admit only BSA-regulated financial institutions.*

This recommendation is intended to address evolution in payment processors business models that may have not been originally considered when the PPE was being envisioned almost 25 years ago.⁸ In this regard, while payment processors may have opted to maintain accounts/relationships with the public to improve customer experience, these business models effectively allow multiple payment funding sources for a single customer and have visibility into and facilitate transactions across borders, e-commerce platforms, and businesses without any customer identification or due diligence, record retention, transaction monitoring or suspicious activity reporting requirements. The Workstream concluded that payment processors that maintain and allow customer accounts/relationships potentially could lead to a gap in the US AML framework by not performing customer identification or due diligence to verify customers' identities or ensuring customers' funding sources are legitimate. Furthermore, the Workstream recognized that these payment processor models do not have suspicious activity reporting obligations despite having broad visibility into customer transactions (e.g., being able to see transactions by a customer using multiple payment methods across merchants, retailers, e-commerce platforms, and financial institutions), which can be of a high degree of usefulness to law enforcement.

Mirroring the above previous recommendation, due to the low-risk nature of utility payments, payment processors facilitating only these transactions, despite from/to where funds originate/settle, could remain operating under the PPE.⁹

⁷ For the purposes of this white paper, "utilities" include public utilities (such as light, power, internet, or water) or comparable services.

⁸ Please see the regulatory exemptions for certain payments for goods and services included in FinCEN's 1997 [[HYPERLINK "https://www.govinfo.gov/content/pkg/FR-1997-05-21/pdf/97-13304.pdf"](https://www.govinfo.gov/content/pkg/FR-1997-05-21/pdf/97-13304.pdf)] amending the definition of and requirements for MSBs (Federal Register Volume 62, Issue 98).

⁹ For the purposes of this white paper, "utilities" include public utilities (such as light, power, internet, or water) or comparable services.

Recommendation 2Problem Statement

At this time, persons operating under the PPE are not subject to BSA/AML compliance program requirements under FinCEN regulations, and therefore are not required to conduct suspicious activity reporting and in turn are not explicitly afforded safe harbor for filing SARs voluntarily. In many cases, these processors are contractually required by bank partners to monitor transactions and to notify the bank of potentially suspicious activity so that the bank can file SARs (at their discretion), but in other cases the bank does not have a relationship of that nature with the processor and potentially suspicious activity may not be reported. In such cases, law enforcement agencies and FinCEN have no visibility into any suspicious activity that payment processors may identify (or fail to identify) and there is no incentive or protection that would prompt payment processors to report suspicious activity through SARs. This combination of factors can potentially be creating a financial intelligence gap for law enforcement agencies and FinCEN because payment processors may have broad visibility of an illicit actor's actions by virtue of being able to identify patterns of transactional activity across multiple transactional channels, financial institutions, and products.

Recommendation

Extend existing SAR safe harbor protections to any person operating under the payment processor exemption that chooses to file a SAR, even though a person operating under the PPE (and that is not otherwise an MSB) does not have an express regulatory obligation to file SARs in such situations and therefore is not within the scope of the safe harbor.

This recommendation intends to encourage the reporting of information with a high degree of usefulness to law enforcement by payment processors despite current requirements, which ultimately could also lead to increased financial transparency and enhance the strength of the US AML framework.

Recommendation 3Problem Statement

Currently, the full extent, size, and makeup of the universe of financial firms operating under the PPE (and what their business models are) is unknown at a national level. In an age of rapid financial services evolution due to technology innovation, this represents a potential AML vulnerability in the US financial system. In addition, there is a sense among financial industry members that entities are not properly or uniformly interpreting the applicability of the PPE to their business models. For example, throughout the emergence of new financial services models over the past few years, some FinTech firms have tended to decline their classification as financial firms by claiming their status as technology companies.

Recommendation

Require persons operating under the PPE to register with FinCEN as MSBs but in an exempt category, and at the time of registration to provide a brief explanation why their operations/business model fall within the PPE.

This recommendation would bring transparency and order to the payment processor sector by applying the same registration requirement that MSBs have, irrespective of whether payment processors are exempted from AML program requirements. Perhaps most importantly, this requirement would allow FinCEN to (1) evaluate whether some payment processors are correctly operating under the PPE and (2) study whether additional regulation would be needed to regulate this sector, which would put FinCEN in a favorable position to account for future innovation advances in financial services business models. While there may be some regulatory burden concerns with this proposed new requirement, in many instances payment processors already register at the state level as part of their licensure by using the same information used in the Registration of Money Service Business form (RMSB). Furthermore, completing and filing an RMSB takes a relatively short amount of time (minutes in most cases), which would mitigate regulatory burden concerns.

This recommendation could be accomplished by modifying Chapter X of Title 31 to include payment processors as part of the persons required to register as MSBs (but not subject to BSA/AML program requirements for MSBs, per the PPE), and updating the RMSB form to allow for this type of registration. To accommodate this new registration requirement, FinCEN should further consider including sub-categories in the RMSB form of the most common payment processor business models.¹⁰

To summarize, the members of the Payment Processor Exemption Workstream submit the above three recommendations to the Acting-Director of FinCEN based on the analysis conducted of the evolution of business models and AML risks of payment processing firms.

Submitted on behalf of the members of the Payment Processor Exemption Workstream, BSAAG
FinTech & RegTech Working Group.

¹⁰ To provide options to FinCEN as it considers how to implement a registration requirement for payment processors, the Workstream members alternatively considered requiring payment processors to formally file with FinCEN their status as entities operating under the PPE and concluded that this alternate approach would accomplish the goals contemplated by the original registration recommendation outlined in this white paper.

III. The Democrats' use of lawfare to target political opponents

During the Biden-Harris Administration, Democrats in Washington, D.C., and in certain states have engaged in an unprecedented campaign of lawfare to target and attack President Donald Trump.¹³⁸ Across the country, rogue political prosecutors stretched legal theories to secure unjust indictments against President Trump and his associates in an effort to keep President Trump off of the campaign trail, drain him of resources, and attempt to prevent millions of American citizens from being able to cast a ballot for their candidate of choice.

On April 25, 2024, the Select Subcommittee released a report, “[An Anatomy of a Political Prosecution: The Manhattan District Attorney’s Office’s Vendetta Against President Donald J. Trump](#),” revealing the unprecedented nature of the New York County District Attorney’s Office’s (DANY) multi-year investigation into President Trump. Starting in 2018, the DANY searched for any legal theory on which to bring charges against President Trump from his property valuations to his business records, to even New York’s racketeering statute.¹³⁹ As Special Assistant District Attorney Mark Pomerantz detailed in his memoir, none of the theories panned out.¹⁴⁰ The deficiencies in the case led to the investigation going dormant, until District Attorney Alvin Bragg—who campaigned for office with a promise of investigating President Trump—revived the case and charged President Trump with 34 felony counts for falsifying business records.¹⁴¹ Using a novel and untested legal theory, Bragg took what would ordinarily be misdemeanors subject to a two-year statute of limitations and “bootstrapped” them to federal campaign finance law to make the charges into felonies and thereby extending the statute of limitations to five years. In reviving this “zombie”¹⁴² case, it is clear that Bragg’s motivation to finally indict President Trump, only came after President Trump announced his intention to run for President in the 2024 election.

The Select Subcommittee held a series of hearings examining Bragg’s lawfare, including releasing a second report, “[Lawfare: How the Manhattan District Attorney’s Office and a New York State Judge Violated the Constitutional and Legal Rights of President Donald J. Trump](#).” The testimony the Select Committee received from distinguished legal scholars and attorneys at the hearings, as laid out in the report, make clear that Bragg’s political prosecution of President Trump was riddled with legal and procedural defects.¹⁴³ For example, one witness, constitutional

¹³⁸ See William K. Rashbaum et al. *Manhattan prosecutors begin presenting Trump case to grand jury*, N.Y. TIMES (Jan. 30, 2023) (discussing Manhattan DA prosecution); Glenn Thrush, et al., *Jack Smith, the special counsel, will take over two inquiries into Trump*, N.Y. TIMES (Nov. 18, 2022) (Attorney General Garland announced Jack Smith’s appointment as special counsel three days after President Trump announced his run for office); Indictment, *Georgia v. Donald John Trump et al.*, No. 23SC188947 (Aug. 14, 2023, Fulton Co. Sup. Ct.) (Fulton County DA Fani Willis began an investigation into President Trump in February 2021 but did not bring charges until after he had announced his candidacy for the 2024 election).

¹³⁹ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., AN ANATOMY OF A POLITICAL PROSECUTION: THE MANHATTAN DISTRICT ATTORNEY’S OFFICE’S VENDETTA AGAINST PRESIDENT DONALD J. TRUMP (Comm. Print Apr. 25, 2024).

¹⁴⁰ See *id.* at 2 (internal citation omitted).

¹⁴¹ *Id.* (internal citation omitted).

¹⁴² MARK POMERANTZ, PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT 36-38, 46 (2023).

¹⁴³ See STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., LAWFARE: HOW THE MANHATTAN DISTRICT ATTORNEY’S

law scholar and attorney Elizabeth Price Foley, testified that jury instructions of the trial judge, Judge Juan Merchan, violated President Trump’s due process rights.¹⁴⁴ Another witness, Federal Election Commission (FEC) Commissioner James “Trey” E. Trainor, III, testified that Bragg’s prosecution of President Trump “‘usurped the jurisdiction that Congress has explicitly reserved for the federal authorities” and “undermine[d] the statutory framework established by [the Federal Election Campaign Act].”¹⁴⁵ Finally, the Select Subcommittee’s investigation and report shed light on Judge Merchan’s political bias and his prejudicial rulings throughout the trial, including Judge Merchan’s decision to unconstitutionally silence President Trump by issuing a gag order, permitting Bragg to admit inadmissible testimony at trial, and denying FEC Commissioner Bradley Smith from providing fulsome testimony as an expert witness on President Trump’s behalf.¹⁴⁶ The Select Subcommittee’s investigation and report makes abundantly clear that Bragg’s political prosecution, overseen by an overtly bias judge, was riddled with constitutional defects and violated President Trump’s due process rights.¹⁴⁷

During its investigation, the Select Subcommittee found that shortly after President Trump announced his presidential candidacy, Bragg’s office “jump-start[ed]” a criminal investigation into the former President “that once seemed to have reached a dead end.”¹⁴⁸ Just weeks later, it was reported that Bragg had hired Matthew B. Colangelo, “a former senior Justice Department official with a history of taking on Donald J. Trump and his family business as the office seeks to ramp up its investigation into the former president.”¹⁴⁹ Before joining Bragg’s office, Colangelo served as a senior official in the Biden-Harris Administration’s Justice Department.¹⁵⁰ Among other positions, Colangelo was the number three official in the Department.¹⁵¹ Moreover, in Bragg’s press release that announced Colangelo’s hiring, Bragg boasted that Colangelo “investigat[ed] the Trump Foundation” during his tenure with the New York State Office of the Attorney General.¹⁵² After Bragg hired Colangelo for a first-of-its-kind position in the New York County District Attorney’s Office,¹⁵³ he then served as a top prosecutor in the criminal case against former President Trump. Because of Colangelo’s role as a high-ranking political appointee in the Biden-Harris Administration’s Justice Department, currently, a top prosecutor in the New York County District Attorney’s Office’s criminal prosecution of President Trump, the Committee continues to investigate Bragg’s apparent politically motivated hiring of Colangelo.

OFFICE AND A NEW YORK STATE JUDGE VIOLATED THE CONSTITUTIONAL AND LEGAL RIGHTS OF PRESIDENT DONALD J. TRUMP (Comm. Print July 9, 2024)

¹⁴⁴ *Id.* at 14-20.

¹⁴⁵ *Id.* at 21-24 (internal citation omitted).

¹⁴⁶ *Id.* at 24-32.

¹⁴⁷ *See generally id.*

¹⁴⁸ Jonah E. Bromwich et al., *Manhattan Prosecutors Move to Jump-Start Criminal Inquiry Into Trump*, N.Y. TIMES (Nov. 21, 2022).

¹⁴⁹ Jonah E. Bromwich, *Manhattan D.A. Hires Ex-Justice Official to Help Lead Trump Inquiry*, N.Y. TIMES (Dec. 5, 2022).

¹⁵⁰ *Id.*

¹⁵¹ Staff Profile, U.S. Dep’t of Justice, Former Acting Associate Attorney General Matthew Colangelo (last updated Apr. 22, 2021).

¹⁵² Press Release, District Attorney Bragg Announces Matthew Colangelo as New Senior Counsel (Dec. 5, 2022).

¹⁵³ *Id.* (“This is the first time the Manhattan D.A.’s Office will have an executive position focusing on these priority areas.”).

In addition to investigating Bragg’s politicized indictment, the Select Subcommittee’s work explored how the Justice Department enabled hyper-partisan prosecutors, in particular Special Counsel Jack Smith, to criminalize politics in America. The Select Subcommittee uncovered evidence demonstrating how Smith and his team engaged in a series of improper actions and unethical conduct that violate the Department’s duty to conduct impartial justice. First, the Select Subcommittee found that Jay Bratt, a senior attorney on Smith’s team, met with Biden-Harris White House officials numerous times before the Special Counsel’s Office indicted President Trump.¹⁵⁴ In September 2021, Bratt reportedly met with an advisor to the White House Chief of Staff,¹⁵⁵ and, in November 2021, went to the White House to meet with Administration officials.¹⁵⁶ Additionally, on March 31, 2023, only nine weeks prior to Smith’s indictment of President Trump, Bratt met with a White House Counsel’s Office official for a “case-related interview.”¹⁵⁷

Next, the Select Subcommittee discovered evidence that Bratt improperly pressured Stanley Woodward, a lawyer representing Walt Nauta, a co-defendant in Smith’s classified documents case against President Trump, by implying that the Biden-Harris Administration would look more favorably on Woodward’s candidacy for a judgeship if his client cooperated with the Office of the Special Counsel.¹⁵⁸ According to Mr. Woodward, Bratt advised him that Bratt “wouldn’t want [Woodward] to do anything to mess that up,” in reference to Mr. Woodward’s judgeship application, and Bratt’s desire to turn his client into a government cooperator.¹⁵⁹

Further, the Select Subcommittee uncovered evidence suggesting that Bratt attempted to retaliate against Woodward for disclosing Bratt’s unethical conduct. For example, on August 2, 2023, Bratt filed a motion in Nauta’s case raising alleged conflicts of interests presented by Woodward’s representation of two other witnesses “who could be called to testify at a trial in the case involving classified documents at Mar-a-Lago.”¹⁶⁰ Bratt further suggested that the court should “procure independent counsel” to be present at the hearing “to advise Mr. Woodward’s clients regarding the potential conflicts.”¹⁶¹ Woodward’s reply brief stated that Bratt’s intimidation threats were merely “an attempt to diminish the Court’s authority over the proceedings in this case and to undermine attorney-client relationships without any basis specific

¹⁵⁴ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Jay I. Bratt, Counselor to the Special Counsel, U.S. Dep’t of Justice at 2 (“According to . . . reports, you also met with Biden White House officials numerous times before the Special Counsel’s Office indicted President Trump.”) (hereinafter “Bratt Letter”); Jon Levine, *Biden staffers met with special counsel Jack Smith aides before Trump indictment*, N.Y. POST (Aug. 26, 2023).

¹⁵⁵ Bratt Letter at 2.

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*; Ken Dilanian, *Lawyer for witness in Trump docs probe alleges prosecutorial misconduct*, NBC NEWS (Jun. 8, 2023).

¹⁵⁹ *Id.* (quoting Letter from Stan M. Brand & Stanley E. Woodward Jr. to the Hon. James E. Boasberg, Chief Judge, U.S. Dist. Ct. for the Dist. of Columbia (June 7, 2023)).

¹⁶⁰ *Id.* at 2-3 (citing Glenn Thrush, et al., ‘*Divided Loyalties*’ May Afflict Lawyer in Mar-a-Lago Case, *Prosecutors Say*, N.Y. TIMES (Aug 2, 2023)).

¹⁶¹ *Id.* at 2 (citing Mot. for *Garcia* Hearing at 1–2, U.S. v. Donald J. Trump et al., No. 23-80101 (S.D. Fl. filed Aug. 2, 2023)).

to the facts of such representation.”¹⁶² The federal judge overseeing the prosecution was so concerned about these allegations that she “twice ordered the parties, on her own, to explore and report to her on possible prosecutorial misconduct.”¹⁶³

Additionally, the Select Subcommittee investigated Bratt’s acknowledgment in a May 3, 2024, court filing that some of the evidence in President Trump’s classified documents case was altered or manipulated after the FBI seized it during its raid on Mar-a-Lago in 2022.¹⁶⁴ After Woodward notified the Court on May 1, 2024, that there were discrepancies in the evidence—suggesting that the boxes of documents that the Special Counsel’s Office produced for defense review were potentially tampered with or compromised¹⁶⁵—Bratt admitted that “there are some boxes where the order of items within that box is not the same as in the associated scans,”¹⁶⁶ and that this new admission “[wa]s inconsistent with what Government counsel previously understood and represented to the Court.”¹⁶⁷ Bratt’s apparent manipulation of material evidence even led some legal experts to conclude that Bratt’s conduct was tantamount to “evidence tampering.”¹⁶⁸

The Select Subcommittee investigated other egregious ethical lapses by Smith and his team—in particular by J.P. Cooney, who served as another one of Smith’s top prosecutors. According to a July 2024 report by the Justice Department’s Office of the Inspector General (OIG), Cooney previously “supervised a team of four attorneys” who led the prosecution of Roger Stone, a former campaign aide of President Trump, for allegedly obstructing Special Counsel Robert Mueller’s investigation into the widely debunked Russian collusion hoax.¹⁶⁹ After securing a verdict against Stone, Cooney sought an “unprecedented” sentence of seven to nine years in prison for Stone, which was reportedly “dramatically beyond what others convicted of similar crimes faced.”¹⁷⁰ When Cooney’s supervisors learned of his excessive sentencing

¹⁶² *Id.* at 3 (citing Opp. to Mot. for *Garcia* Hearing at 8, U.S. v. Donald J. Trump et al., No. 23-80101 (S.D. Fl. filed Aug. 2, 2023)).

¹⁶³ *Id.* (citing Roger Parloff, *The Return of the Stanley Woodward Mess*, LAWFARE (May 7, 2024)).

¹⁶⁴ *Id.* (citing Resp. to Mot. to Extend Time, U.S. v. Donald J. Trump et al., No. 23-80101 (S.D. Fl. filed May 3, 2024) (hereinafter “Government’s Response”)); John Solomon, *Trump Whodunnit: Prosecutors admit key evidence in document case has been tampered with*, JUSTTHENEWS (May 3, 2024).

¹⁶⁵ Mot. to Extend Time, U.S. v. Donald J. Trump et al., No. 23-80101 (S.D. Fl. filed May 1, 2024).

¹⁶⁶ Government’s Response, *supra* note 164, at 8.

¹⁶⁷ *Id.* at 8 n.3.

¹⁶⁸ See Bratt Letter, *supra* note 154, at 3; Solomon, *supra* note 164. Harvard Law Professor Emeritus Alan Dershowitz stated, “Prosecutors and investigators should never tamper with or alter evidence in their possession, including the order of documents in a box because no one knows what may become relevant or crucial to a court or jury later in a case.” *Id.*

¹⁶⁹ Mollie Hemingway, *Jack Smith’s Anti-Trump Deputy Excoriated For Inappropriate Behavior At DOJ*, THE FEDERALIST (July 26, 2024) (“Mueller’s two-year, \$32 million investigation was itself spun up by anti-Trump officials in the Justice Department after the Democrat National Committee and Democrat presidential nominee Hillary Clinton bought and paid for an information operation falsely alleging the Trump campaign was in cahoots with Russia to steal the 2016 election. Two members of Cooney’s team also worked on the Mueller investigation.”).

¹⁷⁰ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Jeffrey Ragsdale, Counsel, Office of Prof’l Resp., U.S. Dep’t of Justice (Aug. 2, 2024) (citing OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, 24-081, AN INVESTIGATION OF ALLEGATIONS CONCERNING THE DEPARTMENT OF JUSTICE’S HANDLING OF THE GOVERNMENT’S SENTENCING RECOMMENDATION IN *UNITED STATES V. ROGER STONE* (July 24, 2024) (hereinafter “OIG Report”)); see also Hemingway, *supra* note 169. Meanwhile, when “developing that sentencing goal,” Cooney

recommendation for Stone, “they all agreed that the sentencing recommendation was too high” and expressed “concern that seeking such a high sentence . . . could negatively impact the credibility of the Department. . . .”¹⁷¹

After receiving pushback for his excessive sentencing recommendation, Cooney began “spreading an elaborate conspiracy theory with no supporting evidence that [former President] Trump, [Attorney General William] Barr, and [Interim U.S. Attorney Timothy] Shea were being improperly political.”¹⁷² Cooney admitted to OIG investigators that “he had no information suggesting that anyone from Main Justice (i.e., DOJ leadership offices) was involved in the Stone sentencing at this time and no evidence pointing to improper motivations influencing these discussions” when he initiated and spread the conspiracy theory.¹⁷³ Meanwhile, in phone calls and other conversations with the prosecution team, Cooney pushed a false narrative that Shea “was acting out of fear of then President Trump and, more particularly, fear of the consequences of not seeking a lower sentence for an influential friend of then President Trump.”¹⁷⁴ Cooney later told the OIG that he “was not [actually] aware of specific evidence to that effect.”¹⁷⁵ In its report, the OIG said that Cooney’s “speculative comments in meetings with the [Stone] trial team about the political motivations”¹⁷⁶ of Trump officials “in connection with their handling of the Stone sentencing contributed to an atmosphere of mistrust”¹⁷⁷ that “unnecessarily further complicated an important decision in the case.”¹⁷⁸

In addition, the Select Subcommittee conducted oversight into Fulton County District Attorney Fani Willis’s politicized prosecution of President Trump. Just days before Willis indicted President Trump, her campaign highlighted the investigation into President Trump in an effort to raise money.¹⁷⁹ Members of Willis’s team also met with the Biden-Harris White House, Special Counsel Smith’s team, and with individuals connected with the Democrat-led partisan January 6th Committee.¹⁸⁰ The Select Subcommittee also investigated the reported misuse of federal funds by Willis’s office.¹⁸¹ As part of this investigation, and after receiving credible

and his team, by their own admission, “thought the ‘closest analog’ to the Stone conviction was that of Scooter Libby, a target of a previous special counsel in a highly controversial prosecution.” *Id.* “Libby’s proposed sentencing range was 30-37 months and he was sentenced to 30 months,” which former President George W. Bush “derided as ‘excessive.’” *Id.*; Scott Shane, et al., *Bush Commutes Libby Sentence, Saying 40 Months ‘Is Excessive,’* N.Y. TIMES (July 3, 2007).

¹⁷¹ *Id.* at 2 (citing OIG Report at 18-19).

¹⁷² *Id.* (citing Hemingway, *supra* note 169).

¹⁷³ *Id.* (citing OIG Report at 17).

¹⁷⁴ *Id.* (citing OIG Report at 31 (“[Cooney] explained that he did not have any direct knowledge as to Shea’s motivations to conclude that Shea was, in fact, being influenced by something other than the facts of the case.”)).

¹⁷⁵ *Id.* (citing OIG Report at 83).

¹⁷⁶ *Id.* (citing OIG Report at 74).

¹⁷⁷ *Id.*

¹⁷⁸ *Id.* (citing OIG Report at 78).

¹⁷⁹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Fani T. Willis, Dist. Att’y, Fulton Cty. Dist. Att’y’s Office at 1 (Aug. 24, 2023) (citing Tim Darnell, ‘We have an announcement’ – Fulton DA Willis launches fundraising website, ATLANTA NEWS FIRST (Aug. 10, 2023)) (hereinafter “Willis Letter”).

¹⁸⁰ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Nathan Wade (Jan. 12, 2024); *See, e.g.*, Glenn Thrush & Danny Hakim, *Georgia Case Lays the Ground for Parallel Prosecutions of Trump*, N.Y. TIMES (Aug. 15, 2023); Betsy Woodruff, et al., *Jan. 6 committee helped guide early days of Georgia Trump probe*, POLITICO (Jan. 10, 2024).

¹⁸¹ *See* Willis Letter, *supra* note 179.

whistleblower testimony to that effect, the Committee subpoenaed the Fulton County District Attorney’s Office (FCDAO) for documents, records, and correspondence relating to its receipt and use of federal funds.¹⁸² Further, the Select Subcommittee conducted a deposition of Nathan Wade, a former Special Prosecutor for the FCDAO, regarding his tenure and his experience leading the FCDAO’s investigation and indictment of President Trump and his allies.¹⁸³ During the deposition, the Select Subcommittee learned that, even before she assumed office in January 2021, Willis was preparing to prosecute President Trump.¹⁸⁴ Wade also confirmed that he and other employees of the FCDAO had several meetings with Biden-Harris White House officials during the FCDAO’s investigation of President Trump, but refused to disclose critical details about such meetings.¹⁸⁵ Wade also that he had several meetings with “individuals associated with the [Select Committee to Investigate the January 6th Attack on the United States Capitol],” but refused to disclose any relevant details about the meetings.¹⁸⁶ Additionally, the Select Subcommittee learned that, prior to his appointment as a Special Prosecutor, Wade had no relevant experience to serve in such role, and that he had to attend trainings to gain relevant experience.¹⁸⁷

Partisan Democrats weaponized the rule of law through the use of lawfare tactics to target Republicans, and particularly President Trump. These actions are a vivid demonstration of a two-tiered system of justice that extends from the highest offices in the Justice Department to the local and state law-enforcement offices run by some ambitious Democrat prosecutors. Rather than debate political opponents on substance, Democrats employed partisan lawfare as a strategy to attempt to win the 2024 election. It is clear that Democrats will continue to use lawfare in the future to undermine legitimate candidates and take electoral decisions away from voters.

* * *

Throughout the 118th Congress, the Select Subcommittee sought to protect and strengthen the fundamental rights of the American people. Through these investigations, the Select Subcommittee has heard from federal officials, concerned citizens, and whistleblowers. Through numerous reports and hearings, the Select Subcommittee has crafted legislation and influenced federal agencies to change policies to ensure that the federal government ceases working against its citizens.

¹⁸² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Fani T. Willis, Dist. Att’y, Fulton Cty. Dist. Att’y’s Off. (Feb. 2, 2024) (enclosing subpoena to the FCDAO for two categories of documents and communications).

¹⁸³ See Deposition of Mr. Nathan Wade, former Special Prosecutor, Fulton Cty. Dist. Att’y’s Off. (Oct. 15, 2024).

¹⁸⁴ *Id.* at 52-54.

¹⁸⁵ *Id.* at 122-24.

¹⁸⁶ *Id.* at 94-98, 106-12.

¹⁸⁷ *Id.* at 53-56.



**AN ANATOMY OF A POLITICAL PROSECUTION: THE MANHATTAN DISTRICT
ATTORNEY'S OFFICE'S VENDETTA AGAINST PRESIDENT DONALD J. TRUMP**

Interim Staff Report of the
Committee on the Judiciary
U.S. House of Representatives



April 25, 2024

EXECUTIVE SUMMARY

If the prosecutor is obliged to choose his cases, it follows that he can choose his defendants. Therein is the most dangerous power of the prosecutor: that he will pick people that he thinks he should get, rather than pick cases that need to be prosecuted.

– Attorney General Robert H. Jackson, April 1, 1940¹

The New York County District Attorney’s Office’s (DANY) multi-year investigation into former President Donald J. Trump is unprecedented. As revealed in former Special Assistant District Attorney Mark F. Pomerantz’s self-serving book, *People vs. Trump: An Insider’s Account*,² since at least 2018, the DANY has weaponized the criminal justice system, scouring every aspect of President Trump’s personal life and business affairs, going back decades, in the hopes of finding some legal basis—however far-fetched, novel, or convoluted—to bring charges against him. When one legal theory would not pan out, instead of discontinuing its politically motivated investigation, the DANY simply pivoted to a new theory, constantly searching for a crime—any crime—to prosecute President Trump.

The story behind the DANY’s investigation into President Trump and the people involved illustrate the clear partisan aim of this case. Pomerantz is a former federal prosecutor who eagerly volunteered to serve as a special assistant district attorney to solely work on the efforts to prosecute President Trump.³ Working under former District Attorney Cyrus Vance, Pomerantz assisted with “lead[ing] the effort” in developing a case against President Trump until he abruptly resigned in February 2022 shortly after District Attorney Alvin Bragg took office.⁴ Prior to his election, Bragg openly boasted about his experience suing the Trump Administration “more than 100 times” and campaigned on a platform of “holding [President Trump] accountable.”⁵ However, when Bragg did not move quickly enough to file charges against President Trump,⁶ Pomerantz opted to go public, writing a book and orchestrating a pressure campaign to force Bragg into action.⁷ And it worked.

Pomerantz’s book, described as a “300-page exercise in score-settling and scorn,”⁸ revealed the extent to which the DANY’s investigation of President Trump was politically motivated. Pomerantz described his eagerness to investigate President Trump, writing that he

¹ Robert H. Jackson, Atty Gen., U.S. Dep’t of Justice, Address at the Second Annual Conference of United States Attorneys: The Federal Prosecutor at 4 (Apr. 1, 1940) [hereinafter 1940 Attorney General Jackson Speech].

² MARK POMERANTZ, *PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT* (2023).

³ *Id.* at 7, 21.

⁴ Shayna Jacobs, *Ex-prosecutor’s book could hurt Trump investigation, district attorney worries*, WASH. POST (Jan. 18, 2023).

⁵ Maria Ramirez Uribe & Loreben Tuquero, *Here’s what Manhattan District Attorney Alvin Bragg said about Donald Trump during his DA campaign*, POLITIFACT (Apr. 12, 2023).

⁶ Jacobs, *supra* note 4.

⁷ Ruth Marcus, *Trump prosecutor Mark Pomerantz was wrong to litigate-and-tell*, WASH. POST (Feb. 8, 2023).

⁸ Lloyd Green, *People vs Donald Trump review: Mark Pomerantz pummels Manhattan DA*, THE GUARDIAN (Feb. 11, 2023).

was “delighted” to join an unpaid group of lawyers advising on the Trump investigation, and joking that salary negotiations had gone “great” because he would have paid to join the investigation.⁹ He baselessly compared President Trump to notorious mob boss John Gotti,¹⁰ and claimed that the District Attorney’s Office was “warranted in throwing the book” at President Trump because, in Pomerantz’s view, the “collective weight” of President Trump’s conduct over the years “left no doubt in [his] mind that [President] Trump deserved to be prosecuted.”¹¹ In other words, as a special assistant district attorney empowered by New York County, Pomerantz seemed, for reasons unrelated to the facts of this particular investigation, to have been searching for any basis on which to bring politically motivated criminal charges against President Trump.¹²

The DANY has been investigating President Trump since at least 2018, searching for any legal theory on which to bring charges.¹³ One legal theory pushed by Pomerantz suffered from serious deficiencies—notably the credibility of the star witness, convicted perjurer Michael Cohen—so much so that the case became known as the “zombie” case.¹⁴ On April 4, 2023, District Attorney Bragg succumbed to Pomerantz’s pressure campaign, charging President Trump with 34 felony counts for falsifying business records.¹⁵ These charges are normally misdemeanors subject to a two-year statute of limitations, but Bragg used a novel and untested legal theory—previously declined by federal prosecutors—to bootstrap the misdemeanor allegations as a felony, which extended the statute of limitations to five years, by alleging that records were falsified to conceal a second crime.¹⁶

The timing and basis for the DANY’s prosecution of President Trump provide a clear inference that Bragg is motivated by political calculations. The facts at the center of Bragg’s political prosecution have not changed since 2018 and no new witnesses emerged between then and the date on which Bragg filed the indictment.¹⁷ The Justice Department examined the facts in 2019 and chose not to prosecute the case. Even still, according to reporting, Bragg “convened a new grand jury in January [2023] to evaluate the issue.”¹⁸ Bragg ultimately settled on a novel legal theory untested anywhere in the country and one that federal authorities declined to pursue to resurrect the matter. The only intervening factor, it appears, was President Trump’s

⁹ POMERANTZ, *supra* note 2, at 6, 21–22.

¹⁰ *Id.* at 108–09.

¹¹ *Id.* at 112–13.

¹² See Rachel Maddow Show, *Watch Rachel Maddow Highlights: Feb. 6*, YOUTUBE (Feb. 6, 2023) (“[W]e were trying to work quickly. Bringing a racketeering case, particularly one that includes [other crimes], it’s such a big ball of wax that, ultimately, we decided, you know what, let’s focus on a smaller, more contained set of charges. That’s when we started to focus on the financial statements.”).

¹³ Andrew Feinberg, *New York prosecutors warn Trump of possible indictment, report says*, THE INDEPENDENT (Mar. 10, 2023).

¹⁴ POMERANTZ, *supra* note 2, at 36–38, 46.

¹⁵ See Indictment, *People v. Donald J. Trump* (N.Y. 2023).

¹⁶ See *id.*; Ben Protess, et al., *In Trump Case, Bragg Pursues a Common Charge With a Rarely Used Strategy*, N.Y. TIMES (May 7, 2023); Jonathan Turley, *Get ready for Manhattan DA’s made-for-TV Trump prosecution: high on ratings, but short on the law*, THE HILL (Mar. 18, 2023).

¹⁷ Mark Berman et al., *The prosecutor, the ex-president and the ‘zombie’ case that came back to life*, WASH. POST (Mar. 17, 2023).

¹⁸ *Id.*

announcement that he would be a candidate for President in 2024.¹⁹

Congress has a specific and manifestly important interest in preventing politically motivated prosecutions of current and former Presidents by elected state and local prosecutors, particularly in jurisdictions—like New York County—where the prosecutor is popularly elected and trial-level judges lack life tenure.²⁰ In response to Bragg’s decision to pursue a politically motivated prosecution—while adopting progressive criminal justice policies that allow career “criminals [to] run[] the streets” of Manhattan²¹—the Committee had an obligation to conduct oversight of Bragg’s unprecedented and shocking prosecutorial conduct. The Committee used its constitutional oversight responsibility to understand how public safety funds appropriated by Congress are implemented by local law-enforcement agencies. In addition, Bragg’s decision to pursue criminal charges against a former president and current declared candidate for that office required the Committee to consider potential legislative reforms to insulate current and former Presidents from such politically motivated state and local prosecutions.

To help inform the Committee’s oversight, the Committee sought testimony from Pomerantz about his work on the political prosecution of President Trump. Based on Pomerantz’s unique role as a special assistant district attorney leading the investigation into President Trump, he was uniquely situated to inform the Committee’s oversight and potential legislative reforms. Pomerantz’s public discussion of the investigation in his book and his media tour undercut any argument that he could not comply on the basis of confidentiality or privilege.²² Bragg sued to prevent the Committee from interviewing Pomerantz; however, the U.S. District Court for the Southern District of New York agreed with the Committee and ordered Pomerantz to appear for a deposition.²³ On May 12, 2023, after stonewalling by Pomerantz and the DANY—including a frivolous lawsuit—Pomerantz sat for a deposition.

When Pomerantz appeared before the Judiciary Committee to discuss his book and politically motivated investigation, he was unusually silent—refusing to answer even the most basic of questions. But Pomerantz’s own words, as detailed in his book, paint a startling picture of prosecutorial abuse. Pomerantz’s own words show how the Manhattan District Attorney’s Office, populated with partisans who openly bragged about their desire to get President Trump, used its immense power in the persecution of a person, not a crime.

¹⁹ Max Greenwood, *Trump announces 2024 run for president*, THE HILL (Nov. 15, 2022).

²⁰ See Letter from Rep. Jim Jordan, H. Comm. on the Judiciary, et al., to Alvin L. Bragg, Jr., Manhattan District Att’y (Mar. 25, 2023).

²¹ Alyssa Guzman, *Priorities, eh? Woke DA Alvin Bragg who’s set to indict Trump is one of America’s most controversial prosecutors after charging self-defense shopkeeper with murder and sending soft-on-crime memo*, DAILY MAIL (Mar. 18, 2023); Andrea Cavallier, *REVEALED: Woke Manhattan DA Alvin Bragg has downgraded over HALF of felony cases to misdemeanors as criminals are free to roam streets of the Big Apple*, DAILY MAIL (Nov. 27, 2022).

²² See Letter from Rep. Jim Jordan, H. Comm. on the Judiciary, to Mark F. Pomerantz, Former N.Y. Co. Special Assistant District Att’y (Apr. 6, 2023).

²³ See Opinion and Order Denying Temporary Restraining Order, *Bragg v. Jordan*, 1:23-cv-3032 (MKV) (S.D.N.Y. Apr. 19, 2023).

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS	4
I. INTRODUCTION.....	5
A. Bragg’s Disregard for Rising Violent Crime in New York City	6
B. The DANY’s Politicized Prosecution of President Trump Has Been an Ongoing Effort Led by Politically-Biased Prosecutors	9
C. The Committee’s Oversight of the DANY’s Unprecedented and Politically Motivated Prosecution.....	11
D. Federal Court Ordered Pomerantz to Cooperate with the Committee’s Oversight	12
E. Pomerantz Appeared for His Deposition but Declined to Answer Most Questions.....	13
II. POMERANTZ WAS HIRED BY THE DISTRICT ATTORNEY FOR NEW YORK COUNTY SOLELY TO DEVELOP A CASE AGAINST PRESIDENT TRUMP	16
III. POMERANTZ WAS FANATICAL ABOUT PROSECUTING PRESIDENT TRUMP	18
A. Pomerantz Shifted Through Many Novel and Untested Legal Theories in Search of a Crime.....	18
B. Pomerantz’s Politicized Reliance on Convicted Perjurer Michael Cohen.....	19
C. Pomerantz’s Personal Animus Towards and Obsession with President Trump	24
IV. POMERANTZ RESIGNED AFTER BRAGG INITIALLY REFUSED TO AUTHORIZE THE PROSECUTION OF PRESIDENT TRUMP	27
V. UNDER PUBLIC PRESSURE FROM POMERANTZ, DISTRICT ATTORNEY BRAGG RESURRECTED THE “ZOMBIE” CASE AGAINST PRESIDENT TRUMP.....	30
VI. THE COMMITTEE’S PROPOSED LEGISLATIVE REFORMS TO ADDRESS POLITICIZED PROSECUTIONS	32
VII. CONCLUSION	34
APPENDIX	35

I. INTRODUCTION

Since at least 2018, the DANY has been investigating President Trump, looking for any legal theory on which to bring charges. The facts surrounding DANY’s case against President Trump have “been known for years.”²⁴ Michael Cohen, President Trump’s disgraced former lawyer and convicted perjurer, pleaded guilty over five years ago to charges based on the same facts.²⁵ At the time, the Justice Department determined that no one else was responsible for the conduct.²⁶ Yet, in April 2023, Bragg indicted President Trump on the same facts.²⁷

There are special responsibilities and principles that come with being a prosecutor. As Attorney General Robert Jackson warned in 1940, “[t]herin is the most dangerous power of the prosecutor: that he [can] pick people that he thinks should [be prosecuted], rather than pick cases that need to be prosecuted.”²⁸ And because of this, a “prosecutor has more control over life, liberty, and reputation than any other person in America.”²⁹ A prosecutor—like Alvin Bragg or Mark Pomerantz—“can pick[] some person whom he dislikes . . . and then look[] for an offense”³⁰ And it is at this point where “the real crime becomes that of being unpopular with the predominant or governing group, being attached to the wrong political views”³¹

Because of the potential to abuse these powers, there are several core principles that all prosecutors must follow. Although each jurisdiction has its own standard, the American Bar Association (ABA) provides model standards that “are intended to provide guidance for the professional conduct and performance of prosecutors”³² The standards set forth ideals by which all prosecutors should abide. In particular, Standard 3-1.6, *Improper Bias Prohibited*, states in part:

A prosecutor should not use other improper considerations, such as partisan or political or personal considerations, in exercising prosecutorial discretion. A prosecutor should strive to eliminate implicit biases, and act to mitigate any improper bias or prejudice when credibly informed that it exists within the scope of the prosecutor’s authority.³³

²⁴ Berman, *supra* note 17.

²⁵ Shawna Chen, *Timeline: The probe into Trump’s alleged hush money payments to Stormy Daniels*, AXIOS (Mar. 18, 2023).

²⁶ Letter from Rep. Jim Jordan, H. Comm. on the Judiciary, to Mark F. Pomerantz, Former N.Y. Co. Special Assistant Dist. Att’y (Mar. 22, 2023).

²⁷ See Statement of Facts, *People v. Donald J. Trump* (N.Y. 2023).

²⁸ 1940 Attorney General Jackson Speech at 4-5.

²⁹ *Id.* at 1.

³⁰ *Id.* at 5.

³¹ *Id.*

³² ABA, STANDARDS FOR CRIMINAL JUSTICE, PROSECUTION FUNCTION, Standard 3-1.6(a) (AM. BAR. ASS’N 2017, 4th ed.).

³³ *Id.*

These principles are meant to protect against the risk of unfair prosecutions. A prosecutor must be objective. A prosecutor must prosecute a crime. A prosecutor must not pick a defendant and then go on a hunt to find a case or create a crime.

The DANY under Alvin Bragg and Mark Pomerantz has failed to uphold these principles. The Office has allowed violent crime in Manhattan to rise unabated and go unprosecuted while exploring every avenue and leaving no stone unturned when it comes to investigating and harassing President Trump.

A. Bragg’s Disregard for Rising Violent Crime in New York City

Against the backdrop of District Attorney Bragg’s decision to find any reason to prosecute President Trump are Bragg’s actions to institute pro-crime, anti-victim policies that resulted in an increase in violent crime and created a dangerous community for New York City residents. Immediately upon taking office in January 2022, District Attorney Bragg issued a ten-page policy memorandum to the Manhattan District Attorney Office staff, which instituted progressive soft-on-crime, anti-victim policies.³⁴ This so-called “Day One” memo, dated January 3, 2022, directed his assistant district attorneys not to prosecute several crimes, including trespassing, resisting arrest, and engaging in prostitution.³⁵ The memorandum stated that armed robberies should not be prosecuted as felonies.³⁶ Instead, the new District Attorney directed armed robberies to be considered as misdemeanor larceny unless someone was shot during the course of the robbery.³⁷ Additionally, Bragg stated that his office will not seek prison sentences except for homicides and other particularly heinous crimes, such as domestic violence felonies, sex crimes, and public corruption.³⁸ The District Attorney also directed his prosecutors to no longer request prison sentences in excess of 20 years, absent “exceptional circumstances.”³⁹

New York’s law enforcement community immediately pushed back on the District Attorney’s Day One memo. On January 7, 2022, New York City Police Commissioner Keechant Sewell sent an email to all 36,000 members of the New York City Police Department (NYPD), writing that she had “studied these [Day One memo] policies and I am very concerned about the implications to your safety as police officers, the safety of the public and justice for the victims.”⁴⁰ Similarly, Patrick Lynch, President of the Police Benevolent Association, said that “police officers don’t want to be sent out to enforce laws that the district attorneys won’t

³⁴ Letter from Alvin L. Bragg, Manhattan Dist. Att’y, to Manhattan Dist. Att’y Staff (Jan. 3, 2022) [hereinafter Day One Memo].

³⁵ *Id.*

³⁶ *Id.*

³⁷ Nicole Gelinas, *Let’s Break Down Exactly What Manhattan DA Alvin Bragg’s Memo Says*, N.Y. POST (Jan. 11, 2022).

³⁸ Day One Memo.

³⁹ *Id.*

⁴⁰ Jonah E. Bromwich & William K. Rashbaum, *Conflict Quickly Emerges Between Top Prosecutor and Police Commissioner*, N.Y. TIMES (Jan. 10, 2022).

prosecute.”⁴¹ The heavy public backlash forced District Attorney Bragg to walk back some of the policies in his Day One memo.⁴²

In 2022, the DANY downgraded a significant number of felony cases to misdemeanors and failed to obtain convictions in the felony cases the office brought. For example, according to data from the District Attorney’s Office, prosecutors downgraded approximately 52 percent of felony charges to misdemeanors charges.⁴³ According to reports, between 2013 and 2020, under former District Attorney Cyrus Vance, the “percentage of cases the office downgraded had never exceeded 40 [percent].”⁴⁴ Furthermore, Bragg’s office secured a conviction on felony charges in just 51 percent of cases, which was “down from 68 [percent] in 2019, the last year before the pandemic disrupted the court system.”⁴⁵ Similarly, the Office’s misdemeanor conviction rate was 29 percent in 2022, down significantly from 68 percent in 2019.⁴⁶

Also in 2022, Bragg’s first year as Manhattan District Attorney, crime in New York City rose significantly when compared to the previous year. According to NYPD data, New York City saw a 23 percent surge in major crimes.⁴⁷ Further, according to reports:

- “[r]apes climbed 7% (1,591 from 1,481);
- felony assaults rose 13 percent (25,596 from 22,738); and
- robberies (17,138 from 13,592) spiked 26%.”⁴⁸

In New York City:

- burglaries went up 23 percent (15,481 from 12,568);
- grand larcenies were up 26 percent (50,698 from 40,166); and
- auto theft increased 32 percent (13,475 from 10,219).⁴⁹

⁴¹ Sonia Moghe, *Manhattan district attorney announces he won’t prosecute certain crimes*, CNN (Jan. 6, 2022).

⁴² Jonah E. Bromwich, *Manhattan D.A. Sharpens Crime Policies That Led to Weeks of Backlash*, N.Y. TIMES (Feb. 4, 2022).

⁴³ Melissa Klein, *NYC convictions plummet, downgraded charges surge under Manhattan DA Bragg*, N.Y. POST (Nov. 26, 2022).

⁴⁴ *Id.*

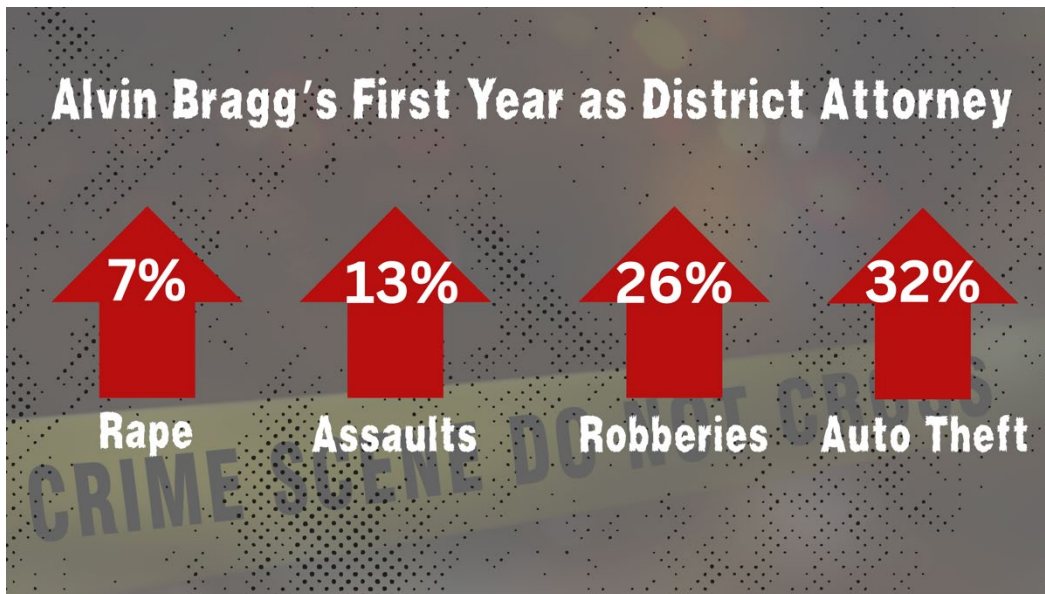
⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ See Dean Balsamini, *NYC murders down but major crimes surge as 2022 draws to a close*, N.Y. POST (Dec. 31, 2022).

⁴⁸ *Id.*

⁴⁹ *Id.*



Because of Bragg's disregard for rising crime in New York City, the Committee held a hearing in Manhattan to examine violent crime in Manhattan and how Bragg's left-wing policies harm the people he was elected to serve.⁵⁰ The Committee received testimony from a parent whose son was attacked "in the heart of Times Square . . . because he was Jewish and wearing a kippa."⁵¹ Bragg offered one of the attackers a "sweetheart slap-on-the-wrist deal."⁵² The parent said that Bragg's decision was "exemplary" of his "incompetence when it comes to carrying out justice."⁵³

The Committee also received testimony from Madeline Brame, whose son was murdered by four people in the streets of Harlem.⁵⁴ Bragg's predecessor, District Attorney Cyrus Vance, originally prosecuted the four suspects, but soon after Bragg took office, "[t]he case immediately began to fall apart with the complete dismissal of 1st degree gang assault [and] 2nd degree murder indictments against 2 of the defendants . . ."⁵⁵ Ms. Brame made clear that "DA Bragg ha[d] demonstrated over and over again that he has no regard or concern for human life or victims of crime . . ."⁵⁶ Yet, despite his decision to not prosecute such heinous crimes, Bragg has spent the DANY's resources to prosecute President Trump for his politics, not his criminal conduct.

⁵⁰ *Victims of Violent Crime in Manhattan: Hearing before the H. Comm. on the Judiciary*, 118th Cong. (2023).

⁵¹ *Id.* (testimony of Barry Borgen).

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Id.* (testimony of Madeline Brame).

⁵⁵ *Id.*

⁵⁶ *Id.*

B. The DANY's Politicized Prosecution of President Trump Has Been an Ongoing Effort Led by Politically-Biased Prosecutors

Instead of prosecuting violent crime, the Manhattan criminal justice authorities set their sights on investigating and prosecuting President Trump. Pomerantz's book underscores the nature of this political prosecution. In December of 2020, Carey Dunne, whom at the time served as "counsel to the office of Manhattan district attorney Cyrus ("Cy") Vance," asked Mark Pomerantz to join a group of outside advisors to Vance's team investigating President Trump, which Pomerantz accepted immediately.⁵⁷ On February 2, 2021, Pomerantz was sworn in as a special assistant district attorney.⁵⁸ Pomerantz wrote in his book that he was "enthusiastic about working on the case and happy to work without pay."⁵⁹

Throughout 2020 and 2021, the DANY's investigation of President Trump continued. In November 2021, shortly after Alvin Bragg won the election to be the next District Attorney, Pomerantz sent a memorandum to District Attorney Vance and Dunne expressing his desire to quickly decide whether to prosecute President Trump.⁶⁰ By the end of Vance's term, however, the DANY had not brought charges against President Trump.⁶¹

In January 2022, soon after Bragg took office, Bragg expressed doubts about the case that Pomerantz and Dunne had assembled using novel legal theories against President Trump and, ultimately, decided to suspend the investigation.⁶² This decision prompted Pomerantz and Dunne to resign in protest.⁶³ Pomerantz penned a scathing resignation letter, which was also leaked to the press,⁶⁴ urging Bragg to follow through with the charges against President Trump.⁶⁵

On November 15, 2022, President Trump formally announced that he was running for President in 2024.⁶⁶ A few months later, on February 7, 2023, Pomerantz published his book, *People v. Donald Trump: An Inside Account*, which excoriated Bragg for not aggressively prosecuting President Trump and laid bare the Office's internal deliberations about the

⁵⁷ POMERANTZ, *supra* note 2, at 4.

⁵⁸ *Id.* at 27.

⁵⁹ *Id.* at 22.

⁶⁰ *Id.* at 167, 172.

⁶¹ *See generally id.*

⁶² Shayna Jacobs et al., *Prosecutor who resigned over stalled Trump probe says ex-president committed felonies*, WASH. POST (Mar. 23, 2022).

⁶³ *Id.*; POMERANTZ, *supra* note 2, at 247, 252.

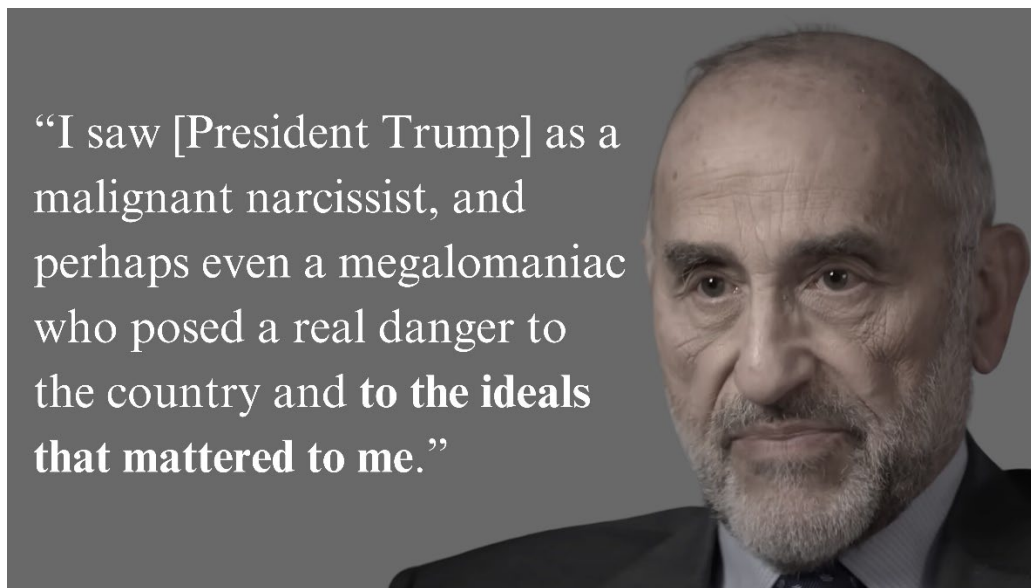
⁶⁴ *See* Ankush Khardori, *The Untold Story of the Lost Trump Investigation Thanks to Mark Pomerantz's fight with Alvin Bragg, we know more than ever*, N.Y. MAG. (Feb. 9, 2023) ("But last February, Pomerantz and a second lawyer, Carey Dunne, ignited a media firestorm when they resigned following Bragg's decision. Since then, senior officials in the DA's office had come to believe he selectively and misleadingly leaked information to the press, including his resignation letter, in order to damage the then newly elected DA. (Pomerantz writes that he 'never' spoke 'to the press at all during my tenure with the district attorney's office,' but he is conspicuously silent on whether he spoke to the press after he resigned, which he did.)").

⁶⁵ POMERANTZ, *supra* note 2, at 248–51.

⁶⁶ Greenwood, *supra* note 19.

investigation and political animus toward President Trump.⁶⁷ Pomerantz went on a media tour to promote his book and attack President Trump and Bragg.⁶⁸ Pomerantz did not hide his deep animosity toward President Trump in his memoir or his media tour. For example, he claimed:

- “[Trump’s] empire was built on lies.”⁶⁹
- Trump was “practiced in the art of intimidation.”⁷⁰
- Trump was “ruthless and avaricious,” “a bully,” and “cunning.”⁷¹
- Trump was “a malignant narcissist” and “a megalomaniac” who “posed a real danger to the country and to the ideals that mattered to me.”⁷²
- “His behavior made me angry, sad, and even disgusted.”⁷³



But Pomerantz was not the only DANY prosecutor who openly discussed his animosity towards President Trump. Throughout his campaign for district attorney, Bragg himself made

⁶⁷ See generally POMERANTZ, *supra* note 2.

⁶⁸ See, e.g., 60 Minutes, *Mark Pomerantz on investigating Donald Trump*, CBS NEWS (Feb. 5, 2023).

⁶⁹ *Id.*

⁷⁰ Morning Joe, *Attorney Mark Pomerantz confident Trump book not interfering with investigation*, MSNBC (Feb. 7, 2023).

⁷¹ POMERANTZ, *supra* note 2, at 109.

⁷² *Id.* at 176-177.

⁷³ *Id.* at 177.

clear that he, too, had animosity towards President Trump. Bragg made President Trump a focal point of his campaign.⁷⁴ For example, on December 13, 2020, Bragg stated:

Let's talk about what's waiting for the new DA. The docket. We know there's a Trump investigation. I have investigated Trump and his children and held them accountable for their misconduct with the Trump Foundation. I also sued the Trump administration more than 100 times for DACA, the travel ban, separation of children from their families at the border. So I know that work. I know how to follow the facts and hold people in power accountable.⁷⁵

On March 17, 2021, Bragg indicated that, if elected as district attorney, he “will hold [Trump] accountable”⁷⁶ Just a few days later, on March 23, 2021, he again bragged that he had “sued the Trump administration over 100 times”⁷⁷ In June 2021, Bragg doubled down, stating, “It is a fact that I have sued Trump more than a hundred times. I can't change that fact, nor would I. That was important work. That's separate from anything that the D.A.'s office may be looking at now.”⁷⁸ And on November 23, 2022, Bragg boasted, “I think I'm probably the only lawyer in the country who can say, we are right now, prosecuting a criminal case against the Trump organization.”⁷⁹ In other words, Bragg assumed office with seemingly one goal: to prosecute President Trump. But, as discussed below, after assuming office, something changed—Bragg realized the case was thin and no longer seemed interested in quickly prosecuting President Trump. This prompted Pomerantz to resign. And the case was not resurrected until Pomerantz went public, putting political pressure on Bragg to prosecute President Trump.

C. The Committee's Oversight of the DANY's Unprecedented and Politically Motivated Prosecution

After news broke that DANY would be indicting President Trump, the Committee was concerned about the unprecedented abuse of prosecutorial authority: the indictment of a former President of the United States and current declared candidate for that office. Because of this, the Committee launched an investigation to examine whether legislative reforms are necessary to insulate former and current Presidents from politically motivated prosecutions by state and local officials. Because Pomerantz had spoken publicly about his work in investigating President

⁷⁴ See, e.g., Uribe & Tuquero, *supra* note 5; Katelyn Caralle, *Meet the Dems competing to prosecute Trump: Manhattan DA candidate BRAGGED about suing Donald 'more than 100 times' – while his opponent interviewed to be federal judge but didn't get it*, DAILY MAIL (June 2, 2021).

⁷⁵ Uribe & Tuquero, *supra* note 5; Katelyn Caralle, *Meet the Dems competing to prosecute Trump: Manhattan DA candidate BRAGGED about suing Donald 'more than 100 times' – while his opponent interviewed to be federal judge but didn't get it*, DAILY MAIL (June 2, 2021).

⁷⁶ Uribe & Tuquero, *supra* note 5.

⁷⁷ Emily Ngo, *Why the Manhattan DA Candidates Say They're Ready to Take on the Trump Investigation*, SPECTRUM NEWS NY 1 (Mar. 23, 2023).

⁷⁸ Jonah E. Bromwich et al., *2 Leading Manhattan D.A. Candidates Face the Trump Question*, N.Y. Times (June 2, 2021).

⁷⁹ *Manhattan DA Alvin Bragg on Election Results and More, The Brian Lehrer Show*, WNYC (Nov. 23, 2022) (transcript available at <https://www.wnyc.org/story/manhattan-da-alvin-bragg-election-results-and-more/>).

Trump and the political animus that fueled his work, on March 22, 2023, the Committee asked Pomerantz to provide relevant documents and testimony about his role as a special assistant district attorney leading the investigation into President Trump.⁸⁰ On March 27, 2023, Pomerantz responded to the Committee and stated that, at the DANY’s instruction, he would not cooperate with the Committee’s oversight.⁸¹ In light of Pomerantz’s refusal to cooperate with the Committee, on April 6, 2023, the Committee issued a deposition subpoena to Pomerantz.⁸² In the subpoena’s cover letter, the Committee reiterated that Pomerantz had already discussed the issues the Committee sought information on in both his book and media appearances.⁸³

D. Federal Court Ordered Pomerantz to Cooperate with the Committee’s Oversight

Soon after, on April 11, 2023, District Attorney Bragg filed a lawsuit against the Committee to enjoin its enforcement of the deposition subpoena to Pomerantz, alleging, in part, that the Committee sought “highly sensitive and confidential local prosecutorial information”⁸⁴ On April 19, 2023, Judge Mary Kay Vyskocil eviscerated District Attorney Bragg’s arguments that sought to prevent Pomerantz from appearing before the Committee.⁸⁵ Judge Vyskocil wrote, in part:

The book referenced in [Chairman] Jordan’s letter is *People vs. Donald Trump: An Inside Account*, written by Pomerantz and published in early 2023. As its subtitle indicates, the book recounts Pomerantz’s insider insights, mental impressions, and his front row seat to the investigation and deliberative process leading up to the DANY case against former President and current presidential candidate Donald Trump.

* * *

Bragg cannot seriously claim that any information already published in Pomerantz’s book and discussed on prime-time television in front of millions of people is protected from disclosure as attorney work product (or otherwise).⁸⁶

⁸⁰ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mark F. Pomerantz, Former N.Y. Co. Special Assistant Dist. Att’y (Mar. 22, 2023).

⁸¹ Letter from Mark F. Pomerantz, Former N.Y. Co. Special Assistant Dist. Att’y, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Mar. 27, 2023).

⁸² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mark F. Pomerantz, Former N.Y. Co. Special Assistant Dist. Att’y (Apr. 6, 2023).

⁸³ *Id.*

⁸⁴ Complaint, *Bragg v. Jordan*, 1:23-cv-3032 (MKV) (S.D.N.Y. Apr. 11, 2023).

⁸⁵ Opinion and Order Denying Temporary Restraining Order, *Bragg v. Jordan*, 1:23-cv-3032 (MKV) (SDNY Apr. 19, 2023).

⁸⁶ *Id.* at 2, 22–23 (internal citations omitted).

Judge Vyskocil concluded that the Committee’s “subpoena was issued with a ‘valid legislative purpose’ in connection with the ‘broad’ and ‘indispensable’ congressional power to ‘conduct investigations.’”⁸⁷ The Committee, she added, “identified several valid legislative purposes underlying the subpoena.”⁸⁸ Those legislative purposes includes “the use of federal forfeiture funds in connection with DANY’s investigation of President Trump” and “the possibility of legislative reforms to insulate current and former presidents from state prosecutions[.]”⁸⁹ Judge Vyskocil made clear that Congress has the authority to investigate these legislative reforms.⁹⁰

Bragg and Pomerantz appealed Judge Vyskocil’s ruling and the U.S. Court of Appeals for the Second Circuit granted a temporary administrative stay of the Committee’s deposition subpoena to Pomerantz.⁹¹ After negotiation with the Committee, Pomerantz agreed to sit for a deposition on May 12, 2023, so long as the District Attorney’s Office could have a representative present.⁹²

As a last-ditch effort to prevent Pomerantz from providing meaningful testimony, the DANY threatened to pursue legal charges against Pomerantz because he disclosed details in his book about a pending investigation. Prior to publishing his book, the DANY “warned [him] that [he] could face criminal liability if . . . [he] disclosed grand jury material or violated a provision of the New York City Charter dealing with the misuse of confidential information.”⁹³ Pomerantz heard nothing more from the DANY, however, and his book was released. More than two months after the release of his book, on April 19—after the Committee sought to speak with Pomerantz—the DANY indicated in court that Pomerantz’s book “exposed [him] to criminal liability.”⁹⁴ In other words, the DANY did not take any action or seemingly care about Pomerantz’s book or his media appearances until *after* the Committee expressed interest in speaking to him about it. At that point, the DANY threatened criminal liability to silence Pomerantz.

E. Pomerantz Appeared for His Deposition but Declined to Answer Most Questions

At the deposition on May 12, 2023, Pomerantz was accompanied by his lawyers and Leslie Dubeck, General Counsel for the New York County District Attorney’s Office.⁹⁵ At the outset of the deposition, during his opening statement, Pomerantz indicated that he would invoke

⁸⁷ *Id.* at 1.

⁸⁸ *Id.* at 12.

⁸⁹ *Id.*

⁹⁰ *Id.* at 12-13.

⁹¹ Jane Wester, *2nd Circuit Grants Last-Minute Stay of Pomerantz Deposition Before House Committee*, N.Y. LAW JOURNAL (Apr. 20, 2023).

⁹² Katherine Faulders & Aaron Katersky, *Manhattan DA Bragg, Jordan resolve dispute over deposition of former Trump prosecutor*, ABC NEWS (Apr. 21, 2023).

⁹³ Deposition of Mark F. Pomerantz, Former N.Y. Co. Special Assistant Dist. Att’y, at 10 (May 12, 2023).

⁹⁴ *Id.*

⁹⁵ *Id.* at 5.

three separate reasons to decline to answer certain questions. Pomerantz identified these bases as follows:

- The Manhattan District Attorney’s Office instructed Pomerantz that he should maintain the Office’s claims of privilege and confidentiality to “protect the integrity of the pending prosecution and continuing investigation of Donald Trump,” and thus would not answer questions to which the District Attorney’s Office objected.⁹⁶
- Pomerantz, if necessary, would invoke his rights under the Fifth Amendment to not answer questions that could be used against him in a criminal case.⁹⁷
- Pomerantz indicated that he would decline to answer questions that he independently determined were not related to Congress’s legislative function, or that sought information that was, according to his own analysis, protected by the First Amendment.⁹⁸

Pomerantz invoked these three excuses approximately 216 times.⁹⁹ He invoked the excuses to decline to answer questions unrelated to either investigation—the DANY’s investigation of President Trump or the DANY’s investigation into Pomerantz—such as:

- “Did you have your own desk [at the District Attorney’s Office]?”¹⁰⁰;
- “Since you’ve left the employ of the Manhattan D.A., do you use email as a method of communication?”¹⁰¹; and
- “How long have you known [former district attorney] Cy Vance?”¹⁰²

⁹⁶ *Id.* at 9.

⁹⁷ *Id.* at 9-10.

⁹⁸ *Id.* at 10.

⁹⁹ *Id.* at 12, 13, 14, 15, 16, 17, 18, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 46, 47, 49, 50, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 64, 65, 67, 68, 70, 71, 72, 73, 74, 87, 88, 89, 90, 91, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 106, 107, 108, 110, 111, 113, 114, 116, 117, 118, 122, 123, 125, 126, 127, 128, 129, 130, 131, 132, 133, 135, 136, 137, 138.

¹⁰⁰ *Id.* 107.

¹⁰¹ *Id.* at 90.

¹⁰² *Id.* at 36.

**Pomerantz refused to
answer approximately
216 questions.**



Although Pomerantz's stated rationale for refusing to answer questions related to the investigation into President Trump was largely due to the DANY's pending criminal investigation, Pomerantz also declined to answer any questions regarding communications he has had with the District Attorney's Office regarding its pending criminal investigation of Pomerantz.¹⁰³ However, in his opening statement, Pomerantz broadly stated that he is "certain [he] broke no laws."¹⁰⁴

Beyond acknowledging that he wrote the book, Pomerantz refused to answer questions regarding specific claims and statements made in his book. However, Pomerantz testified that his book is accurate, that there are no lies in the book, and that he stands fully behind it.¹⁰⁵

¹⁰³ *E.g., id.* at 113 ("Respectfully, I decline to answer your question about communications with the District Attorney's Office.").

¹⁰⁴ *Id.* at 10.

¹⁰⁵ *Id.* at 39.

II. POMERANTZ WAS HIRED BY THE DISTRICT ATTORNEY FOR NEW YORK COUNTY SOLELY TO DEVELOP A CASE AGAINST PRESIDENT TRUMP

Pomerantz’s book confirms that his decision to join the Manhattan District Attorney’s Office was driven by political animus. In December 2020, Carey Dunne, counsel to then-New York County District Attorney Cyrus Vance, recruited Pomerantz to “join[] a group of outside lawyers who would advise Cy Vance in connection with his pending investigation of Donald Trump.”¹⁰⁶ Pomerantz was “delighted”¹⁰⁷ to do so, as it “would allow [him] to peek through the window at whatever the district attorney was doing” in the investigation.”¹⁰⁸ He nonetheless acknowledged that “the concept of a public prosecutor’s office convening an advisory group of private lawyers to help with a pending investigation seemed a bit odd.”¹⁰⁹

It was through this advisory group that Pomerantz learned that the “DA’s investigation of [President] Trump was much broader” than just an alleged “hush money” payment, “and would grow to cover many aspects of his business operations.”¹¹⁰ During the advisory group’s first call, “[t]he main topic of the conversation, and the issue that seemed to have prompted the formation of the ‘outside advisors’ group,”¹¹¹ was alleged “fraud in connection with taxation of [President Trump’s] 40 Wall Street building by undervaluing his property.”¹¹² At that time, “presentation of felony charges to grand juries had come to a virtual standstill” due to New York City’s COVID-19 pandemic related closures.¹¹³ Dunne and Vance therefore asked the advisory group “to provide a reality check on whether” the DANY could or should file a felony complaint as opposed to the traditional method of empaneling a grand jury to secure an indictment.¹¹⁴

Pomerantz recalled that the felony complaint idea “never got off the ground,” however, because the “NYC’s Law Department advised DANY that ‘everybody’ submits lowball property valuations in the effort to lower property taxes on Manhattan office buildings.”¹¹⁵ The city explained that the “owner’s initial valuation figures are not taken seriously, and are regarded as simply the first step in a series of negotiations.”¹¹⁶ Despite the fact that “the city did not regard itself as having been defrauded,”¹¹⁷ Pomerantz believed that President Trump “would have been a good target for prosecution”¹¹⁸ because “there was the aggravating factor that . . . he had urged the public to trust in his integrity by running for the presidency.”¹¹⁹ The DANY nonetheless

¹⁰⁶ POMERANTZ, *supra* note 2, at 4.

¹⁰⁷ *Id.* at 6.

¹⁰⁸ *Id.*

¹⁰⁹ *Id.* at 7.

¹¹⁰ *Id.* at 8.

¹¹¹ *Id.* at 8-9.

¹¹² *Id.* at 10.

¹¹³ *Id.* at 9-10.

¹¹⁴ *Id.* at 11.

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ *Id.* at 12.

¹¹⁹ *Id.*

elected not to further pursue charges related to President Trump’s 40 Wall Street property at that time.¹²⁰

Although “the DANY investigative team . . . had identified several areas of inquiry into Trump’s activities,”¹²¹ Pomerantz was concerned that the DANY’s investigation was too sprawling, unfocused, and in need of a “narrator.”¹²² Pomerantz explained that white-collar cases often feature a “narrator” to explain the suspicious transactions, events, and circumstances to the jury.¹²³ Most of the time, this “narrator” is able to tell jurors about a defendant’s crimes because they played a part in committing them.¹²⁴

By mid-January, Pomerantz noted “[t]here was a long and unfocused laundry list of topics to investigate, no reliable cooperator other than Michael Cohen (a convicted perjurer), and DANY was still waiting to receive Trump’s tax and accounting materials.”¹²⁵ At that point, Pomerantz emphasized that he was merely an “outside advisor” who “did not have a big emotional investment in the investigation.”¹²⁶

A few days after President Trump left the White House in late-January 2021, Vance asked Pomerantz to “join the investigation as more than an outside advisor” and “be sworn in as a special assistant district attorney” to work exclusively on the investigation into President Trump.¹²⁷ Pomerantz replied that he “was ready, willing, and able to get started as soon as [he] could be sworn in.”¹²⁸ He even joked that salary negotiations had gone “great” because he and Vance had “reached agreement that [Pomerantz] would work on the case for nothing before [he] was even asked how much [Pomerantz] was willing to pay the DA’s office!”¹²⁹

Pomerantz’s discussion of this offer reveals his animus, both personally and politically, against President Trump and the thrill he felt in being given the opportunity to bring a criminal case against President Trump. Although Pomerantz asserted in his book that his “enthusiasm to work on the investigation had nothing to do with [his] views about Trump’s politics,” he simultaneously detailed the reasons he was “not a fan”¹³⁰ of and “had little regard”¹³¹ for President Trump.¹³²

¹²⁰ *Id.*

¹²¹ *Id.* at 13.

¹²² *Id.* at 15.

¹²³ *Id.*

¹²⁴ *Id.* at 79.

¹²⁵ *Id.* at 18.

¹²⁶ *Id.* at 18.

¹²⁷ *Id.* at 21.

¹²⁸ *Id.*

¹²⁹ *Id.* at 22.

¹³⁰ *Id.* at 23.

¹³¹ *Id.* at 22.

¹³² *Id.* at 23.

III. POMERANTZ WAS FANATICAL ABOUT PROSECUTING PRESIDENT TRUMP

Mark Pomerantz’s book details his infatuation with investigating and prosecuting President Trump. Pomerantz’s overzealousness to get President Trump led to him disregarding the fundamental tenets of a prosecutor’s job. It resulted in Pomerantz sifting through several unprecedented and convoluted legal theories in search of a crime. It resulted in Pomerantz relying on a star witness, convicted perjurer Michael Cohen, with a history of lying and a clear animus against President Trump. Pomerantz’s book plainly shows, in black and white, that the Manhattan District Attorney’s prosecution of President Trump is a political hit job.

A. Pomerantz Shifted Through Many Novel and Untested Legal Theories in Search of a Crime

Throughout his book, Pomerantz explained that he considered many legal theories to prosecute President Trump. Pomerantz made clear that his goal was to prosecute President Trump, for any crime, and that it was just a matter of finding the crime to pin on him.¹³³ After he was sworn in, Pomerantz considered alleged “hush money” payments, which the DANY had been investigating since 2018.¹³⁴ By the end of 2019, however, Vance elected not to bring charges “against anyone in connection with the hush money paid to [Stephanie] Clifford or the phony invoicing scheme by which Michael Cohen had been reimbursed for the money he had laid out.”¹³⁵ Pomerantz explained that although the alleged “hush money and phony invoicing scheme had generated false business records, . . . creating a false business record is only a misdemeanor under New York law”¹³⁶ with a maximum jail sentence of less than a year.¹³⁷

When President Trump left office, Pomerantz decided to “revisit”¹³⁸ “whether there were other felony charges that could be brought in connection with the payment that Cohen had made to Clifford and the ensuing coverup.”¹³⁹ Pomerantz at this point concocted a “novel legal theory” under New York’s money laundering statute, which he admitted was “neither intuitive nor obvious.”¹⁴⁰ Money laundering, as he explained, is a series of financial transactions that are designed to “conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of criminal conduct.”¹⁴¹ Pomerantz’s money laundering theory was “novel” because the “proceeds” were based on Clifford’s criminal conduct, i.e., her “extortion of Donald

¹³³ See generally POMERANTZ, *supra* note 2.

¹³⁴ *Id.* at 43-44.

¹³⁵ *Id.* at 41-42.

¹³⁶ *Id.* at 40.

¹³⁷ See N.Y. PENAL LAW § 175.05 (“Falsifying business records in the second degree is a class A misdemeanor.”); N.Y. PENAL LAW § 70.15 (“A sentence of imprisonment for a class A misdemeanor shall be a definite sentence. When such a sentence is imposed the term shall be fixed by the court, and shall not exceed three hundred sixty-four days.”).

¹³⁸ POMERANTZ, *supra* note 2 at 43.

¹³⁹ *Id.* at 44.

¹⁴⁰ *Id.* at 58.

¹⁴¹ *Id.* at 44; N.Y. PENAL LAW § 470.10.

Trump.”¹⁴² That legal theory fizzled out when Pomerantz realized that New York’s money laundering statute required the payments that Cohen allegedly agreed to be made on Trump’s behalf—or the “dirty money” to have been actually received by Clifford.¹⁴³

After realizing that there was no criminal case on the Clifford facts, Pomerantz began focusing on President Trump’s Statements of Financial Condition (SOFC), which he believed, based on the claims of Michael Cohen, must be criminal.¹⁴⁴ Pomerantz began examining multiple years’ worth of the financial statements made for multiple golf properties, Deutsche Bank, the Old Post Office Hotel, Doral Resort, Trump International Hotel & Tower in Chicago, Mar-A-Lago, Seven Springs, 40 Wall Street, the Triplex Apartment, and Trump Tower.¹⁴⁵

Pomerantz further explored the possibility of charging President Trump under New York’s Enterprise Corruption statute involving “pattern crimes.”¹⁴⁶ In effect, Pomerantz sought to amalgamate several unrelated and baseless allegations against President Trump into a crime. Pomerantz’s actions make clear that he prejudged the results of this case and had decided that President Trump would be prosecuted for some crime—any crime—but it was just a matter of finding the crime to pin on him.

Pomerantz had one serious issue, though: his colleagues did not entirely agree with him. In his book, Pomerantz made clear his contempt for his DANY colleagues. Pomerantz accused his fellow DANY lawyers and investigators of being “relentlessly negative, dwelling on all the difficulties and issues with the case, and refusing to acknowledge the positives” during an internal meeting on December 10, 2021, referring to his former colleagues as “conscientious objectors”¹⁴⁷ merely for opining that the case was “weak” and pointing to its “many fatal flaws.”¹⁴⁸ He ultimately dismissed their concerns about the investigation by suggesting that they were either too lazy to do the work, did not know the evidence, or were somehow afraid of bringing charges against President Trump.¹⁴⁹

B. Pomerantz’s Politicized Reliance on Convicted Perjurer Michael Cohen

One of the more bizarre aspects of Pomerantz’s book is his reverence for Michael Cohen, President Trump’s disgraced former lawyer. Cohen, a convicted felon who lied six times before

¹⁴² POMERANTZ, *supra* note 2, at 57.

¹⁴³ *Id.* at 60.

¹⁴⁴ *Id.* at 97-100.

¹⁴⁵ *Id.* at 64, 74, 99, 152, 165, 167, 185, 208.

¹⁴⁶ *Id.* at 105-106.

¹⁴⁷ Of his DANY team, Pomerantz states: “[I]t was frustrating to feel like we were about to march into battle, and were strapping on our guns and equipment, but when we looked around at the rest of the platoon we saw a lot of conscientious objectors.” *Id.* at 194.

¹⁴⁸ *Id.* at 191-92, 194.

¹⁴⁹ *Id.* at 160, 171-72.

Congress,¹⁵⁰ has a demonstrable prejudice against President Trump, which gives him a serious credibility problem.¹⁵¹

In August 2018, Cohen “pleaded guilty to five counts of willful tax evasion; one count of making false statements to a bank; one count of causing an unlawful campaign contribution; and one count of making an excessive campaign contribution.”¹⁵² Three months later, Cohen also pleaded guilty to lying to Congress.¹⁵³ Federal prosecutors in Manhattan described Cohen’s criminal conduct in that case as “knowing and calculated acts—acts Cohen executed in order to profit personally, build his own power, and enhance his level of influence.”¹⁵⁴ When sentencing Cohen in 2018, Judge William H. Pauley, III called his wrongdoing “extensive” and “a veritable smorgasbord of fraudulent conduct.”¹⁵⁵ Judge Pauley found that all of Cohen’s crimes “involved deception and each appears to have been motivated by personal greed and ambition.”¹⁵⁶

Even after he pleaded guilty of lying to Congress, Cohen lied to Congress again. On February 28, 2019, Republicans on the House Committee on Oversight and Reform referred Cohen to the Department of Justice for committing perjury and knowingly making false statements during his testimony before the Committee on February 27.¹⁵⁷ Cohen lied repeatedly in his testimony, making willfully and intentionally false statements that were contradicted by the record established by the Justice Department in *United States v. Cohen*.¹⁵⁸ Parts of Cohen’s testimony were in direct contradiction to assertions made by the U.S. Attorney’s Office for the Southern District of New York (SDNY) in its pleadings.¹⁵⁹ Other parts of Cohen’s testimony were immediately contradicted by witnesses with firsthand knowledge of the subject matter.¹⁶⁰ For example, Cohen denied committing various fraudulent acts, such as defrauding a bank,

¹⁵⁰ See, e.g., Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight & Accountability, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov’t Operations, to Hon. William P. Barr, Att’y Gen., U.S. Dep’t of Justice (Feb. 28, 2019).

¹⁵¹ See, e.g., Nicholas Fandos & Maggie Haberman, *In Congressional Testimony, Cohen Plans to Call Trump a ‘Con Man’ and a ‘Cheat’*, N.Y. TIMES (Feb. 26, 2019); Berman, *supra* note 17.

¹⁵² Press Release, U.S. Attorney’s Office, Southern District of New York, Michael Cohen Pleads Guilty In Manhattan Federal Court To Eight Counts, Including Criminal Tax Evasion And Campaign Finance Violations (Aug. 21, 2018); Information, *United States v. Cohen*, No. 18-cr-602 (S.D.N.Y. Aug. 21, 2018).

¹⁵³ Information, *United States v. Cohen*, No. 18-cr-850 (S.D.N.Y. Nov. 29, 2018).

¹⁵⁴ The Government’s Sentencing Memorandum at 27-28, *United States v. Cohen*, No. 18-cr-602 (S.D.N.Y. Dec. 7, 2018).

¹⁵⁵ Statement of Judge William H. Pauley III, *United States v. Cohen*, Nos. 18-cr-602, 18-cr-850, at 31 (S.D.N.Y. Dec. 12, 2018) (sentencing hearing).

¹⁵⁶ *Id.*

¹⁵⁷ Letter from Rep. Jim Jordan & Rep. Mark Meadows to William Barr, Att’y Gen. (Feb. 28, 2019); *Hearing with Michael Cohen, Former attorney for President Donald Trump: Hearing before the H. Comm. on Oversight & Reform*, 116th Cong. (2019).

¹⁵⁸ 18-cr-602 (S.D.N.Y. Aug. 21, 2018); Letter from Rep. Jim Jordan & Rep. Mark Meadows to William Barr, Att’y Gen. (Feb. 28, 2019).

¹⁵⁹ *Id.*; The SDNY, in a court filing, scorched Cohen for his many lies, writing: “After cheating the IRS for years, lying to banks and to Congress, and seeking to criminally influence the Presidential election, Cohen’s decision to plead guilty – rather than seek a pardon for his manifold crimes – does not make him a hero.” The Government’s Sentencing Memorandum, *United States v. Cohen*, 18-cr-602 (S.D.N.Y. Sept. 7, 2018).

¹⁶⁰ *Id.*

despite pleading guilty the year before for making false statements to a banking institute.¹⁶¹ Cohen also “testified that he did not seek employment in the White House,” which was “in direct conflict with court filings made by the United States Attorney’s Office for the SDNY”¹⁶²

In 2023, Cohen, again, admitted to lying to Congress. Just last year, at a court hearing in the lawsuit brought by the New York Attorney General against President Trump, Cohen admitted to lying under oath again at his 2019 deposition before the House Permanent Select Committee on Intelligence.¹⁶³ Cohen was asked if he lied during the deposition when asked if he was directed to inflate certain financial numbers.¹⁶⁴ Cohen responded, “Yes.”¹⁶⁵ This prompted the Chairman of the House Permanent Select Committee on Intelligence, Congressman Mike Turner, to send a criminal referral to the Department of Justice demanding that the Department investigate Cohen for perjury and knowingly making false statements to Congress.¹⁶⁶

Cohen’s metamorphosis into a crusader against President Trump appears to have been orchestrated, in part, by Lanny Davis, a prominent Democrat activist and longtime Clinton-family confidant.¹⁶⁷ Just months before hiring Davis, Cohen admitted that he had no incriminating information about President Trump. Based on information made available to the Committee, in April 2018, when federal law enforcement investigated Cohen for his crimes, his attorney asked him if he had “any info on Trump,” to which Cohen replied that “he didn’t have anything on him, nothing.” Cohen also vowed, though, to never spend a day in jail, telling his attorney, “One thing I can tell you is that I am never going to spend one day in jail, never. I will do what I have to do, but I will never spend one day in jail.” In the following months, however, Cohen flipped, and Davis began to use Cohen to attack and undermine President Trump for political advantage.

Davis admitted that he orchestrated Cohen’s testimony to Congress, recalling how he “convinced [then Oversight Committee] Chairman Cummings to make Cohen the first announced witness of his chairmanship” and “Chairman Cummings agreed to [Davis’s] overtures”¹⁶⁸ Chairman Cummings, under the pressure of Davis, also “unilaterally and

¹⁶¹ Letter from Rep. Jim Jordan & Rep. Mark Meadows to William Barr, Att’y Gen. (Feb. 28, 2019).

¹⁶² *Id.*

¹⁶³ Letter from Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence, and Elise Stefanik, Member of Congress, to Merrick Garland, Att’y Gen., U.S. Dep’t of Justice (Nov. 14, 2023) (citing Transcript of Record at 2407:24-2410:22, *People of the State of New York v. Donald J. Trump et al.*, No. 452564/2022, Part 37 (N.Y. Sup. Ct. Oct. 25, 2023)).

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

¹⁶⁶ Letter from Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence, and Elise Stefanik, Member of Congress, to Merrick Garland, Att’y Gen., U.S. Dep’t of Justice (Nov. 14, 2023).

¹⁶⁷ Darren Samuelsohn, *Michael Cohen hires Clinton scandal veteran Lanny Davis*, POLITICO (July 5, 2018).

¹⁶⁸ Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight & Accountability, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov’t Operations, to Lanny Davis (Feb. 21, 2019).

unnecessarily attempted to limit the scope of Cohen’s testimony.”¹⁶⁹ Davis also bragged about how he was responsible for Bragg’s prosecution, explaining that he called the New York County District Attorney’s office, led at the time by Cyrus Vance, after “Michael was sent to prison” because “the evidence of financial fraud was on the record in the [congressional] hearings and that Vance’s office should interview Michael And that’s how it began.”¹⁷⁰



In their first meeting during Cohen’s home confinement, Pomerantz said Cohen impressed him as “smart but manipulative,” because he reminded Pomerantz of a cooperating drug dealer who testified for him in a trial forty years ago, and he thought Cohen was telling the truth.¹⁷¹ Blinded by the idea of using Cohen in a prosecution against President Trump, Pomerantz looked past the fact that Cohen had his “own agenda” and the likelihood that “jurors would know that Cohen was furious with Donald Trump, and wanted to see him convicted.”¹⁷² Specifically, Pomerantz recounted that Cohen “did not have to be pressured, cajoled, or coaxed into answering questions” because Cohen “wanted to make sure that Donald Trump was prosecuted and held accountable for his crimes.”¹⁷³

¹⁶⁹ *Id.*; Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight & Accountability, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov’t Operations, to Rep. Elijah E. Cummings, Chairman, H. Comm. on Oversight & Accountability (Jan. 31, 2019) (“Davis exclusively picked our Committee for Cohen to testify in based on his longstanding friendship with you. Davis allowed he had to convince both you and Cohen to have the hearing According to Davis, you seemingly had your own reservations, but Davis told us after “one or two months” you finally came around[.]”).

¹⁷⁰ Politico Staff, *Porn Stars, felons, and spin doctors: Who will jurors believe in Trump’s case?*, POLITICO (Mar. 24, 2023).

¹⁷¹ POMERANTZ, *supra* note 2, at 49.

¹⁷² *Id.* at 51–52.

¹⁷³ *Id.*

DANY prosecutors raised red flags about Cohen’s participation in a case against President Trump. Pomerantz recounted in his book how DANY prosecutors reacted negatively when Pomerantz mentioned Cohen’s potential involvement in their litigation plans.¹⁷⁴ For example, during a meeting with Bragg’s new team, Pomerantz argued that Cohen’s testimony would be part of their proof against President Trump, and the team’s discussion “degenerated into chaos and confusion.”¹⁷⁵ Pomerantz’s defense for Cohen’s liabilities as a witness was “virtually all cooperators have liabilities,” and Pomerantz believed that “most” of the team agreed Cohen was eligible to testify.¹⁷⁶ Yet, Cohen continued to be a point of contention between Pomerantz and his DANY colleagues in further discussions about charging President Trump, resulting in Pomerantz frequently defending the convicted perjurer.¹⁷⁷

Pomerantz even continued to defend Cohen’s credibility when Cohen made enthusiastic public appearances after New York State Attorney General Letitia James filed a petition to compel President Trump and members of his family to give depositions in her civil investigation.¹⁷⁸ Even though Cohen’s “penchant for publicity, exaggeration, and grandiose statements played into the hands of people who distrusted him,” Pomerantz deflected this “self-aggrandizement,” explaining that he did not view Cohen as an “inveterate liar,” but merely a “complicated person.”¹⁷⁹ In the face of opposition from his DANY colleagues about the wisdom of relying on Cohen, Pomerantz wrote that he felt like he was “always arguing the reasons for prosecuting Trump until [he] was blue in the face.”¹⁸⁰

Pomerantz recounted a “mini-revolt” that occurred following an internal meeting on September 21, 2021, about the investigations into President Trump.¹⁸¹ He offered details about a disagreement between himself and the DANY’s Major Economic Crimes Bureau Chief, Julieta Lozano, about Michael Cohen’s credibility as a witness in the investigation.¹⁸² He also complained about concerns expressed by Chris Conroy, the DANY’s Investigative Division Chief, during a meeting on November 12, 2021.¹⁸³ According to Pomerantz, Conroy “spoke about his misgivings” about the Trump investigation, which stemmed from a case involving financial and accounting fraud charges that mirrored the charges that the DANY was considering pursuing against President Trump.¹⁸⁴ That case apparently ended poorly for the DANY.¹⁸⁵

Early on in District Attorney Bragg’s tenure, Pomerantz defended using Cohen as a witness against President Trump to Bragg. At one point during a team meeting, Bragg told

¹⁷⁴ *See, e.g., id.* at 159, 212-13.

¹⁷⁵ *Id.* at 213.

¹⁷⁶ *Id.* at 159.

¹⁷⁷ *Id.* at 208–09, 213, 227.

¹⁷⁸ *Id.* at 211.

¹⁷⁹ *Id.* at 226.

¹⁸⁰ *Id.* at 225.

¹⁸¹ *Id.* at 159.

¹⁸² *Id.*

¹⁸³ *Id.* at 171.

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

Pomerantz “that he ‘could not see a world’ in which we would indict Trump and call Michael Cohen as a prosecution witness.”¹⁸⁶ But it seems, in less than a year, Bragg’s view of Cohen drastically changed. In addition to the novel and untested legal theory Bragg used in President Trump’s indictment, Michael Cohen has become Bragg’s star witness.¹⁸⁷ Bragg’s case relies heavily on the testimony of Michael Cohen, a perjurer with a demonstrable prejudice against President Trump.¹⁸⁸ Cohen has been vocal about his deeply personal animus toward President Trump.¹⁸⁹ Ultimately, the idea of utilizing Michael Cohen as a witness in *any* case against President Trump should be a red flag given Cohen’s obvious vendetta and numerous public attacks against President Trump.

C. Pomerantz’s Personal Animus Towards and Obsession with President Trump

Although Pomerantz contends that he only “wanted the Trump case brought because [he] thought a prosecution was necessary to serve the public interest,”¹⁹⁰ he makes little effort to hide his personal animus towards President Trump in his book. His *ad hominin* characterizations of President Trump include, among other things:

- An “unscrupulous wheeler-dealer”¹⁹¹ with a “narcissistic personality;”¹⁹²
- A “bully”¹⁹³ with an “affinity for lying;”¹⁹⁴
- A “master of breaking the law”¹⁹⁵ who is “incredibly cheap and completely dishonest;”¹⁹⁶
- A “malignant narcissist”¹⁹⁷ and “megalomaniac”¹⁹⁸ who “pos[ed] a real danger to the country and to the ideals that mattered . . . ;”¹⁹⁹
- A “ruthless and avaricious”²⁰⁰ businessman with “a dark side to his prosperity;”²⁰¹ and

¹⁸⁶ *Id.* at 208–09, 213, 227.

¹⁸⁷ Berman, *supra* note 17.

¹⁸⁸ Christopher Lopez, *Progressive DA Alvin Bragg’s case against Trump hinges on witnesses with ‘credibility problems’*: Andy McCarthy, FOX NEWS (Mar. 19, 2023); Marisa Schultz, *Jim Jordan, Mark Meadows ask Justice Department to probe Cohen for perjury*, N.Y. POST (Feb. 28, 2019).

¹⁸⁹ *See, e.g.*, Nicholas Fandos & Maggie Haberman, *supra* note 151.

¹⁹⁰ POMERANTZ, *supra* note 2, at 264.

¹⁹¹ *Id.* at 22.

¹⁹² *Id.* at 98.

¹⁹³ *Id.* at 109.

¹⁹⁴ *Id.* at 103.

¹⁹⁵ *Id.* at 112.

¹⁹⁶ *Id.* at 99.

¹⁹⁷ *Id.* at 176–77.

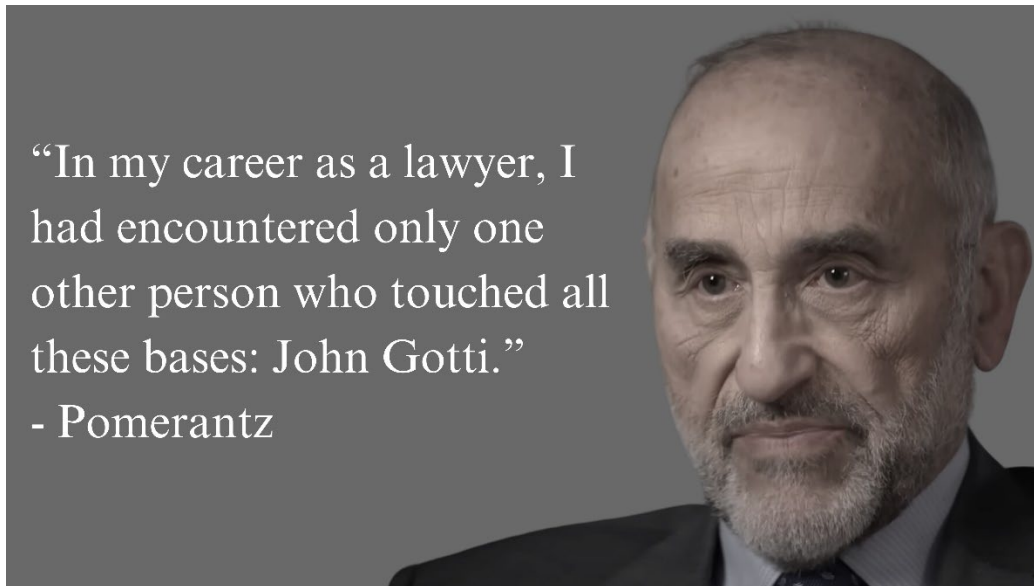
¹⁹⁸ *Id.* at 177.

¹⁹⁹ *Id.*

²⁰⁰ *Id.* at 109.

²⁰¹ *Id.*

- “[N]ot just a pathological liar, but a hapless, arrogant, and horrible liar”²⁰² who “could no longer process the difference between [expletive] and reality.”²⁰³



Pomerantz revealed his overwhelming contempt for President Trump when he likened him to convicted mob boss John Gotti, writing that “[i]n my career as a lawyer, I had encountered only one other person who touched all these bases: John Gotti.”²⁰⁴ While Pomerantz repeatedly denied that his political motive drove his investigation of President Trump, he admitted that he volunteered thousands of hours of his time, working day and night, pouring through hundreds of thousands of documents, and canceling vacations, all to try to figure out if some convoluted legal theory could be used to bring a criminal case against President Trump.²⁰⁵

The personal sacrifices that Pomerantz made in pursuit of his goal of prosecuting President Trump are not that of someone who “did not have a big emotional investment in the investigation.”²⁰⁶ For example, Pomerantz wrote, “[I] decided to plunge into the task of learning everything I could about Trump’s financial statements . . . I would work for a few hours, walk the dog to break up the monotony, come back to the statements and spreadsheets and work for a few more hours, and walk the dog again.”²⁰⁷ Pomerantz claimed that he “was completely submerged in the fact investigation, doing witness outlines and interviews, parsing documents, reading through testimony transcripts, and doing a million other things. By this point I was

²⁰² *Id.* at 103.

²⁰³ *Id.* at 187.

²⁰⁴ *Id.* at 109.

²⁰⁵ *See id.* at 119, 201.

²⁰⁶ *Id.* at 18.

²⁰⁷ *Id.* at 94.

working days, evenings, and weekends.”²⁰⁸ Pomerantz even admitted to spending “thousands of hours thinking about Donald Trump’s conduct . . .”²⁰⁹

For the investigation, Pomerantz accumulated “a small library” of books specifically for this investigation, including “Cohen’s book, *Disloyal*, and another fifteen or so Trump-related books I immersed myself in what had been written about Trump’s business empire and . . . began a detailed study of Trump’s yearly financial statements, thinking that they might become the fulcrum of a case against him . . .”²¹⁰

Even during a hurricane, Pomerantz prioritized President Trump over everything else. During Hurricane Ida in 2021, Pomerantz and his wife “watched with dismay as the water level rose around our home, and finally water began pouring into the house.”²¹¹ Rather than worrying about themselves or items of sentimental or personal value, Pomerantz and his wife “scurr[ie]d around [their] home office to rescue all of [his] Trump files from the flood and carry them upstairs to safety.”²¹² Pomerantz and his wife even went as far as “cancel[ing] [their] stay in Sonoma for most of the winter” even though it may have “meant forfeiting the large deposit [they] had paid to rent a house there. There was just too much to do to finalize the charges and get ready for the return of the Trump indictment.”²¹³

These are not actions of a prosecutor seeking to do justice. These are the actions of a rogue, overzealous prosecutor acting with political motivations. And that motivation infected the investigation from the start.

²⁰⁸ *Id.* at 158.

²⁰⁹ *Id.* at 285

²¹⁰ *Id.* at 91.

²¹¹ *Id.* at 156.

²¹² *Id.* at 156.

²¹³ *Id.* at 201.

IV. POMERANTZ RESIGNED AFTER BRAGG INITIALLY REFUSED TO AUTHORIZE THE PROSECUTION OF PRESIDENT TRUMP

On January 1, 2022, Alvin Bragg was sworn in as New York County’s District County.²¹⁴ Pomerantz noted that on that day, “things started to go south almost immediately.”²¹⁵ Pomerantz and Dunne had “growing unease” about the pace of the investigation into President Trump—even after meeting with Bragg and his team several times.²¹⁶ On January 8, 2022, Pomerantz met individually with Bragg. During the one-on-one, Pomerantz told Bragg that his case against President Trump “was ready to be charged.”²¹⁷ On January 11, 2022, Pomerantz and Dunne gave a presentation on former President Trump’s financial statements to Bragg and his team.²¹⁸ At this meeting, Bragg’s team expressed “considerable ‘angst’” about using Cohen as a witness and sought to pivot away from Pomerantz’s suggested fraud charges.²¹⁹

On January 24, 2022, according to Pomerantz, an investigative team meeting “quickly degenerated into a whirlwind of negativity” because other DANY officials rightly questioned the credibility of Pomerantz’s main witness, Michael Cohen.²²⁰ Pomerantz also took issue with the fact that Bragg seemed disinterested in the meeting—Bragg arrived late to the meeting, “spent much of the time looking at his phone, and then left early . . .”²²¹ Two days later, Pomerantz and Dunne agreed that both would resign if Bragg did not move forward with an indictment and exchanged resignation letters for the other to review.²²² Prior to a scheduled surgery, which he had “delayed . . . because work had become so frenzied,” Pomerantz “prepared a resignation letter . . . [to] inform [Bragg] that [he] did not want to continue ‘in the absence of clarity about a decision to prosecute and without the ability to secure the resources that [he] believe[d] the case require[d].’”²²³ Pomerantz did not follow through with submitting this resignation letter and, instead, “in the wee hours of the morning” before the scheduled surgery, Pomerantz decided to write a “blunt” letter to Bragg indicating that he was “not happy” with how Bragg was handling the investigation.²²⁴

²¹⁴ Michael Gold & Jonah E. Bromwich, *Who Is Alvin Bragg, the D.A. Leading the Prosecution of Trump*, N.Y. TIMES (Apr. 13, 2023).

²¹⁵ POMERANTZ, *supra* note 2, at 201.

²¹⁶ *Id.* at 202, 203, 205–07, 207–08, 212–13.

²¹⁷ *Id.* at 205-07.

²¹⁸ *Id.* at 207-08.

²¹⁹ *Id.* at 208-209.

²²⁰ *Id.* at 212 (“As I started to detain Cohen’s potential testimony against Trump, Susan Hoffinger brought her phone out to play a recording of one of Cohen’s recent media appearances, in which he had taken credit as the person who had first spoken about he false financial statements and had crowed about his importance as a witness in the case. This was exactly opposite to the point I was making at the meeting . . .”); *Id.* at 213 (“Although the new team knew nothing about the underlying facts, and nothing about how the Weisselberg case had been put together, they had read the defense motion papers attributing critical importance to Cohen, dumping all over him, and claiming that he had tainted the prosecution.”).

²²¹ *Id.* at 213.

²²² *Id.* at 217.

²²³ *Id.* at 217.

²²⁴ *Id.* at 217-220.

Throughout the first few weeks of February 2022, Pomerantz and Dunne held several conversations with Bragg and his team to explain their multi-faceted investigation into President Trump.²²⁵ After one of the sessions, Pomerantz indicated he felt that it was “us vs. them” with regards to Bragg’s team and how they viewed the investigation.²²⁶

On February 20, 2022, Bragg indicated that he would not authorize the prosecution based upon the facts that Pomerantz and Dunne had developed, prompting Pomerantz to formally resign on February 23, 2022.²²⁷ In his resignation letter, which was leaked to the *New York Times*, Pomerantz offered a scathing rebuke of Bragg, vowing to not be a “passive participant” to Bragg’s “grave failure of justice.”²²⁸ Pomerantz’s public resignation reportedly left Bragg “deeply stung,” and caused him to issue an “unusual” public statement, “emphasizing that the investigation into Trump and his business was far from over.”²²⁹

Notably, Pomerantz’s resignation letter had several misleading and inconsistent statements. In his resignation letter, Pomerantz wrote, “[t]he team that has been investigating Mr. Trump harbors no doubt about whether he committed crimes – he did.”²³⁰ Pomerantz’s book, however, told a different story. By his own admission, during a December 9, 2021 meeting with attorneys in the District Attorney’s Office, many of the lawyers were “relentlessly negative.”²³¹ Pomerantz noted that “one lawyer opined that it had ‘many fatal flaws.’”²³² Another lawyer “expressed a view that the case might be ‘way out there.’”²³³ Pomerantz later stated that “[i]t was common knowledge in the office that there had been ‘defectors’ from the Trump investigation.”²³⁴ Bragg also told Pomerantz that “the consensus among the group of prosecutors with whom he had been speaking was not to go forward.”²³⁵

Pomerantz also wrote in his resignation letter that “I and others have advised you that we have evidence sufficient to establish Mr. Trump’s guilt beyond a reasonable doubt, and we believe that the prosecution would prevail if charges were brought and the matter were tried to an impartial jury.”²³⁶ In his book, however, Pomerantz wrote, “I know that the case against Donald Trump is not an easy one, and there is a big risk that it will not end in a conviction. It is

²²⁵ *Id.* at 221-26, 228.

²²⁶ *Id.* at 228.

²²⁷ *Id.* at 243-252; Shayna Jacobs & Josh Dawsey, *Prosecutors in Trump probe quit after new DA seems to abandon plan to seek indictment of former president*, WASH. POST (Feb. 23, 2022).

²²⁸ *Read the Full Text of Mark Pomerantz’s Resignation Letter*, N.Y. TIMES (Mar. 23, 2022).

²²⁹ Mark Berman et al., *The prosecutor, the ex-president and the ‘zombie’ case that came back to life*, WASH. POST (Mar. 17, 2023).

²³⁰ POMERANTZ, *supra* note 2, at 249.

²³¹ *Id.* at 191-92.

²³² *Id.*

²³³ *Id.* at 192.

²³⁴ *Id.* at 209.

²³⁵ *Id.* at 230.

²³⁶ *Id.* at 250.

impossible to quantify that risk. I believe that the prosecution would prevail, but a lot of uncertainty is baked into the situation.”²³⁷

Finally, Pomerantz wrote in his resignation letter, “You have devoted significant time and energy to understanding the evidence we have accumulated with respect to the Trump financial statements, as well as the applicable law.”²³⁸ This assertion, too, is inconsistent with Pomerantz’s description of Bragg in his book. At the outset of his book, Pomerantz claimed Bragg “was responsible for a ‘grave failure of justice’” for not promptly indicting President Trump.²³⁹ Pomerantz went on to write that Bragg was “distracted” and “thought about Alvin’s relative youth and wondered if he was in over his head.”²⁴⁰ He accused Bragg of not “jump[ing] in to embrace the investigation or to learn the facts.”²⁴¹ Pomerantz also believed that it was better for Bragg to send his investigation to the U.S. Attorney’s Office “than simply ‘take a knee’ by keeping the case in the district attorney’s office to die a lingering death.”²⁴²

²³⁷ *Id.* at 235.

²³⁸ *Id.* at 249.

²³⁹ *Id.* at 1.

²⁴⁰ *Id.* at 218–19.

²⁴¹ *Id.* at 201.

²⁴² *Id.* at 243.

**V. UNDER PUBLIC PRESSURE FROM POMERANTZ, DISTRICT ATTORNEY BRAGG
RESURRECTED THE “ZOMBIE” CASE AGAINST PRESIDENT TRUMP**

Though both the SDNY and DANY previously declined to further investigate the alleged hush money payments to Clifford,²⁴³ Bragg opted to revive the DANY’s investigation at a politically opportune moment. Shortly after President Trump announced his White House run, the DANY pivoted back to what Pomerantz frequently referred to as the “zombie” case that originated nearly five years ago.²⁴⁴ The case earned its zombie nickname due to a tendency it had to “[spring] back to life” as it did in 2019, 2021, and again in 2023.²⁴⁵ Nonetheless, Bragg’s decision to bring forth this case following Pomerantz’s public pressure campaign—and after essentially abandoning the DANY’s previous Trump investigations at the beginning of his tenure²⁴⁶—raises considerable suspicion as to whether political pressure played a role in his decision.

According to Pomerantz, the “zombie” case had multiple pitfalls, and notwithstanding possible “work-arounds,” Pomerantz wrote that none were appealing.²⁴⁷ Further, his DANY colleagues were “dubious about whether Trump had been ‘extorted’ in the first place.”²⁴⁸ However, Bragg may have decided to move forward on this matter purely for convenience and familiarity. Pomerantz noted that in October 2019, well before New York citizens elected Bragg, the DANY prosecutors and investigators “had done a lot of work developing the facts surrounding the [Clifford] hush money payment,” and “ramped up their efforts” once federal prosecutors said they were finished looking at this information.²⁴⁹

In the following months, Bragg and his team at the DANY likely noticed the acclaim that New York Attorney General Letitia James received from Democrats for bringing a civil action against President Trump, his children, and the Trump Organization.²⁵⁰ Bragg experienced bad press almost immediately at the start of his term because he announced in a memorandum that he would not prosecute certain “low-level crimes, all while promising to downgrade criminal charges and to decriminalize crimes such as resisting arrest.”²⁵¹ Subsequently, when Pomerantz and Dunne resigned, prominent voices on the left attacked Bragg, in part, for his inaction on

²⁴³ POMERANTZ, *supra* note 2, at 39, 61; *see also* Berman, *supra* note 17; Chen, *supra* note 25.

²⁴⁴ POMERANTZ *supra* note 2, at 46; *see also* William K. Rashbaum et al., *Manhattan prosecutors begin presenting Trump case to grand jury*, N.Y. TIMES (Jan. 30, 2023).

²⁴⁵ Rashbaum, *supra* note 244; *see also* POMERANTZ, *supra* note 2, at 39, 42, 46, 61.

²⁴⁶ POMERANTZ, *supra* note 2, at 249.

²⁴⁷ *Id.* at 61.

²⁴⁸ *Id.*

²⁴⁹ *Id.* at 39.

²⁵⁰ Tristan Snell (@TristanSnell) TWITTER (Aug. 10, 2022, 10:49 AM), <https://twitter.com/TristanSnell/status/1557378663615692801>; *see also* Jonah E. Bromwich et al., *Hyperbole or fraud? The question at the heart of Trump investigation*, N.Y. TIMES (Jan. 19, 2022).

²⁵¹ Carl Campanile, *Petition to oust Manhattan DA Alvin Bragg renews bid for recalls in NY*, N.Y. POST (Jan. 12, 2022).

President Trump.²⁵² In other words, as a popularly elected prosecutor, Bragg needed a political win by the end of his first year in office to enhance his public standing.

Bragg also had to consider his political future. During his race for District Attorney, Bragg made big promises to go after President Trump. Bragg frequently reminded voters that while working at the New York Attorney General’s office, he sued the Trump Administration “more than a hundred times.”²⁵³ A spokeswoman for Bragg’s primary opponent even noted that Bragg attacked President Trump “for political advantage every chance he gets.”²⁵⁴ Bragg’s eventual election and subsequent blunder with his Day One memorandum put additional pressure on his decision to resurrect the “zombie” case as a vehicle to deliver on his campaign promises. It is this improper political bias that fueled Bragg to reevaluate his prior decision, vowing instead that his investigation of President Trump was continuing as he noted in an interview the day that Pomerantz and Dunne resigned.²⁵⁵ In fact, Bragg noted that he hoped “driving down gun violence and the population at Rikers while pushing ahead on the Trump investigation . . . [would] ‘neutralize’ the noise around him.”²⁵⁶

Fast forward to March 2023, and Bragg seemed to have succumbed to that noise. Bragg opted to file charges, even though multiple years had passed since the DANY initiated its investigation and the facts of the “zombie” case had remained unchanged.²⁵⁷ The facts had not changed. The law had not changed. The credibility of Bragg’s star witness, Michael Cohen, had not improved. There was only one significant intervening factor between the DANY’s previous decision not to pursue charges and Bragg’s indictment: President Trump announced his candidacy for the 2024 presidential election.

²⁵² Jonah E. Bromwich, *Alvin Bragg says he’s not a politician. Is that the root of his trouble?* N.Y. TIMES (Apr. 9, 2022) (“Between the backlash to the [Day One] memo and the fallout from the Trump investigation, Bragg managed, in less than 12 weeks, an unlikely feat: He united the New York Post’s editorial board and the viewers of MSNBC in a posture of mutual disdain.”); *Id.* (Congressman Daniel Goldman, who was not in public office at the time, stated, “That transition has been bumpy for Alvin and I think that when you get off to a bad start, it’s very difficult to get back on the right track[.]”); Glenn Kirschner, *This New York prosecutor thinks Trump is guilty. Why won’t the DA charge him?*, MSNBC (Mar. 30, 2022).

²⁵³ Bromwich, *supra* note 78.

²⁵⁴ *Id.*

²⁵⁵ Bromwich, *supra* note 252.

²⁵⁶ *Id.*

²⁵⁷ See Statement of Facts, *People v. Donald J. Trump* (N.Y. 2023); Berman, *supra* note 17; Ian Millhiser, *The dubious legal theory at the heart of the Trump indictment, explained*, VOX (Apr. 4, 2023).

VI. THE COMMITTEE’S PROPOSED LEGISLATIVE REFORMS TO ADDRESS POLITICIZED PROSECUTIONS

Bragg’s indictment of President Trump is just the tip of the iceberg for politically motivated prosecutions, and the Committee intends to investigate the circumstances out of which this litigation was reborn. Contrary to Bragg’s assertion in defense of his unprecedented indictment,²⁵⁸ the indictment of a former President of the United States by an elected local prosecutor of the opposing political party (who faces the prospect of re-election to office, much like President Trump is seeking), implicates substantial *federal* interests. Bragg’s indictment of President Trump has led to copycat indictments by other politically motivated, popularly elected local prosecutors.

On August 14, 2023, Fulton County District Attorney Fani Willis brought a 41-count indictment against 19 defendants, including President Trump, alleging that they participated in a “criminal enterprise.”²⁵⁹ Like Bragg, the Committee has sought information from Willis about her use of federal grant funds,²⁶⁰ and the Justice Department has acknowledged there are “inconsistencies” in her actions.²⁶¹ If state or local prosecutors like Bragg and Willis are allowed to engage in politically motivated prosecutions of former or current U.S. Presidents for personal acts, this could have a profound impact on how Presidents choose to exercise their official duties while in office.

There are several pieces of legislation pending in Congress to address these politically motivated local prosecutions. Congressman Russell Fry introduced H.R. 2553, the No More Political Prosecutions Act, a bill that would provide former and current Presidents and Vice Presidents the option to remove their own civil or criminal cases from a state court to a federal court.²⁶² On September 28, 2023, the Committee approved H.R. 2553, reporting it to the floor for consideration by the full House.²⁶³ Congressman Andy Biggs has introduced two bills: (1) H.R. 2581, the Accountability for Lawless Violence In Our Neighborhoods Act, which would “prohibit[] federal funds from being awarded to the Manhattan District Attorney’s Office and

²⁵⁸ Letter from Leslie B. Dubeck, Gen. Counsel, N.Y. Co. District Att’y Off., to Rep. Jim Jordan, H. Comm. on the Judiciary, et al. (Mar. 23, 2023).

²⁵⁹ Indictment, *Georgia v. Donald John Trump et al.*, No. 23SC188947 (Aug. 14, 2023, Fulton Co. Sup. Ct.); The Committee remains engaged with both the Fulton County District Attorney’s office and the Department of Justice to obtain information regarding the federal grants received by the Fulton County DA’s office. The Committee has subpoenaed the Fulton County DA’s office to obtain relevant records and have received document productions pursuant to that subpoena. Though the Fulton County DA’s office produced some documents, its compliance with the Committee’s subpoena remains deficient. *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Dist. Att’y Fani T. Willis, Fulton Cnty. Dist. Atty’s Office (Mar. 14, 2024).

²⁶⁰ *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Dist. Att’y Fani T. Willis, Fulton Cnty. Dist. Att’y’s Office (Mar. 14, 2024).

²⁶¹ Andrew Kerr, *Justice Department Uncovers ‘Inconsistencies’ in Fani Willis’s Use of Federal Grant Funds*, WASH. FREE BEACON (Apr. 10, 2024).

²⁶² Press Release, *Congressman Russell Fry (SC-07) Introduces the No More Political Prosecutions Act* (Apr. 11, 2023).

²⁶³ No More Political Prosecutions Act of 2023, H.R. 2553, 118th Cong. (2023) (as reported by H. Comm. on the Judiciary, Sept. 28, 2023).

requires the Office to repay federal funds granted after January 1, 2022”; and (2) H.R. 2582, the No Federal Funds for Political Prosecutions Act, which would “prohibit[] state or local law enforcement agencies from using funds or property seized through asset forfeiture, to investigate or prosecute the President, Vice President, or a candidate for the office of President in a criminal case.”²⁶⁴ The Committee continues to examine areas in which it can legislate to ensure former or current Presidents are not subject to politically-motivated prosecutions like those undertaken by Bragg and Willis. There is no place for local, politically motivated prosecutors to weaponize the criminal justice system against former or current Presidents.

²⁶⁴ Accountability for Lawless Violence In our Neighborhoods Act, H.R. 2581, 118th Cong. (2023); No Federal Funds for Political Prosecutions Act, H.R. 2582. 118th Cong. (2023).

VII. CONCLUSION

Despite Pomerantz's refusal to answer questions throughout his deposition, his book makes one thing clear: from the start, the New York County District Attorney's investigation, and later indictment, of President Trump is a product of prosecutorial focus on one individual in search of a crime. Pomerantz, in his own words, confirms what Americans instinctively know. Pomerantz was a politically motivated prosecutor who sought to use the immense resources available to him to charge President Trump under a novel legal theory and suspect evidence—evidence on which federal prosecutors refused to bring charges. Like Pomerantz, Bragg's actions showed that he, too, was a politically motivated prosecutor. During his campaign, Bragg bragged about suing President Trump several times. The DANY allowed political motivations and animus to infect its prosecutorial discretion. As a result, the DANY now has a case that rests on questionable and untested legal grounds.²⁶⁵

The New York County District Attorney's indictment of President Trump opened a dangerous new possibility of politically motivated prosecutions or threatened prosecutions of political opponents, including presidents. This case establishes a dangerously low threshold for these investigations and prosecutions to commence. With this indictment, Bragg has opened the door for future prosecutions of a former president—or current candidate—that would be widely perceived as politically motivated. As we have already seen, other prosecutors have followed Bragg's lead and pursued politically motivated investigations and indictments of President Trump.

The fundamental mission of any prosecutor's office is to uphold the rule of law. And one of the hallmarks of this mission is to ensure that justice is blind—applied fairly and equally. Bragg's politically motivated indictment of President Trump threatens to destroy this notion of blind justice by using the criminal justice system to attack an individual he disagrees with politically, and, in turn, eroding the confidence of the American people.

²⁶⁵ See, e.g. Millhisser, *supra* note 257; Richard L. Hasen, *Donald Trump Probably Should Not Have Been Charged With (This) Felony*, SLATE (Apr. 4, 2023); Jonathan Turley, *Bragg's case is a legal mess – what is he even charging Trump with?*, N.Y. POST (Apr. 4, 2023).

APPENDIX

1. January 11, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, to the Hon. Elijah E. Cummings, Chairman, H. Comm. on Oversight and Reform.
2. January 15, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, to the Hon. Elijah E. Cummings, Chairman, H. Comm. on Oversight and Reform.
3. January 22, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to Guy Petrillo.
4. January 31, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to the Hon. Elijah E. Cummings, Chairman, H. Comm. on Oversight and Reform.
5. February 21, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to Lanny Davis.
6. February 25, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to the Hon. Elijah E. Cummings, Chairman, H. Comm. on Oversight and Reform.
7. February 28, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to the Hon. William Barr, Atty Gen., U.S. Dep't of Justice.
8. March 8, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to Michael D. Monico.
9. March 13, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to the Hon. Elijah E. Cummings, Chairman, H. Comm. on Oversight and Reform.
10. June 7, 2019: Letter from Rep. Jim Jordan, Ranking Member, H. Comm. on Oversight and Reform, and Rep. Mark Meadows, Ranking Member, Subcomm. on Gov't Operations, to the Hon. Elijah E. Cummings, Chairman, H. Comm. on Oversight and Reform.

Reform.

11. March 20, 2023: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, Rep. Bryan Steil, Chairman, H. Comm. on House Administration, and Rep. James Comer, Chairman, H. Comm. on Oversight and Accountability to Alvin L. Bragg Jr., Dist Atty., New York County.
12. March 22, 2023: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Carey R. Dunne.
13. March 22, 2023: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mark F. Pomerantz.
14. March 23, 2023: Letter from Alvin L. Bragg Jr., Dist Atty., New York County, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, Rep. Bryan Steil, Chairman, H. Comm. on House Administration, and Rep. James Comer, Chairman, H. Comm. on Oversight and Accountability
15. March 25, 2023: Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, Rep. Bryan Steil, Chairman, H. Comm. on House Administration, and Rep. James Comer, Chairman, H. Comm. on Oversight and Accountability, to Alvin L. Bragg Jr., Dist Atty., New York County.
16. March 27, 2023: Letter from Carey R. Dunne, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary.
17. March 27, 2023: Letter from Mark F. Pomerantz, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary.
18. April 6, 2023: Subpoena Cover Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mark F. Pomerantz.
19. April 19, 2023: Opinion and Order Denying Temporary Restraining Order, Bragg v. Jordan, 1:23-cv-3032 (MKV) (SDNY Apr. 19, 2023).
20. May 12, 2023: Deposition of Mark F. Pomerantz



Congress of the United States
House of Representatives
Washington, DC 20515

January 11, 2019

The Honorable Elijah E. Cummings
Chairman
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

It has now been twenty months since the inception of the Special Counsel Robert S. Mueller III probe.¹ During this period, the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) refused to allow Members of Congress to inquire about unsubstantiated allegations and admissions made by Michael D. Cohen, citing the Department's position of not discussing ongoing criminal investigations. Over the course of fifteen transcribed interviews before Congress, DOJ and FBI blocked witnesses from answering questions more than seventy times citing the need to prevent revealing information about the Special Counsel's ongoing investigation.

In contrast with your statement expressing, "no interest in inappropriately interfering with any ongoing criminal investigations," one of your first moves as Chairman was to announce a hearing to bring in Michael Cohen, a witness in two high-profile federal criminal investigations, one by the Special Counsel and the other by the U.S. Attorney's Office for the Southern District of New York.² According to your press release, you set this hearing without finishing consultations with the Special Counsel's office. You also did not consult with the minority Members of the Committee. I do understand from public reporting you have been working with Lanny J. Davis in producing the February 7, 2019, hearing.³

¹U.S. Department of Justice, Order Number 3915-2017 (May 17, 2017), <https://www.justice.gov/opa/pr/appointment-special-counsel>.

² Press Release, from Elijah E. Cummings, H. Comm. on Oversight & Reform, Chairman Cummings Announces Oversight Committee Hearing Schedule (Jan. 10, 2019), <https://oversight.house.gov/news/press-releases/chairman-cummings-announces-oversight-committee-hearing-schedule>.

³ See The Beat with Ari Miller, "Michael Cohen's Lawyer on How Cohen Will Expose Trump to Congress", MSNBC, Jan. 10, 2019, <http://www.msnbc.com/the-beat-with-ari-melber/watch/michael-cohen-s-lawyer-on-how-cohen-will-expose-trump-to-congress-1423816771546>; Dan Mangan and Brian Schwartz, "Trump's Ex-Lawyer Michael Cohen will testify Publicly to House Oversight Committee Before Entering Prison", CNBC, Jan. 10, 2019; <https://www.cnbc.com/2019/01/10/ex-trump-lawyer-michael-cohen-to-testify-to-house-oversight-committee.html>; Mark Hosenball, "Ex-Trump Lawyer Cohen to Testify Publicly Before Congress", Reuters, Jan. 10, 2019;

The Honorable Elijah E. Cummings

January 11, 2019

Page 2

This past July you urged the Committee to “protect the integrity of the Special Counsel’s ongoing criminal investigation.”⁴ Your colleagues have likewise emphasized the importance of not interfering with the Special Counsel. In July then-Judiciary Committee Ranking Member Jerrold Nadler asked then-Judiciary Chairman Bob Goodlatte, “Are we no longer going to wait until Special Counsel Mueller concludes his work, Mr. Chairman?”⁵ Democrats’ turnabout here is remarkable.

You indicated yesterday you are talking with the Cohen camp about the contours of his testimony. I ask you to include representatives of the minority in future discussions about Cohen’s testimony. Preventing the minority from participating deprives us of the ability to meaningfully prepare our Members for the hearing.⁶ I also understand your staff is now having private conversations with the staff from the Special Counsel’s office. Minority staff should be included in these deliberations as well.

To ensure that all Members of the Committee are prepared adequately for this hearing, I request you seek documents and testimony from DOJ and the FBI, and from Cohen. At minimum, the Committee should take a transcribed interview or depose Cohen before his public testimony. The following documents and information are necessary for the Committee to have a fact-based hearing—and avoid reckless speculation and conjecture at the hearing. Accordingly, I trust you will require the DOJ and the FBI to produce, in unredacted form, the following documents:

1. All FD-302 forms and any other investigative reports created by the DOJ or FBI in their investigations into Michael Cohen;
2. All FD-1023 forms that may have been created involving Michael Cohen;
3. All contact reports involving Michael Cohen and the FBI;
4. All cooperation agreements between Michael Cohen and DOJ;

<https://www.reuters.com/article/us-usa-trump-russia-cohen/former-trump-lawyer-cohen-to-testify-publicly-before-congress-idUSKCN1P42MQ>.

⁴ *Oversight of FBI and DOJ Actions Surrounding the 2016 Election: Hearing Before the H. Comm. on Oversight & Gov’t Reform and H. Comm. on Judiciary: Testimony by FBI Deputy Assistant Director Peter Strzok*, 115th Cong. (July 12, 2018) (statement of Ranking Member Elijah E. Cummings, H. Comm. on Oversight & Gov’t Reform), https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2471-Sharp%20Color%20Copier%40mail.house.gov_20180712_084701_0.pdf.

⁵ *Oversight of FBI and DOJ Actions Surrounding the 2016 Election: Hearing Before the H. Comm. on Oversight & Gov’t Reform and H. Comm. on Judiciary: Testimony by FBI Deputy Assistant Director Peter Strzok*, 115th Cong. (July 12, 2018) (statement of Ranking Member Jerrold Nadler, H. Comm. on Judiciary), <https://judiciary.house.gov/news/press-releases/statement-ranking-member-nadler-hearing-oversight-fbi-and-doj-actions>.

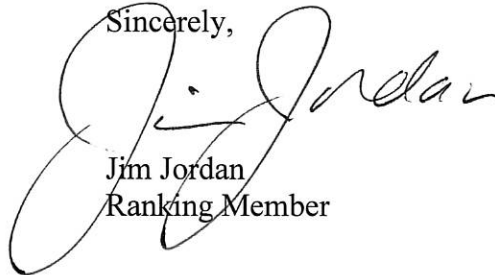
⁶ Maggie Haberman and Nicholas Fandos, *Former Trump Lawyer Michael Cohen Agrees to Testify to Congress*, N.Y. TIMES, Jan. 10, 2019, <https://www.nytimes.com/2019/01/10/us/politics/michael-cohen-trump-testimony.html>.

The Honorable Elijah E. Cummings
January 11, 2019
Page 3

5. All sentencing memorandum prepared by DOJ involving Michael Cohen;
6. All notes taken by DOJ or FBI during their multiple interviews of Michael Cohen;
and
7. Documentation of all agreements Michael Cohen has with DOJ, the FBI, and any other foreign government's law enforcement agencies.

It is incumbent on our Committee to conduct our work thoroughly and responsibly. I hope you will work with me and the minority Members to avoid an unproductive and chaotic hearing. If you are going to provide a platform for this convicted felon and perjurer, we ought to ensure we have the necessary information to prepare to question him. I look forward to hearing back from you as the Committee prepares for this seminal hearing in your tenure.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Jordan". The signature is written in a cursive, flowing style with large loops and a long horizontal stroke at the end.

Jim Jordan
Ranking Member



Congress of the United States
House of Representatives
Washington, DC 20515

January 15, 2019

The Honorable Elijah E. Cummings
Chairman
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am writing to request additional information about the Committee's hearing scheduled for February 7, 2019, at which you have invited Michael D. Cohen, a convicted felon sentenced to prison, to testify.¹ Cohen pleaded guilty to providing intentionally false testimony to a Congressional committee.² You invited Cohen to testify before finishing consultations with the Special Counsel's Office and without consulting the minority.³ As the Committee prepares for your first major hearing, there is still much we do not know about your plans for the hearing.

Shortly after you announced the hearing, Michael Avenatti, an attorney for Stephanie Clifford, who presents herself in the adult performance industry under the stage name *Stormy Daniels*, announced that he will attend the hearing with Ms. Clifford.⁴ Avenatti did not say whether you invited them to attend the hearing or whether they will testify. I hope you can clarify Mr. Avenatti's and Ms. Clifford's roles in the hearing.

¹ Press Release, H. Comm. on Oversight & Reform, Chairman Cummings Announces Oversight Committee Hearing Schedule, Jan. 10, 2019, <https://oversight.house.gov/news/press-releases/chairman-cummings-announces-oversight-committee-hearing-schedule>.

² See Plea Agreement, U.S. v. Michael Cohen, No. 1:18-cr-850 (S.D.N.Y. 2018), <https://www.justice.gov/file/1115566/download>; Indictment, U.S. v. Michael Cohen, No. 1:18-cr-850 (S.D.N.Y. 2018), <https://www.justice.gov/file/1115596/download>; Devlin Barrett et.al., *Michael Cohen, Trump's former lawyer, pleads guilty to lying to Congress about Moscow project*, Nov. 29, 2018, https://www.washingtonpost.com/politics/michael-cohen-trumps-former-lawyer-pleads-guilty-to-lying-to-congress/2018/11/29/5fac986a-f3e0-11e8-bc79-68604ed88993_story.html?utm_term=.657f859fc6c4.

³ Letter from Jim Jordan, Ranking Member, H. Comm. on Oversight & Reform, to Elijah E. Cummings, Chairman, H. Comm. on Oversight & Reform (Jan. 11, 2019).

⁴ Morgan Gstalter, *Avenatti says he and Stormy Daniels will attend Cohen's congressional hearing*, THE HILL, Jan. 14, 2019, <https://thehill.com/homenews/administration/425029-avenatti-says-he-and-stormy-daniels-will-attend-cohens-congressional>.

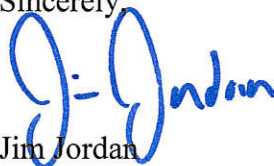
The Honorable Elijah E. Cummings
January 15, 2019
Page 2

According to news reports, the Committee's hearing would not be the first time Mr. Avenatti and Ms. Clifford have appeared at an official proceeding involving Mr. Cohen. Mr. Avenatti previously appeared at a procedural hearing in Mr. Cohen's criminal case in Federal District Court in the Southern District of New York.⁵ One report described Mr. Avenatti's interjection at Mr. Cohen's hearing and the hearing's "circus-like atmosphere."⁶ According to another report describing the court hearing, the appearance of Ms. Clifford and Mr. Avenatti turned the court's proceeding into a "three-ring circus."⁷ To avoid a public charade at a Congressional hearing—your seminal foray as Chairman—please provide answers to the following questions:

1. Have you, your staff, or any Democratic Member extended an invitation for either Michael Avenatti or Stephanie Clifford to attend the Committee's February 7, 2019, hearing?
2. Have you, your staff, or any Democratic Member arranged for reserved seats for either Michael Avenatti or Stephanie Clifford to attend the Committee's February 7, 2019, hearing? If so, is there a new Committee policy for reserving seats? If there is, is the minority permitted to reserve seats?
3. Is it your intention to call either Michael Avenatti or Stephanie Clifford as a witness at the February 7, 2019, hearing, or at any future Committee hearings?
4. Are there any other witnesses you intend to bring before the Committee at the February 7, 2019, hearing?

We should agree that the Committee's work is serious business that should not be discredited by publicity hounds and witnesses seeking to advance their own agenda. I look forward to hearing from you soon.

Sincerely,



Jim Jordan
Ranking Member

⁵ See Marcus Baram, *Inside a tense Michael Cohen court hearing: Stormy's lawyer and "taint team" concerns*, FAST COMPANY, April 13, 2018, <https://www.fastcompany.com/40558846/inside-a-tense-michael-cohen-court-hearing-stormys-lawyer-and-taint-team-concerns>.

⁶ *Id.*

⁷ See Kaja Whitehouse et. al., *How Cohen's day in court turned into the Stormy Daniels show*, April 16, 2018, NEW YORK POST, <https://nypost.com/2018/04/16/how-cohens-day-in-court-turned-into-the-stormy-daniels-show/>.

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074

<http://oversight.house.gov>

January 22, 2019

Guy Petrillo, Esq.
Petrillo Klein & Boxer LLP
655 Third Avenue, 22d Floor
New York, NY 10017

Dear Mr. Petrillo:

We write concerning your client, Michael D. Cohen. Our staff recently met with Lanny J. Davis, who identified himself as Cohen's Washington, D.C. attorney and media advisor. Davis, a veteran Democrat political operative with expertise in public relations,¹ was unable to answer several questions about Cohen's appearance. He suggested you – as Cohen's criminal defense attorney – are best positioned to provide this assistance.

Scope of Cohen's testimony

Davis told us Cohen's testimony will exclude any matter "under investigation." The non-exhaustive list of issues that Cohen will refuse to address include matters involving the Attorney General for the State of New York, the United States Attorney's Office for the Southern District of New York, and the office of Special Counsel Robert S. Mueller III.

Of course, this is not an easy list of topics to sidestep at a Congressional hearing with such intense public interest. Our Members intend to ask Cohen whatever question they deem appropriate. Among other matters, we learned from Davis our Members will not receive answers to why Cohen defrauded the United States and the State of New York through his business dealings. He will not speak about representations and affirmations he made while seeking loans and other forms of credit from financial institutions. We will not be hearing testimony about why Cohen intentionally provided false and misleading testimony to the United States Congress in previous appearances. We will not be able to learn more about Cohen's role in federal campaign finance law violations. In fact, according to Davis, Cohen's testimony will be circumscribed to what *he* and you are comfortable with *him* addressing.

¹ According to publicity materials, Davis served as Special Counsel to President Clinton and was spokesman for the President and the Clinton White House on wide variety of matters. *Lanny J. Davis, About The Author*, Simon & Schuster, <https://www.simonandschuster.com/authors/Lanny-J-Davis/1446943> (last visited Jan. 18, 2019).

Origins of Cohen's appearance

According to Davis, he has been working with Chairman Elijah E. Cummings for “one or two months” on Cohen’s appearance before the Committee. After an unspecified number of meetings and communications, Davis indicated the Chairman finally “came around” to the idea of having a hearing.

Davis conceded Cohen did not want to testify—and in fact cannot testify about much due to the far-flung criminal investigations of which he is a target, subject or defendant—and Cohen is fearful for his family. Davis acknowledged, “I pushed him to do this,” explaining “this was my idea; nobody else’s.”

Davis confirmed he did not have any discussions with the Department of Justice or the Attorney General for the State of New York before offering Cohen’s appearance to the Committee. Davis is not asking permission, he told us. Instead, Davis stated, “I told them what our decision was.” “I picked this Committee,” Davis said, as the exclusive venue for Cohen to tell his own personal story. Davis indicated his longstanding personal relationship with Chairman Cummings was determinative. Davis stated Cohen does not plan to testify before any other congressional committees in open or closed session.

Purpose of Cohen's appearance

According to Davis, the sole purpose of Cohen’s appearance before the Committee is to allow Cohen to share his personal anecdotes about his time working for the then-private citizen Donald J. Trump, and his experiences after Mr. Trump became President. Pressed on how Cohen’s testimony is jurisdictionally related to the Committee’s role in overseeing the functioning, efficiency, and effectiveness of the federal government, Davis stated Cohen has “anecdotes about his time with the President.” He forewarned the hearing will likely be “unsatisfying” and “frustrating” for Members of the Committee.

Conflict of interest issues and compensation

Given Davis’s close association with former President Bill Clinton and 2016 Democratic nominee for President and former Secretary of State Hillary Rodham Clinton, we also have questions about how Cohen’s legal representatives resolve the conflict of interest Davis’s representation presents.² Davis’s role as consigliere for the Clintons and those close to them raises the specter his client loyalties may be divided. We seek clarification on whether any waivers have been executed.

We do know Cohen is not paying Davis. Davis told us his firm has a representation agreement with a fee. When asked directly whether Cohen is paying his fee, Davis cryptically

² The D.C. Bar Rules of Professional Conduct Rule 1.7 states: (b) . . . a lawyer shall not represent a client with respect to a matter if: . . . (4) The lawyer’s professional judgment on behalf of the client will be or reasonably may be adversely affected by the lawyer’s responsibilities to or interests in a third party or the lawyer’s own financial, business, property, or personal interests.

Guy Petrillo, Esq.
 January 22, 2019
 Page 3

said he could not answer but if Cohen was paying his fee, “I would say yes.” If Davis is providing free media advisory or legal services, or if someone else is paying Davis’s fees, it adds to the perception Cohen’s appearance is a media stunt initiated, produced, and financed by career Democrat political operatives as a way of scoring political points against the President.

* * *

Several of our questions to Davis went unanswered. Davis, however, believed you were the person to whom we needed to speak.

One of the inherent challenges with the upcoming hearing Lanny Davis has arranged for Chairman Cummings is it will be occurring against the backdrop of news accounts published about the Special Counsel’s work that have proven untrue. Cohen is at the heart of two of these stories. On January 17, 2019, *BuzzFeed News* released a story titled, “President Trump Directed His Attorney Michael Cohen To Lie To Congress About The Moscow Tower Project,” reportedly citing evidence possessed by the Special Counsel’s office.³ Shortly after the publication, in an extremely rare public comment, the Special Counsel’s office released a statement, “BuzzFeed’s description of specific statements to the special counsel’s office, and characterization of documents and testimony obtained by this office, regarding Michael Cohen’s congressional testimony are not accurate.”⁴

The Buzzfeed story was not the first time a public report of this type had to be corrected. In August, Davis made inaccurate public statements about Cohen’s testimony to the Special Counsel about the June 2016 Trump Tower meeting.⁵ After Davis was forced to correct the record, the *Washington Post* reported, “[Davis] is backing away from confident assertions he made that Cohen has information to share with investigators that shows Trump knew in 2016 of Russian efforts to undermine Democratic nominee Hillary Clinton.”⁶ These stories represent some of the misinformation and confusion surrounding Cohen’s criminal cases. With this background, it is important for the Committee to receive accurate information to ensure a fact-based hearing.

³ Jason Leopold and Anthony Cormier, *President Trump Directed His Attorney Michael Cohen To Lie To Congress About The Moscow Tower Project*, BUZZFEED NEWS (Jan. 17, 2019), https://www.buzzfeednews.com/article/jasonleopold/trump-russia-cohen-moscow-tower-mueller-investigation?ref=hpsplash&bftw=&utm_term=4ldqfp#4ldqfp.

⁴ Statement of Peter Carr, U.S. Dep’t of Justice, Special Counsel’s Office (Jan. 18, 2019); Mary Clare Jalonick and Eric Tucker, *Mueller Disputes Accuracy of BuzzFeed Report on Trump*, AP (Jan. 18, 2019), <https://www.apnews.com/58e8eff8dabb4b5289e4db16435a2b02/>.

⁵ Tom Hamburger and Rosalind S. Helderman, *Attorney For Michael Cohen Backs Away From Confidence That Cohen Has Information About Trump’s Knowledge On Russian Efforts*, WASH. POST. (Aug. 26, 2018), https://www.washingtonpost.com/politics/attorney-for-michael-cohen-backs-away-from-confidence-that-cohen-has-information-about-trumps-knowledge-on-russian-efforts/2018/08/26/09d7f26e-a876-11e8-97ce-cc9042272f07_story.html?utm_term=.4ad53fcd6876 https://www.washingtonpost.com/politics/attorney-for-michael-cohen-backs-away-from-confidence-that-cohen-has-information-about-trumps-knowledge-on-russian-efforts/2018/08/26/09d7f26e-a876-11e8-97ce-cc9042272f07_story.html?utm_term=.4ad53fcd6876.

⁶ *Id.*

Guy Petrillo, Esq.

January 22, 2019

Page 4

In preparation for the hearing, we have asked Chairman Cummings to require Cohen to participate in a transcribed interview, so we may better understand the matters on which he is and is not willing to speak. Davis told us, however, he will not allow this to happen. We also asked the Chairman to seek basic information from the Department of Justice or the Cohen legal team relating to the cases in which Cohen is a criminal defendant. Davis was able to provide some documents related to Cohen's sentencing hearing, but he referred us to you as someone well-positioned to be more responsive.

These are the information and materials we request:

1. Any FD-302 forms and any other investigative reports created by the DOJ or FBI in their investigations into Michael Cohen;
2. Any FD-1023 forms that may have been created involving Michael Cohen;
3. All cooperation agreements between Michael Cohen and DOJ;
4. Any notes taken by DOJ or FBI during their multiple interviews of Michael Cohen;
5. Documentation of all agreements Michael Cohen has with DOJ, the FBI, and any other foreign government's law enforcement agencies;
6. Any copies of waivers referring or relating to Cohen's client representations, whether related to attorney-client, conflict of interest, or otherwise;
7. Any copies of waivers referring or relating to Davis's representation of Cohen whether related to attorney-client, conflict of interest, or otherwise;
8. Identify the scope of Cohen's intended testimony before the Committee on February 7, 2019; and
9. Identify consultations the Cohen legal team has had with the Justice Department, the New York State Attorney General or other investigative or prosecutorial offices with an ongoing investigation of Cohen. For each consultation, identify the government official, the date, and the attendant or resulting testimonial scope limitation.

In summary, Davis made clear that Cohen's upcoming appearance before the Committee is entirely a result of Davis's orchestration. According to Davis, the hearing was Davis's idea and his alone. Cohen apparently did not want to testify—but Davis has persuaded Cohen to appear despite his concerns and fears. Davis picked our Committee as the exclusive venue for Cohen's appearance based on his long-standing personal friendship with Chairman Cummings,

Guy Petrillo, Esq.
January 22, 2019
Page 5

and it took Chairman Cummings one to two months to agree to Davis's plan for Cohen's appearance. Cohen will not testify to any matter "under investigation," and Davis predicted that this constraint will leave Members of the Committee "frustrated" and "unsatisfied." Cohen is apparently not paying Davis for Davis's considerable efforts in advance of this hearing.

As Cohen's February 7, 2019, appearance – the first major hearing for the Chairman – is quickly approaching, we hope you will provide the requested documents and other information no later than January 25, 2019. We look forward to hearing from you.

Sincerely,



Jim Jordan



Mark Meadows

cc: The Honorable Elijah E. Cummings, Chairman, Committee on Oversight and Reform
The Honorable Doug Collins, Committee on the Judiciary
The Honorable Devin Nunes, Permanent Select Committee on Intelligence
The Honorable Matthew Whitaker, Acting Attorney General, U.S. Dep't of Justice
The Honorable Robert S. Mueller III, Special Counsel, U.S. Dep't of Justice
The Honorable Geoffrey S. Berman, U.S. Attorney for the Southern District of New York
The Honorable Letitia James, New York State Attorney General
Lanny J. Davis, Esquire

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051

MINORITY (202) 225-5074

<http://oversight.house.gov>

January 31, 2019

The Honorable Elijah E. Cummings
Chairman
Committee on Oversight and Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

We write with questions about the upcoming hearing with Michael Cohen. At least one news organization has reported you may schedule the hearing for next week.¹ Based on communications with our staff, Michael Cohen's attorney and media adviser, Lanny J. Davis, has notified you Cohen's testimony will be limited in scope. According to Davis, you have acceded to an unusual arrangement whereby Cohen will be permitted to appear voluntarily and be afforded the leeway to answer only those questions he so chooses. His testimony, Davis advised, will be extremely limited. All questions touching on possible ongoing investigations have been deemed off limits by Davis.

By letter dated January 11, 2019, we asked you to obtain a basic set of documents from the Department of Justice so our Members may meaningfully prepare for the Cohen hearing, the first major hearing of your Chairmanship.² We also sought to question Cohen at a transcribed interview so we could better-understand the scope limitations you have agreed to. Your decision not to do so raises the prospect you are leading us towards a circus of a hearing.

Our January 18, 2019, meeting with Davis yielded stunning information about the origins of the hearing. We learned:

- Cohen's public testimony will exclude all matters involving the United States Attorney's Office for the Southern District, the Attorney General for the State of New York, and the office of Special Counsel Robert S. Mueller III;

¹ Jeremy Herb & Kara Scannell, *Michael Cohen agrees to testify behind closed doors, House Intel chairman says*, CNN (January 28, 2019), <https://www.cnn.com/2019/01/28/politics/michael-cohen-agrees-to-testify-february-8-closed-doors/index.html> ("Cohen's Oversight Committee testimony is not yet finalized, but he's in discussions to appear on February 7...").

² Letter from Jim Jordan, Ranking Member, H. Comm on Oversight & Reform, to Elijah E. Cummings, Chairman, H. Comm on Oversight & Reform (Jan. 11, 2019), <https://republicans-oversight.house.gov/wp-content/uploads/2019/01/2019-01-11-JDJ-to-EEC-re-Cohen-Testimony.pdf>.

The Honorable Elijah E. Cummings
 January 31, 2019
 Page 2

- *Davis* exclusively picked our Committee for Cohen to testify in based on his longstanding friendship with *you*. *Davis* allowed he had to convince both you and Cohen to have the hearing. Cohen did not want to testify—*Davis* said, “I pushed him to do this,” explaining, “this was my idea; nobody else’s.” According to *Davis*, you seemingly had your own reservations, but *Davis* told us after “one or two months” you finally “came around;”
- The sole purpose of Cohen’s appearance before the Committee is to allow Cohen to share his personal anecdotes about his time working for the then-private citizen Donald J. Trump, and his experiences after Mr. Trump became President. Pressed on how Cohen’s testimony is jurisdictionally related to our Committee’s role in overseeing the functioning, efficiency, and effectiveness of the federal government, *Davis* stated Cohen has “anecdotes about his time with the President.” He confessed the hearing will likely be “unsatisfying” and “frustrating” for Members of the Committee;
- *Davis* conceded Cohen has not been paying for his services. *Davis* told us his firm has a representation agreement with a fee. When asked directly whether Cohen is paying his fee, *Davis* cryptically said he could not answer but if Cohen was paying his fee, “I would say yes.”

We are perplexed by the authority you have ceded to *Davis* in producing this made-for-television hearing. Lanny *Davis* is a close associate of former President Bill Clinton and former 2016 Democratic presidential candidate, Hillary Rodham Clinton. His undisputed remarks to our staff on January 18, 2019, create the perception that Cohen’s appearance is a media stunt initiated and financed by career Democrat political operatives as a way of meting out retribution against the President. *Davis*’s representation of Cohen has not been error-free. For instance, *Davis* was forced to walk back unfounded accusations he made against the President. The *Washington Post* reported, “[*Davis*] is backing away from confident assertions he made that Cohen has information to share with investigators that shows Trump knew in 2016 of Russian efforts to undermine Democratic nominee Hillary Clinton.”³

We hope you share our mission in ensuring our Committee is serious minded in its pursuit of fact based oversight and investigative work.⁴ Although you have been unwilling to

³ Tom Hamburger and Rosalind S. Helderman, *Attorney For Michael Cohen Backs Away From Confidence That Cohen Has Information About Trump’s Knowledge On Russian Efforts*, WASH. POST. (Aug. 26, 2018), https://www.washingtonpost.com/politics/attorney-for-michael-cohen-backs-away-from-confidence-that-cohen-has-information-about-trumps-knowledge-on-russian-efforts/2018/08/26/09d7f26e-a876-11e8-97ce-cc9042272f07_story.html?utm_term=.4ad53fcd6876.

⁴ *Oversight of the FBI and DOJ Actions in Advance of the 2016 Election before the H. Comm. on Oversight & Gov’t Reform joint with the Judiciary*, 115th Cong. 147 (June 19, 2018) (statement of Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov’t Reform) (“You know, as I sit here and I think about life, you know, and I tell my constituents this, I tell them I wish there were not a Republican and a Democratic party. I wish I was not a, quote, ‘politician.’ You know why? Because I think that when people hear us a lot of time, or hear me, they just assume that I’m saying things based upon political expediency or trying to help a party. My party. But there are

The Honorable Elijah E. Cummings
January 31, 2019
Page 3

seek documents from the Justice Department or a transcribed interview with Cohen, we hope you will reflect on your decision and keep an open mind about reversing yourself.

We hope to obtain the requested information as soon as possible to thoroughly prepare for the hearing. We look forward to hearing from you.

Sincerely,



Jim Jordan
Ranking Member



Mark Meadows
Ranking Member
Subcommittee on Government Operations

certain things that are about -- are bigger than party, like country and being a human being. And I think that when we talk about -- you know, when I read your report and I looked at what you've done, it's the people like the ones that's sitting behind you that take an oath to do their very, very best and to be honest and to uphold the Constitution of our country. Those are the people that will keep our democracy together. And I say it with all of the sincerity I have in my heart.”).

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051

MINORITY (202) 225-5074

<http://oversight.house.gov>

February 21, 2019

Mr. Lanny J. Davis
Davis Goldberg & Galper PLLC
1700 K Street NW, Suite 825
Washington, DC 20006

Dear Mr. Davis:

Your client, Michael Cohen, is scheduled to testify before our Committee on February 27, 2019. Cohen is expected to make accusations against President Trump, his former legal client. Cohen is a convicted criminal who has admitted to crimes of deception and lies for his personal greed and ambition. Our Members have a number of questions they intend to pose Cohen; however, Chairman Elijah Cummings has refused to request material necessary to prepare for Cohen's anticipated testimony. Therefore, we write to you to seek additional information about one facet of Cohen's work: the strategic consulting, lobbying, and foreign agent work he sought to undertake after he was denied a staff position in President Trump's White House.

As you boasted to our staff on January 18, 2019, you arranged for Cohen to testify before our Committee before he begins serving his prison sentence and you convinced Chairman Cummings to make Cohen the first announced witness of his chairmanship. Chairman Cummings agreed to your overtures, but he has unilaterally and unnecessarily attempted to limit the scope of Cohen's testimony. To be clear, and as our staff conveyed to you at the January meeting, our Members are not bound by the extremely narrow terms you have established with the Chairman. Our Members intend to pose questions they deem appropriate and they may ask your client about any of the following issues:

- The crimes of deception and lies to which Cohen pleaded guilty;
- Other criminal activity in which Cohen participated, but refused to disclose or cooperate with the U.S. Attorney's Office for the Southern District of New York (SDNY);
- Cohen's business dealings and international financial dealings, including those involving his relatives;
- Cohen's actions and boasts probative of his character, including his book deals, his desire to be a cable television personality, the fantastic claim he delivered his

Mr. Lanny J. Davis

February 21, 2019

Page 2

own baby, the delusional aim to be Mayor of the City of New York, and the fake *Women For Cohen* social media initiative he commissioned;¹ and

- Cohen’s strategic consulting, lobbying, and foreign agent work.

Federal court records show how Cohen sought to use his association with President Trump for personal gain. According to the SDNY prosecutors, in January 2017, around the time of President Trump’s inauguration, Cohen began offering lobbying and consulting services to a number of companies.² The prosecutors determined that Cohen “secured a substantial amount of consulting business for himself throughout 2017 by marketing to corporations what he claimed to be unique insights about and access to [President Trump].”³ Cohen’s list of major domestic and foreign corporate clients included AT&T, Novartis, BTA Bank of Kazakhstan, Columbus Nova, and Korea Aerospace Industries. His efforts landed Cohen a number of lucrative consulting deals worth millions of dollars. For example:

- AT&T paid Cohen \$600,000 for insight on how the Administration would approach its controversial proposed merger with Time Warner.⁴
- Swiss pharmaceutical company Novartis paid Cohen \$1.2 million for promised access to the White House on health care policy.⁵
- Kazakhstan’s BTA Bank, which Cohen has previous business ties to, paid Cohen a large sum under a consulting agreement.⁶
- Columbus Nova, a company whose biggest investor is owned by a Russian oligarch, paid Cohen \$500,000 for advice on “potential sources of capital and potential investments.”⁷

¹ Letter from Jim Jordan, Ranking Member, H. Comm. on Oversight & Reform, to Elijah E. Cummings, Chairman, H. Comm. on Oversight & Reform (Feb. 19, 2019), <https://republicans-oversight.house.gov/wp-content/uploads/2019/02/2019-02-19-JDJ-MM-to-EEC-re-Cohen-Testimony.pdf>.

² The Government’s Sentencing Memorandum at 3, United States v. Cohen, No. 18-cr-602 (S.D.N.Y. filed Dec. 7, 2018), <https://assets.documentcloud.org/documents/5453401/SDNY-Cohen-sentencing-memo.pdf>.

³ The Government’s Sentencing Memorandum at 3, United States v. Cohen, No. 18-cr-602 (S.D.N.Y. filed Dec. 7, 2018), <https://assets.documentcloud.org/documents/5453401/SDNY-Cohen-sentencing-memo.pdf>.

⁴ Rosalind S. Helderman et al., *Cohen’s \$600,000 Deal with AT&T Specified He Would Advise on Time Warner Merger, Internal Company Records Show*, WASHINGTON POST (May 10, 2018), https://www.washingtonpost.com/politics/cohens-600000-deal-with-atandt-specified-he-would-advise-on-time-warner-merger-internal-company-records-show/2018/05/10/cd541ae0-5468-11e8-a551-5b648abe29ef_story.html?utm_term=.917bf9be7834.

⁵ MJ Lee et al., *Inside Michael Cohen’s Aggressive Pitch Promising Access to Trump*, CNN (May 10, 2018), <https://www.cnn.com/2018/05/09/politics/michael-cohen-trump-lobbying/index.html>.

⁶ See, e.g., Christopher Brennan, *Trump Associate Received More than \$21M in Kazakh Oligarchs’ Alleged Money Laundering Scheme*, NY DAILY NEWS (Apr. 25, 2018), <https://www.nydailynews.com/news/national/trump-associate-received-21m-alleged-oligarch-scheme-article-1.3953189>; Adam Davidson, *Trump’s Business of Corruption*, NEW YORKER (Aug. 21, 2017), <https://www.newyorker.com/magazine/2017/08/21/trumps-business-of-corruption>.

⁷ Bess Levin, *Michael Cohen Must Be The Most Gifted Consultant in America*, VANITY FAIR (May 9, 2018), <https://www.vanityfair.com/news/2018/05/michael-cohen-must-be-the-most-gifted-consultant-in-america>.

Mr. Lanny J. Davis
 February 21, 2019
 Page 3

- South Korean company Korea Aerospace Industries paid Cohen \$150,000 for “legal consulting concerning accounting standards on production costs” related to part of a multi-billion dollar Pentagon contract the company was bidding on.⁸

Despite collecting a handsome windfall, Cohen apparently performed little to no work. According to the SDNY prosecutors, “while Cohen made millions of dollars for these consulting arrangements, his promises of insight and access proved essentially hollow.”⁹ Instead, it appears that Cohen leveraged his association with President Trump to attract and retain major corporate clients, produced no tangible results, and still walked away with millions of dollars.

Regardless of whether Cohen charged clients with no intention of doing the work, or whether he attempted but failed to deliver what he promised, he reportedly did not register his lobbying activities with the federal government. The *Wall Street Journal* reported that Cohen failed to register as a domestic lobbyist as required under the Lobbying Disclosure Act (LDA).¹⁰ Violators of the LDA can be fined up to \$200,000 per violation or face up to five years in prison.¹¹ Similar registration requirements in the Foreign Agents Registration Act (FARA) apply to an individual lobbying on behalf of a foreign principal if the activity is meant to influence the U.S. government (or any portion of the U.S. public) regarding U.S. policy toward a foreign place.¹² Violators of FARA can face criminal fines or up to five years in prison.¹³

Due to Cohen’s reported agreements with both domestic companies and foreign entities, our Members have questions about whether Cohen was required to register his lobbying activities with the federal government pursuant to either the LDA or FARA. Accordingly, we request that you provide the following documents and information on Cohen’s behalf:

1. All documents and communications related to Michael Cohen’s lobbying and/or consulting agreements, including agreements executed as or on behalf of Essential Consultants LLC;
2. All documents and communications related to all lobbying disclosures contemplated or filed with Congress as required by the LDA; and

⁸ Amanda Macias, *South Korean Defense Company That Paid Trump Lawyer Cohen \$150,000 is Poised to Win Part of a \$16 Billion Pentagon Deal*, CNBC (May 9, 2018), <https://www.cnbc.com/2018/05/09/south-korean-firm-that-paid-trump-lawyer-cohen-poised-to-win-pentagon-deal.html>.

⁹ The Government’s Sentencing Memorandum at 3-4, *United States v. Cohen*, No. 18-cr-602 (S.D.N.Y. filed Dec. 7, 2018), <https://assets.documentcloud.org/documents/5453401/SDNY-Cohen-sentencing-memo.pdf> (“Documents obtained by the Government and witness interviews revealed that Cohen performed minimal work, and many of the consulting contracts were ultimately terminated.”).

¹⁰ Nicole Hong et al., *Prosecutors Investigating Michael Cohen for Possible Illegal Lobbying*, WALL STREET JOURNAL (June 14, 2018), <https://www.wsj.com/articles/prosecutors-investigating-michael-cohen-for-possible-illegal-lobbying-1529012696>.

¹¹ *Lobbying Disclosure Act Guidance – Section 12: Penalties*, U.S. HOUSE OF REPRESENTATIVES (Jan. 31, 2017), https://lobbyingdisclosure.house.gov/amended_lda_guide.html#section12.

¹² 22 U.S.C. § 611 et seq. (2012).

¹³ *FARA Enforcement*, DEP’T OF JUSTICE (July 26, 2018), <https://www.justice.gov/nsd-fara/fara-enforcement>.

Mr. Lanny J. Davis

February 21, 2019

Page 4


3. All documents and communications related to lobbying disclosures contemplated or filed with the Attorney General as required by FARA.

Please provide these documents to the Committee as soon as possible, but no later than February 25, 2019. If you have any questions, please contact Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,



Jim Jordan
Ranking Member



Mark Meadows
Ranking Member
Subcommittee on Government Operations

cc: The Honorable Elijah E. Cummings, Chairman, Comm. on Oversight and Reform
The Honorable Devin Nunes, Ranking Member, Permanent Select Comm. on Intelligence

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074

<http://oversight.house.gov>

February 25, 2019

The Honorable Elijah E. Cummings
Chairman
Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

We renew our request that you call Deputy Attorney General Rod Rosenstein to publicly testify before our Committee, and recommend he appears alongside Michael Cohen on Wednesday, February 27, 2019. Cohen has pleaded guilty to crimes of deception and lies, including lying to Congress.¹ In Cohen's sentencing proceeding, two Justice Department components—the U.S. Attorney's Office for the Southern District of New York and the Special Counsel's Office—provided information about the Department's views of Cohen's crimes and conduct. As the Deputy Attorney General, with direct supervision of these entities, only Rosenstein can speak to the views of both Department components.

Rosenstein's appearance would also allow the Committee to continue its ongoing oversight of the Department of Justice. During our joint investigation with the House Judiciary Committee, former FBI general counsel James Baker testified that between May 9 and May 17, 2017, Rosenstein organized a series of meetings with Department officials, including former FBI Deputy Director Andrew McCabe, to strategize methods to get back at the President for firing FBI Director James Comey.² Rosenstein and others contemplated a range of ideas, from Rosenstein wearing a wire to secretly record the President to Rosenstein recruiting cabinet

¹ Press Release, Dep't of Justice, Michael Cohen Sentenced to 3 Years in Prison (Dec. 12, 2018), <https://www.justice.gov/usao-sdny/pr/michael-cohen-sentenced-3-years-prison>.

² See Transcribed Interview of James Baker 7 Day 2, Oct. 18, 2018 (Mr. Baker: I believe there were a couple of different meetings, and they -- I believe there were a couple of different meetings, and each time, I think, it was the day after because I believe the meetings went late into the evening. That's to the best of my recollection. Mr. Jordan: Okay. And is it your understanding that there were multiple meetings that Mr. McCabe, Ms. Page, Mr. Rosenstein had about the potential of recording the President? Mr. Baker: I don't know. I know that they had multiple meetings with the Deputy Attorney General discussing a lot of things in the immediate aftermath of the firing, and I don't specifically remember how many times this was discussed. Mr. Jordan: So, just to be clear, the firing of Mr. Comey took place on May 9th, and then the hiring of the special counsel took place on May 17th. So these numerous meetings and the one you had with Mr. McCabe and Ms. Page took place between the 9th and the 17th? Mr. Baker: I believe that's correct."). *Id.* at 11 (Mr. Baker: "...And then there are these -- some number of conversations with the Deputy Attorney General about what to do next, what needs to be done, and my recollection is numerous topics were discussed, and these were among them. The wearing the wire and the 25th Amendment were one of a list, one or two of a list of things that we were going -- that people were going through to try to figure out what to do...").

The Honorable Elijah E. Cummings

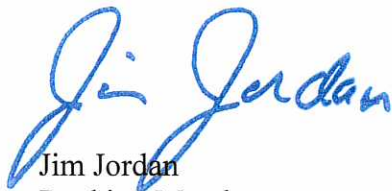
February 25, 2019

Page 2

members to invoke the 25th Amendment.³ McCabe, a participant in some of the Rosenstein meetings, is now relating these facts publicly to promote his book.⁴ Rosenstein has disputed McCabe's account.⁵

If you intend to proceed with Michael Cohen as the star witness of the Committee's first big hearing, Members should have an opportunity to assess his credibility. We have asked several times that you request information and documents from the Justice Department about Cohen and his crimes. You have refused to do so. The next best alternative, if the Committee is to have a fair and thorough hearing, is to have a Justice Department witness to speak to these matters. By virtue of his position, Rosenstein is the appropriate witness for this task. We therefore strongly urge you to invite Rosenstein to the Committee's hearing on February 27, 2019. We appreciate your consideration of this request and look forward to hearing from you.

Sincerely,



Jim Jordan
Ranking Member



Mark Meadows
Ranking Member
Subcommittee on Government Operations

³ Transcribed Interview of James Baker 137 Day 1, Oct. 3, 2018 (Baker: "...It was I believe to the best of my recollection it was some combination of them that they told me that there had been a conversation with the DAG about the idea of the DAG wearing a wire into a conversation or conversations with the President."); *Id.* at 143 (Baker: "...The 25th Amendment conversation, my understanding was that there was a conversation in which it was said I believe by the DAG that there were -- that there were two members of the cabinet who were willing to go down this road already..."); U.S. CONST. AMEND. XXV, § 4.

⁴ *McCabe Says He Ordered the Obstruction of Justice Probe of President Trump*, 60 MINUTES (Feb. 14, 2019), <https://www.cbsnews.com/news/andrew-mccabe-says-he-ordered-the-obstruction-of-justice-case-of-president-trump-60-minutes/>.

⁵ Daniel Chaitin, *DOJ Rebuffs Andrew McCabe: Claim that Rod Rosenstein Sought to Oust Trump 'Inaccurate and Factually Incorrect'*, WASH. EXAMINER (Feb. 14, 2019).

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051

MINORITY (202) 225-5074

<http://oversight.house.gov>

February 28, 2019

The Honorable William Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

Dear Mr. Attorney General:

We write to refer significant evidence that Michael D. Cohen committed perjury and knowingly made false statements during his testimony before an Oversight and Reform Committee (Committee) hearing titled, "Hearing with Michael Cohen, Former attorney for President Donald Trump" on February 27, 2019.

While testifying under oath, Mr. Cohen made what appear to be numerous willfully and intentionally false statements of material fact contradicted by the record established by the Justice Department in *United States v. Cohen*, 18-cr-602 (S.D.N.Y.) (WHP). Mr. Cohen's testimony before the Committee at times was in direct contradiction to assertions contained in pleadings authored by the United States Attorney's Office for the Southern District of New York (SDNY). There are other instances in which Mr. Cohen's statements to the Committee were immediately contradicted by witnesses with firsthand knowledge of the subject matter.

Under 18 U.S.C. § 1621, a witness commits perjury if the witness "willfully" asserts "any material matter which he does not believe to be true" after "having taken an oath" to "testify . . . truly." Under 18 U.S.C. § 1001, a witness commits a crime if the witness "knowingly and willfully" makes "any material false, fictitious, or fraudulent statement or representation" with respect to "any investigation under review, conducted pursuant to the authority of any committee . . . of the Congress." Congress cannot perform its oversight function if witnesses who appear before its committees do not provide truthful testimony. Perjury and false statements before Congress are crimes that undermine the integrity of the Constitutional duty to conduct oversight and inquiries.

The points below support an investigation into whether Mr. Cohen committed perjury or made false statements at the Committee's hearing:

1. Several times during his testimony, Mr. Cohen denied committing various fraudulent acts that he has pleaded guilty to in federal court. Specifically, Mr. Cohen said "I never

defrauded any bank.”¹ These denials are intentionally false. Mr. Cohen pleaded guilty to five counts of income tax evasion, one count of making false statements to a banking institution, one count of causing an unlawful corporate contribution, one count of excessive campaign contribution, and one count of making false statements to Congress. In Mr. Cohen’s plea agreement with the United States Attorney’s Office for the Southern District of New York, prosecutors specifically referred to Mr. Cohen’s crimes of making false statements to financial institutions as “bank fraud.”² This point—Mr. Cohen’s culpability for bank fraud—materially affects the Committee’s assessment of his credibility.

2. Mr. Cohen repeatedly testified that he did not seek employment in the White House following President Trump’s election. This is demonstrably, materially, and intentionally false. This testimony is in direct conflict with court filings made by the United States Attorney’s Office for the SDNY, which state:

During and after the campaign, Cohen privately told friends and colleagues, including in seized text messages, that he expected to be given a prominent role and title in the new administration. When that did not materialize, Cohen found a way to monetize his relationship with and access to the President.³

When confronted at the hearing with the SDNY statement, Mr. Cohen testified that the above statement made by the United States Attorneys in the SDNY was “not accurate.” He testified:

MR. JORDAN: You wanted to work in the White House.

MR. COHEN: No, sir.

MR. ROY: You said clearly to Mr. Cloud and Mr. Jordan that the Southern District of New York lawyers were being untruthful in characterizing your desire to work in the administration. Do you say again that the lawyers of the Southern District of New York are being untruthful

¹ “*Hearing with Michael Cohen, Former attorney for President Donald Trump*”: *Hearing before the H. Comm. on Oversight & Reform*, 116th Cong. (2019) (statement of Michael D. Cohen) [hereinafter “Cohen hearing”].

² Plea Agreement at 3 n.2, *United States v. Michael Cohen*, 18-cr-602 (S.D.N.Y. Aug. 21, 2018).

³ The Government’s Sentencing Memorandum at 25, *United States v. Cohen*, 18-cr-602 (S.D.N.Y. Dec. 7, 2018).

in making that characterization, yes or no?

MR. COHEN: I'm saying that's not accurate.⁴

Shortly after Mr. Cohen's public statements, at 11:13 a.m., former New York City Police detective Bo Dietl tweeted, "Getting sick watching these hearings. I know Michael Cohen personally for many years and he told me several times that he was very angry and upset that he didn't get a post in the WH and that he 'would do what he has to do now to protect his family.'"⁵ At 3:44 p.m., Dr. Darrell Scott, Pastor, New Spirit Revival Center, and a Trump campaign faith-based outreach coordinator tweeted, "Michael Cohen asked ...no, BEGGED me REPEATEDLY, to ask the POTUS to give him a job in the Administration! He's STILL lying under oath!"⁶

Mr. Cohen's testimony is material to the Committee's assessment of Mr. Cohen's motive to monetize his former association with President Trump. It is essential that the Department of Justice investigate these remarkable contradictions between Mr. Cohen, the SDNY prosecutors, and the public accounts of witnesses with firsthand information. In addition, based on the SDNY's reference to having "seized text messages" proving Mr. Cohen's desire for a position in the Trump Administration, it appears that the SDNY may already be in possession of evidence bearing on Mr. Cohen's culpability.

3. Mr. Cohen testified he did not direct the commission of the Twitter account @WomenForCohen. Specifically, Mr. Cohen testified "I didn't actually set that up" and "it was done by a young lady that worked for [the IT firm] RedFinch."⁷ Mr. Cohen's statement in this respect may also be false. The owner of RedFinch, John Gauger, reportedly told *The Wall Street Journal* that RedFinch established the @WomenForCohen account at Mr. Cohen's direction. According to the *Journal*, "Mr. Cohen . . . asked Mr. Gauger to create the @WomenForCohen account, still active in 2019, to elevate his profile."⁸ Mr. Cohen's testimony here is material to the Committee's assessment of Mr. Cohen's character and credibility.
4. Mr. Cohen attested in his signed Truth in Testimony form, submitted as Attachment A to this letter, that he did not have any reportable contracts with foreign government entities.

⁴ Cohen hearing, *supra* note 1.

⁵ Bo Dietl (@BoDietl), TWITTER (Feb. 27, 2019, 11:13 AM), <https://twitter.com/BoDietl/status/1100790950203478018>.

⁶ Dr. Darrell Scott (@PastorDScott), TWITTER (Feb. 27, 2019, 3:44 PM), <https://twitter.com/PastorDScott/status/1100859134948315138>.

⁷ Cohen hearing, *supra* note 1.

⁸ Michael Rothfeld, et al., *Cohen Hired IT Firm to Rig Early CNBC, Drudge Polls to Favor Trump*, WALL ST. J. (Jan. 17, 2019), <https://www.wsj.com/articles/poll-rigging-for-trump-and-creating-womenforcohen-one-it-firms-work-order-11547722801>.

The Honorable William Barr

February 28, 2019

Page 4

We believe this to be false. Mr. Cohen testified during the hearing that he had entered into contractual agreements during 2017 with at least two foreign entities owned in part by foreign governments – BTA Bank of Kazakhstan and Korea Aerospace Industries of South Korea.⁹ Mr. Cohen’s testimony here is material to the Committee’s assessment of Mr. Cohen’s character and credibility.

During the hearing, Representative Meadows referred Mr. Cohen to the Justice Department for investigation into whether any of Mr. Cohen’s lobbying or consulting activities were done in violation of the Foreign Agents Registration Act (FARA). At a minimum Mr. Cohen committed fraud against the companies he agreed to represent by accepting their payment and not performing his contractual obligations. We request the Department investigate Mr. Cohen’s potentially false statement on his Truth in Testimony form, the fraud carried out against the companies he agreed to represent, and his potential violation of FARA.

5. Mr. Cohen’s verbal testimony contradicted various aspects of his written statement submitted in advance of his appearance and appended as Attachment B to this letter. These contradictions between Mr. Cohen’s verbal testimony and his written statement materially affect the Committee’s assessment of Mr. Cohen’s credibility.
 - A. For instance, Mr. Cohen verbally testified that he was a good lawyer who understood the need to present his client with sound legal advice.¹⁰ Mr. Cohen contradicted his verbal testimony in his written statement by testifying that he made a payment to Stephanie Clifford “without bothering to consider whether that was improper, much less whether it was the right thing to do....”¹¹
 - B. Mr. Cohen also contradicted his written statement by verbally testifying that the President directed him and Trump Organization Chief Financial Officer Allen Weisselberg to “go back to his office and figure out how to [make the \$130,000 payment to Ms. Clifford.]”¹² In his written statement, however, Mr. Cohen testified that “Mr. Trump directed me to use my own personal funds from a [HELOC] to avoid any money being traced back to him that could negatively impact his campaign.”¹³

⁹ Cohen hearing, *supra* note 1.

¹⁰ *Id.*

¹¹ *Hearing with Michael Cohen, Former attorney for President Donald Trump*: Hearing before the H. Comm. on Oversight & Reform, 116th Cong. (2019) (written testimony of Michael D. Cohen) [hereinafter “Cohen written testimony”].

¹² Cohen hearing, *supra* note 1.

¹³ Cohen written testimony, *supra* note 11.

The Honorable William Barr
 February 28, 2019
 Page 5

6. Mr. Cohen continued to assert that he committed his crimes out of “blind loyalty” to President Trump. In Mr. Cohen’s closing remarks, he testified: “My loyalty to Mr. Trump has cost me everything – my family’s happiness, friendships, my law license, my company, my livelihood, my honor, my reputation, and soon my freedom.”¹⁴ This too is a false statement. The SDNY prosecutors¹⁵, and Judge Pauley¹⁶, specifically found that Mr. Cohen’s conduct was not the result of “blind loyalty” but of Mr. Cohen’s personal greed and ambition. Mr. Cohen’s attribution of the motivation for his crimes materially affects the Committee’s assessment of his character and credibility.

In sum, Mr. Cohen’s testimony before the Committee on Oversight and Reform on February 27, 2019, was a spectacular and brazen attempt to knowingly and willfully testify falsely and fictitiously to numerous material facts. His testimony included intentionally false statements designed to make himself look better on a national stage. Mr. Cohen’s prior conviction for lying to Congress merits a heightened suspicion that he has yet again testified falsely before Congress. We therefore request that the Department investigate whether any of Mr. Cohen’s testimony warrants another charge for the violation of 18 U.S.C. §§ 1001 or 1621.

Thank you for your attention to this important matter.

Sincerely,



Jim Jordan
 Ranking Member



Mark Meadows
 Ranking Member
 Subcommittee on Government Operations

cc: Robert S. Khuzami, Deputy United States Attorney, Southern District of New York
 Robert Mueller, Special Counsel, Department of Justice
 The Honorable Elijah E. Cummings, Chairman, Committee on Oversight and Reform
 The Honorable Jerrold Nadler, Chairman, Committee on the Judiciary
 The Honorable Doug Collins, Ranking Member, Committee on the Judiciary
 The Honorable Devin Nunes, Ranking Member, Permanent Select Committee on Intelligence
 The Honorable Lindsey Graham, Chairman, Senate Committee on the Judiciary

¹⁴ Cohen hearing, *supra* note 1.

¹⁵ See The Government’s Sentencing Memorandum, *United States v. Cohen*, 18-cr-602 (S.D.N.Y. Dec. 7, 2018).

¹⁶ Statement of Judge William H. Pauley III, *United States v. Cohen*, Nos. 18-cr-602, 18-cr-850, at 31 (S.D.N.Y. Dec. 12, 2018) (sentencing hearing).

The Honorable William Barr
February 28, 2019
Page 6

Enclosures: Attachment A: Michael Cohen's Truth in Testimony form (Feb. 27, 2019)
Attachment B: Michael Cohen's written testimony (Feb. 27, 2019)

Attachment A

Truth in Testimony Disclosure Form

In accordance with Rule XI, clause 2(g)(5)*, of the *Rules of the House of Representatives*, witnesses are asked to disclose the following information. Please complete this form electronically by filling in the provided blanks.

Committee: Committee on Oversight and Reform

Subcommittee: _____

Hearing Date: 2/27/19

Hearing Subject:

Hearing with Michael Cohen, former Attorney
to President Donald Trump

Witness Name: MICHAEL DEAN COHEN

Position/Title: _____

Witness Type: Governmental Non-governmental

Are you representing yourself or an organization? Self Organization

If you are representing an organization, please list what entity or entities you are representing:

If you are a **non-governmental witness**, please list any federal grants or contracts (including subgrants or subcontracts) related to the hearing's subject matter that you or the organization(s) you represent at this hearing received in the current calendar year and previous two calendar years. Include the source and amount of each grant or contract. *If necessary, attach additional sheet(s) to provide more information.*

N/A

If you are a **non-governmental witness**, please list any contracts or payments originating with a foreign government and related to the hearing's subject matter that you or the organization(s) you represent at this hearing received in the current year and previous two calendar years. Include the amount and country of origin of each contract or payment. *If necessary, attach additional sheet(s) to provide more information.*

N/A

False Statements Certification

Knowingly providing material false information to this committee/subcommittee, or knowingly concealing material information from this committee/subcommittee, is a crime (18 U.S.C. § 1001). This form will be made part of the hearing record.

Witness signature



Date

2/27/19

If you are a **non-governmental witness**, please ensure that you attach the following documents to this disclosure. Check both boxes to acknowledge that you have done so.

- Written statement of proposed testimony
- Curriculum vitae

*Rule XI, clause 2(g)(5), of the U.S. House of Representatives provides:

(5)(A) Each committee shall, to the greatest extent practicable, require witnesses who appear before it to submit in advance written statements of proposed testimony and to limit their initial presentations to the committee to brief summaries thereof.

(B) In the case of a witness appearing in a nongovernmental capacity, a written statement of proposed testimony shall include a curriculum vitae and a disclosure of any Federal grants or contracts, or contracts or payments originating with a foreign government, received during the current calendar year or either of the two previous calendar years by the witness or by an entity represented by the witness and related to the subject matter of the hearing.

(C) The disclosure referred to in subdivision (B) shall include—

- (i) the amount and source of each Federal grant (or subgrant thereof) or contract (or subcontract thereof) related to the subject matter of the hearing; and
- (ii) the amount and country of origin of any payment or contract related to the subject matter of the hearing originating with a foreign government.

(D) Such statements, with appropriate redactions to protect the privacy or security of the witness, shall be made publicly available in electronic form not later than one day after the witness appears.

Attachment B

**TESTIMONY OF MICHAEL D. COHEN
COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES**

FEBRUARY 27, 2019

Chairman Cummings, Ranking Member Jordan, and Members of the Committee, thank you for inviting me here today.

I have asked this Committee to ensure that my family be protected from Presidential threats, and that the Committee be sensitive to the questions pertaining to ongoing investigations. Thank you for your help and for your understanding.

I am here under oath to correct the record, to answer the Committee's questions truthfully, and to offer the American people what I know about President Trump.

I recognize that some of you may doubt and attack me on my credibility. It is for this reason that I have incorporated into this opening statement documents that are irrefutable, and demonstrate that the information you will hear is accurate and truthful.

Never in a million years did I imagine, when I accepted a job in 2007 to work for Donald Trump, that he would one day run for President, launch a

campaign on a platform of hate and intolerance, and actually win. I regret the day I said “yes” to Mr. Trump. I regret all the help and support I gave him along the way.

I am ashamed of my own failings, and I publicly accepted responsibility for them by pleading guilty in the Southern District of New York.

I am ashamed of my weakness and misplaced loyalty – of the things I did for Mr. Trump in an effort to protect and promote him.

I am ashamed that I chose to take part in concealing Mr. Trump’s illicit acts rather than listening to my own conscience.

I am ashamed because I know what Mr. Trump is.

He is a racist.

He is a conman.

He is a cheat.

He was a presidential candidate who knew that Roger Stone was talking with Julian Assange about a WikiLeaks drop of Democratic National Committee emails.

I will explain each in a few moments.

I am providing the Committee today with several documents. These include:

- A copy of a check Mr. Trump wrote from his personal bank account – after he became president - to reimburse me for the hush money payments I made to cover up his affair with an adult film star and prevent damage to his campaign;
- Copies of financial statements for 2011 – 2013 that he gave to such institutions as Deutsche Bank;
- A copy of an article with Mr. Trump’s handwriting on it that reported on the auction of a portrait of himself – he arranged for the bidder ahead of time and then reimbursed the bidder from the account of his non-profit charitable foundation, with the picture now hanging in one of his country clubs; and
- Copies of letters I wrote at Mr. Trump’s direction that threatened his high school, colleges, and the College Board not to release his grades or SAT scores.

I hope my appearance here today, my guilty plea, and my work with law enforcement agencies are steps along a path of redemption that will restore faith in me and help this country understand our president better.

Before going further, I want to apologize to each of you and to Congress as a whole.

The last time I appeared before Congress, I came to protect Mr. Trump. Today, I'm here to tell the truth about Mr. Trump.

I lied to Congress about when Mr. Trump stopped negotiating the Moscow Tower project in Russia. I stated that we stopped negotiating in January 2016. That was false – our negotiations continued for months later during the campaign.

Mr. Trump did not directly tell me to lie to Congress. That's not how he operates.

In conversations we had during the campaign, at the same time I was actively negotiating in Russia for him, he would look me in the eye and tell

me there's no business in Russia and then go out and lie to the American people by saying the same thing. In his way, he was telling me to lie.

There were at least a half-dozen times between the Iowa Caucus in January 2016 and the end of June when he would ask me "How's it going in Russia?" – referring to the Moscow Tower project.

You need to know that Mr. Trump's personal lawyers reviewed and edited my statement to Congress about the timing of the Moscow Tower negotiations before I gave it.

To be clear: Mr. Trump knew of and directed the Trump Moscow negotiations throughout the campaign and lied about it. He lied about it because he never expected to win the election. He also lied about it because he stood to make hundreds of millions of dollars on the Moscow real estate project.

And so I lied about it, too – because Mr. Trump had made clear to me, through his personal statements to me that we both knew were false and through his lies to the country, that he wanted me to lie. And he made it

clear to me because his personal attorneys reviewed my statement before I gave it to Congress.

Over the past two years, I have been smeared as “a rat” by the President of the United States. The truth is much different, and let me take a brief moment to introduce myself.

My name is Michael Dean Cohen.

I am a blessed husband of 24 years and a father to an incredible daughter and son. When I married my wife, I promised her that I would love her, cherish her, and protect her. As my father said countless times throughout my childhood, “you my wife, and you my children, are the air that I breathe.” To my Laura, my Sami, and my Jake, there is nothing I wouldn’t do to protect you.

I have always tried to live a life of loyalty, friendship, generosity, and compassion – qualities my parents ingrained in my siblings and me since childhood. My father survived the Holocaust thanks to the compassion and selfless acts of others. He was helped by many who put themselves in harm’s way to do what they knew was right.

That is why my first instinct has always been to help those in need. Mom and Dad...I am sorry that I let you down.

As many people that know me best would say, I am the person they would call at 3AM if they needed help. I proudly remember being the emergency contact for many of my children's friends when they were growing up because their parents knew that I would drop everything and care for them as if they were my own.

Yet, last fall I pled guilty in federal court to felonies for the benefit of, at the direction of, and in coordination with Individual #1.

For the record: Individual #1 is President Donald J. Trump.

It is painful to admit that I was motivated by ambition at times. It is even more painful to admit that many times I ignored my conscience and acted loyal to a man when I should not have. Sitting here today, it seems unbelievable that I was so mesmerized by Donald Trump that I was willing to do things for him that I knew were absolutely wrong.

For that reason, I have come here to apologize to my family, to the government, and to the American people.

Accordingly, let me now tell you about Mr. Trump.

I got to know him very well, working very closely with him for more than 10 years, as his Executive Vice President and Special Counsel and then personal attorney when he became President. When I first met Mr. Trump, he was a successful entrepreneur, a real estate giant, and an icon. Being around Mr. Trump was intoxicating. When you were in his presence, you felt like you were involved in something greater than yourself -- that you were somehow changing the world.

I wound up touting the Trump narrative for over a decade. That was my job. Always stay on message. Always defend. It monopolized my life. At first, I worked mostly on real estate developments and other business transactions. Shortly thereafter, Mr. Trump brought me into his personal life and private dealings. Over time, I saw his true character revealed.

Mr. Trump is an enigma. He is complicated, as am I. He has both good and bad, as do we all. But the bad far outweighs the good, and since taking office, he has become the worst version of himself. He is capable of behaving kindly, but he is not kind. He is capable of committing acts of generosity, but he is not generous. He is capable of being loyal, but he is fundamentally disloyal.

Donald Trump is a man who ran for office to make his brand great, not to make our country great. He had no desire or intention to lead this nation – only to market himself and to build his wealth and power. Mr. Trump would often say, this campaign was going to be the “greatest infomercial in political history.”

He never expected to win the primary. He never expected to win the general election. The campaign – for him – was always a marketing opportunity.

I knew early on in my work for Mr. Trump that he would direct me to lie to further his business interests. I am ashamed to say, that when it was for a real estate mogul in the private sector, I considered it trivial. As the President, I consider it significant and dangerous.

But in the mix, lying for Mr. Trump was normalized, and no one around him questioned it. In fairness, no one around him today questions it, either.

A lot of people have asked me about whether Mr. Trump knew about the release of the hacked Democratic National Committee emails ahead of time. The answer is yes.

As I earlier stated, Mr. Trump knew from Roger Stone in advance about the WikiLeaks drop of emails.

In July 2016, days before the Democratic convention, I was in Mr. Trump's office when his secretary announced that Roger Stone was on the phone. Mr. Trump put Mr. Stone on the speakerphone. Mr. Stone told Mr. Trump that he had just gotten off the phone with Julian Assange and that Mr. Assange told Mr. Stone that, within a couple of days, there would be a massive dump of emails that would damage Hillary Clinton's campaign. Mr. Trump responded by stating to the effect of "wouldn't that be great."

Mr. Trump is a racist. The country has seen Mr. Trump court white supremacists and bigots. You have heard him call poorer countries "shitholes."

In private, he is even worse.

He once asked me if I could name a country run by a black person that wasn't a "shithole." This was when Barack Obama was President of the United States.

While we were once driving through a struggling neighborhood in Chicago, he commented that only black people could live that way.

And, he told me that black people would never vote for him because they were too stupid.

And yet I continued to work for him.

Mr. Trump is a cheat.

As previously stated, I'm giving the Committee today three years of President Trump's financial statements, from 2011-2013, which he gave to Deutsche Bank to inquire about a loan to buy the Buffalo Bills and to Forbes. These are Exhibits 1a, 1b, and 1c to my testimony.

It was my experience that Mr. Trump inflated his total assets when it served his purposes, such as trying to be listed among the wealthiest people in Forbes, and deflated his assets to reduce his real estate taxes.

I am sharing with you two newspaper articles, side by side, that are examples of Mr. Trump inflating and deflating his assets, as I said, to suit his financial interests. These are Exhibit 2 to my testimony.

As I noted, I'm giving the Committee today an article he wrote on, and sent me, that reported on an auction of a portrait of Mr. Trump. This is Exhibit 3A to my testimony.

Mr. Trump directed me to find a straw bidder to purchase a portrait of him that was being auctioned at an Art Hamptons Event. The objective was to ensure that his portrait, which was going to be auctioned last, would go for the highest price of any portrait that afternoon. The portrait was purchased by the fake bidder for \$60,000. Mr. Trump directed the Trump Foundation, which is supposed to be a charitable organization, to repay the fake bidder, despite keeping the art for himself. Please see Exhibit 3B to my testimony.

And it should come as no surprise that one of my more common responsibilities was that Mr. Trump directed me to call business owners, many of whom were small businesses, that were owed money for their services and told them no payment or a reduced payment would be coming. When I advised Mr. Trump of my success, he actually reveled in it.

And yet, I continued to work for him.

Mr. Trump is a conman.

He asked me to pay off an adult film star with whom he had an affair, and to lie to his wife about it, which I did. Lying to the First Lady is one of my biggest regrets. She is a kind, good person. I respect her greatly – and she did not deserve that.

I am giving the Committee today a copy of the \$130,000 wire transfer from me to Ms. Clifford's attorney during the closing days of the presidential campaign that was demanded by Ms. Clifford to maintain her silence about her affair with Mr. Trump. This is Exhibit 4 to my testimony.

Mr. Trump directed me to use my own personal funds from a Home Equity Line of Credit to avoid any money being traced back to him that could negatively impact his campaign. I did that, too – without bothering to consider whether that was improper, much less whether it was the right thing to do or how it would impact me, my family, or the public.

I am going to jail in part because of my decision to help Mr. Trump hide that payment from the American people before they voted a few days later.

As Exhibit 5A to my testimony shows, I am providing a copy of a \$35,000 check that President Trump *personally* signed from his *personal* bank

account on August 1, 2017 – when he was President of the United States – pursuant to the cover-up, which was the basis of my guilty plea, to reimburse me – the word used by Mr. Trump’s TV lawyer -- for the illegal hush money I paid on his behalf. This \$35,000 check was one of 11 check installments that was paid throughout the year – while he was President. Other checks to reimburse me for the hush money payments were signed by Don Jr. and Allen Weisselberg. See, for example, Exhibit 5B.

The President of the United States thus wrote a personal check for the payment of hush money as part of a criminal scheme to violate campaign finance laws. You can find the details of that scheme, directed by Mr. Trump, in the pleadings in the U.S. District Court for the Southern District of New York.

So picture this scene – in February 2017, one month into his presidency, I’m visiting President Trump in the Oval Office for the first time. It’s truly awe-inspiring, he’s showing me around and pointing to different paintings, and he says to me something to the effect of...Don’t worry, Michael, your January and February reimbursement checks are coming. They were Fed-Exed from New York and it takes a while for that to get through the White

House system. As he promised, I received the first check for the reimbursement of \$70,000 not long thereafter.

When I say conman, I'm talking about a man who declares himself brilliant but directed me to threaten his high school, his colleges, and the College Board to never release his grades or SAT scores.

As I mentioned, I'm giving the Committee today copies of a letter I sent at Mr. Trump's direction threatening these schools with civil and criminal actions if Mr. Trump's grades or SAT scores were ever disclosed without his permission. These are Exhibit 6.

The irony wasn't lost on me at the time that Mr. Trump in 2011 had strongly criticized President Obama for not releasing his grades. As you can see in Exhibit 7, Mr. Trump declared "Let him show his records" after calling President Obama "a terrible student."

The sad fact is that I never heard Mr. Trump say anything in private that led me to believe he loved our nation or wanted to make it better. In fact, he did the opposite.

When telling me in 2008 that he was cutting employees' salaries in half – including mine – he showed me what he claimed was a \$10 million IRS tax

refund, and he said that he could not believe how stupid the government was for giving “someone like him” that much money back.

During the campaign, Mr. Trump said he did not consider Vietnam Veteran, and Prisoner of War, Senator John McCain to be “a hero” because he likes people who weren’t captured. At the same time, Mr. Trump tasked me to handle the negative press surrounding his medical deferment from the Vietnam draft.

Mr. Trump claimed it was because of a bone spur, but when I asked for medical records, he gave me none and said there was no surgery. He told me not to answer the specific questions by reporters but rather offer simply the fact that he received a medical deferment.

He finished the conversation with the following comment. “You think I’m stupid, I wasn’t going to Vietnam.”

I find it ironic, President Trump, that you are in Vietnam right now.

And yet, I continued to work for him.

Questions have been raised about whether I know of direct evidence that Mr. Trump or his campaign colluded with Russia. I do not. I want to be clear. But, I have my suspicions.

Sometime in the summer of 2017, I read all over the media that there had been a meeting in Trump Tower in June 2016 involving Don Jr. and others from the campaign with Russians, including a representative of the Russian government, and an email setting up the meeting with the subject line, “Dirt on Hillary Clinton.” Something clicked in my mind. I remember being in the room with Mr. Trump, probably in early June 2016, when something peculiar happened. Don Jr. came into the room and walked behind his father’s desk – which in itself was unusual. People didn’t just walk behind Mr. Trump’s desk to talk to him. I recalled Don Jr. leaning over to his father and speaking in a low voice, which I could clearly hear, and saying: “The meeting is all set.” I remember Mr. Trump saying, “Ok good...let me know.”

What struck me as I looked back and thought about that exchange between Don Jr. and his father was, first, that Mr. Trump had frequently told me and others that his son Don Jr. had the worst judgment of anyone in the world. And also, that Don Jr. would never set up any meeting of any significance alone – and certainly not without checking with his father.

I also knew that nothing went on in Trump world, especially the campaign, without Mr. Trump's knowledge and approval. So, I concluded that Don Jr. was referring to *that* June 2016 Trump Tower meeting about dirt on Hillary with the Russian representative when he walked behind his dad's desk that day -- *and* that Mr. Trump knew that was the meeting Don Jr. was talking about when he said, "That's good...let me know."

Over the past year or so, I have done some real soul searching. I see now that my ambition and the intoxication of Trump power had much to do with the bad decisions I made.

To you, Chairman Cummings, Ranking Member Jordan, the other members of this Committee, and the other members of the House and Senate, I am sorry for my lies and for lying to Congress.

To our nation, I am sorry for actively working to hide from you the truth about Mr. Trump when you needed it most.

For those who question my motives for being here today, I understand. I have lied, but I am not a liar. I have done bad things, but I am not a bad man. I have fixed things, but I am no longer your "fixer," Mr. Trump.

I am going to prison and have shattered the safety and security that I tried so hard to provide for my family. My testimony certainly does not diminish the pain I caused my family and friends – nothing can do that. And I have never asked for, nor would I accept, a pardon from President Trump.

And, by coming today, I have caused my family to be the target of personal, scurrilous attacks by the President and his lawyer – trying to intimidate me from appearing before this panel. Mr. Trump called me a “rat” for choosing to tell the truth – much like a mobster would do when one of his men decides to cooperate with the government.

As Exhibit 8 shows, I have provided the Committee with copies of Tweets that Mr. Trump posted, attacking me and my family – only someone burying his head in the sand would not recognize them for what they are: encouragement to someone to do harm to me and my family.

I never imagined that he would engage in vicious, false attacks on my family – and unleash his TV-lawyer to do the same. I hope this committee and all members of Congress on both sides of the aisle will make it clear: As a nation, we should not tolerate attempts to intimidate witnesses before congress and attacks on family are out of bounds and not acceptable.

I wish to especially thank Speaker Pelosi for her statements in Exhibit 9 to protect this institution and me, and the Chairman of the House Permanent Select Committee on Intelligence Adam Schiff and Chairman Cummings for likewise defending this institution and my family against the attacks by Mr. Trump, and also the many Republicans who have admonished the President as well.

I am not a perfect man. I have done things I am not proud of, and I will live with the consequences of my actions for the rest of my life.

But today, I get to decide the example I set for my children and how I attempt to change how history will remember me. I may not be able to change the past, but I can do right by the American people here today.

Thank you for your attention. I am happy to answer the Committee's questions.

#####

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051

MINORITY (202) 225-5074

<http://oversight.house.gov>

March 8, 2019

Mr. Michael D. Monico
Monico & Spevack
20 S. Clark Street
Suite 700
Chicago, IL 60603

Dear Mr. Monico:

We write concerning contradictions between the testimony of your client, Michael D. Cohen, before the House Oversight and Reform Committee and media statements made by Chairman Adam Schiff of the House Permanent Select Committee on Intelligence (HPSCI). When Cohen's media advisor and attorney, Lanny J. Davis, initially met with our staff on behalf of Cohen on January 18, 2019, he indicated Cohen would only be testifying before our Committee.¹ This representation, of course, did not prove to be accurate. In addition to our Committee, Cohen testified before the Senate Select Committee on Intelligence and HPSCI.

Michael Cohen and Chairman Schiff seem to have provided conflicting versions of discussions they had in advance of Cohen's congressional testimony. During his testimony before our Committee, Cohen discussed how he prepared for his testimony, including talking with Members of Congress. Cohen testified he spoke to Chairman Schiff about "topics" for Cohen's upcoming testimony before HPSCI:

Mr. Jordan. Let me ask you one question... What did you talk to Mr. Schiff about?

Mr. Cohen. I spoke to Mr. Schiff about topics that were going to be raised at the upcoming hearing.²

However, in a subsequent interview on CBS News' *Face The Nation*, Chairman Schiff downplayed and contradicted Michael Cohen's testimony about the nature of their discussions, saying the conversations were limited to Cohen's security at the HPSCI hearing. Chairman Schiff explained:

¹ See Letter from Jim Jordan and Mark Meadows, H. Comm. on Oversight & Reform, to Guy Petrillo (Jan. 22, 2019).

² *Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 121 (2019) (statement of Michael D. Cohen).

Mr. Michael D. Monico
March 8, 2019
Page 2

Margaret Brennan: Was that the extent of your contact [with Michael Cohen]?

Rep. Schiff: The extent of my contact was just inviting him to testify and also trying to allay his concerns about the President's threats against him and his family...³

These conflicting statements cannot both be true – either they discussed hearing “topics” or they did not. If Chairman Schiff’s communications with Cohen were, in fact, as limited as Chairman Schiff stated on *Face the Nation*, then we are faced with the potential that Cohen made another false statement during his testimony before the Committee.⁴

To assist us in evaluating the accuracy and truthfulness of Cohen’s testimony about his discussions with Chairman Schiff in advance of his testimony, please provide:

1. A complete description and account of all communications between Cohen and Chairman Schiff, including dates, times, and “topics” discussed; and
2. A complete description and account of all communications you, or other associates representing Cohen, including Lanny J. Davis, Guy Petrillo, or others, have had with Chairman Schiff or HPSCI regarding Michael Cohen’s testimony prior to his appearances before HPSCI on February 28, 2019, and March 6, 2019.

Please provide this information as soon as possible, but no later than 5:00 p.m. on March 22, 2019. If you have any questions, please contact Committee staff at (202) 225-5074. Thank you for your attention to this matter.

Sincerely,



Jim Jordan
Ranking Member



Mark Meadows
Ranking Member
Subcommittee on Government Operations

cc: The Honorable Elijah E. Cummings, Chairman, Comm. on Oversight and Reform

³ *Face the Nation* (CBS News television broadcast March 3, 2019) <https://www.cbsnews.com/news/transcript-rep-adam-schiff-on-face-the-nation-march-3-2019/>.

⁴ See Letter from Jim Jordan and Mark Meadows to William Barr, Attorney Gen., Dep’t of Justice (Feb. 28, 2019).

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074

<http://oversight.house.gov>

March 13, 2019

The Honorable Elijah E. Cummings
Chairman
Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

This letter follows up on your commitment to ensure Michael Cohen testified truthfully at the Committee's hearing titled, "Hearing with Michael Cohen, Former Attorney for President Donald Trump," on February 27, 2019.¹ As Chairman, it is your obligation to ensure that witnesses are not permitted to lie with impunity when testifying before the Committee.

During the hearing, following Cohen's oath to testify truthfully, you explained to the Committee that you privately admonished Cohen about truthfulness. You warned him "if he [Cohen] came in here and lied I would nail him to the cross."² You then confirmed this statement with Cohen himself, asking "Didn't I tell you that?"³ Cohen replied, "Yes, you did more than once."⁴ Mr. Chairman, there is now clear and indisputable evidence that Cohen did not testify truthfully before the Committee. We expect you will now follow through with your commitment to hold Cohen accountable.

Following the hearing, we wrote to Attorney General William Barr referring Cohen for a perjury investigation regarding six areas of problematic testimony, including Cohen's testimony that he did not want a role in the Trump Administration.⁵ In light of mounting evidence, it appears Cohen likely lied under oath during his appearance before the Committee. Even the Committee's Vice Chair, Rep. Katie Hill, said on Sunday that she expects that you will refer Cohen to the Justice Department for perjury.⁶ We write to ask that you join our referral and

¹ *Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. (2019).

² *Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 171 (2019) [hereinafter "Cohen Hearing Transcript"].

³ *Id.*

⁴ *Id.*

⁵ Letter from Jim Jordan & Mark Meadows, H. Comm. on Oversight & Reform, to William P. Barr, Attorney Gen., Dep't of Justice (Feb. 28, 2019).

⁶ Brett Samuels, *Oversight Dem: "I imagine" chairman will ask for investigation into Cohen for alleged perjury*, The Hill (Mar. 10, 2019).

The Honorable Elijah E. Cummings
March 13, 2019
Page 2

request all relevant documents and communications from Cohen and the Department of Justice (DOJ).

Cohen lied about his desire to work in the Trump Administration

Prior to the hearing, we asked that you request information from the DOJ necessary to question Cohen. You declined to do so, leaving Members to rely on publicly available information. We reviewed court filings by the United States Attorney's Office for the Southern District of New York (SDNY), which discussed Cohen's desire and expectation of receiving a role in the Trump Administration. The SDNY prosecutors explained:

During and after the campaign, Cohen privately told friends and colleagues, including in *seized text messages*, that he expected to be given a prominent role and title in the new administration. When that did not materialize, Cohen found a way to monetize his relationship with and access to the President.⁷

During the hearing, Republican Members pressed Cohen on the SDNY prosecutors' statements. On the record, following his oath, Cohen repeatedly testified that he did not seek employment in the White House following President Trump's election. Cohen also testified that the statement submitted by the SDNY prosecutors to the court was "not accurate."⁸ Several Members followed up with Cohen on this account:

MR. CLOUD: In today's testimony, you [Cohen] said that you were not looking to work in the White House. The Southern District of New York, in their statement, their sentencing memo, says this: ". . . Cohen privately told friends, colleagues, and including seized text messages, that he expected to be given a prominent role in the new administration." . . . So were they lying, or were you lying today?

MR. COHEN: I'm not saying it's a lie. I'm just saying it's not accurate. I did not want to go to the White House.⁹

Following the exchange between Mr. Cloud and Cohen, Mr. Jordan provided Cohen an opportunity to clarify his remarks. He did not.

⁷ The Government's Sentencing Memorandum at 25, *United States v. Cohen*, 18-cr-602 (S.D.N.Y. Dec. 7, 2018) (emphasis added).

⁸ Cohen Hearing Transcript, *supra* note 2, at 96.

⁹ *Id.*

The Honorable Elijah E. Cummings

March 13, 2019

Page 3

MR. JORDAN: Earlier you said that the United States Southern District of New York Attorney's Office, that statement is not accurate. You said it's not a lie. You said it's not accurate. Do you stand by that?

MR. COHEN: Yes, I did not want a role in the new [Trump] Administration.

MR. JORDAN: So the court's wrong?

MR. COHEN: Sir, can I finish, please?

MR. JORDAN: Sure.

MR. COHEN: I got exactly the role that I wanted. There is no shame in being personal attorney to the President. I got exactly what I wanted. I asked Mr. Trump for that job, and he gave it to me.

MR. JORDAN: All I'm asking, if I could -- and I appreciate it, Mr. Chairman -- you're saying that statement from the Southern District of New York attorneys is wrong.

MR. COHEN: I'm saying I didn't write it, and it's not accurate.

MR. JORDAN: All right. Thank you.¹⁰

MR. ROY: You said clearly to Mr. Cloud and Mr. Jordan that the Southern District of New York lawyers were being untruthful in characterizing your desire to work in the administration. Do you say again that the lawyers of the Southern District of New York are being untruthful in making that characterization, yes or no?

¹⁰ Cohen Hearing Transcript, *supra* note 2, at 127.

The Honorable Elijah E. Cummings

March 13, 2019

Page 4

MR. COHEN: I'm saying that's not accurate.¹¹

MR. ROY: Okay. So you're saying they're being untruthful.

MR. COHEN: I'm not using the word untruthful, that's yours. I'm saying that that's not accurate. I did not want a role or a title in the administration.¹²

As indicated by the SDNY prosecutors, text messages exist that prove Cohen sought out a job with the White House, directly contradicting Cohen's statements under oath before our Committee. To maintain the integrity of our investigations and hearings, we must obtain these messages and any other potential evidence to get the truth.

The SDNY prosecutors are not the only individuals who believe that Cohen sought out a job at the White House. Several people have spoken out publicly to refute Cohen's statements before this Committee.¹³ For example, Bo Dietl, a former New York City Police detective, tweeted during the Committee's hearing:

Getting sick watching these hearings. I know Michael Cohen personally for many years and he told me several times that he was very angry and upset that he didn't get a post in the WH and that he 'would do what he has to do now to protect his family.'¹⁴

Dr. Darrell Scott, Pastor at the New Spirit Revival Center and a Trump campaign faith-based outreach coordinator, also tweeted during the hearing: "Michael Cohen asked . . . no, BEGGED me REPEATEDLY, to ask the POTUS to give him a job in the Administration! He's STILL lying under oath!"¹⁵ Bruce LeVell, another person involved in the Trump campaign, replied to Dr. Scott's tweet, "I co-sign that Pastor. I remember that conversation[.]"¹⁶

David Bossie, Trump's deputy campaign manager in 2016, tweeted, "Michael Cohen asked me to support his effort to be Chief of Staff when I helped run the Presidential Transition Team. He perjured himself today."¹⁷

¹¹ *Id.* at 162.

¹² *Id.* at 162-63.

¹³ Chris Cillizza, *Why One Simple Lie by Michael Cohen Could Invalidate His Entire Testimony*, CNN (Feb. 28, 2019), <https://amp.cnn.com/cnn/2019/02/28/politics/michael-cohen-donald-trump-white-house/index.html>.

¹⁴ Bo Dietl (@BoDietl), TWITTER (Feb. 27, 2019, 11:13 AM), <https://twitter.com/BoDietl/status/1100790950203478018>.

¹⁵ Dr. Darrell Scott (@PastorDScott), TWITTER (Feb. 27, 2019, 3:44 PM), <https://twitter.com/PastorDScott/status/1100859134948315138>.

¹⁶ Bruce LeVell (@Bruce_LeVell), TWITTER (Feb. 27, 2019, 3:47 PM), https://twitter.com/Bruce_LeVell/status/1100860065786007565.

¹⁷ David Bossie (@David_Bossie), TWITTER (Feb. 27, 2019, 5:12 PM), https://twitter.com/David_Bossie/status/1100926661397278723.

The Honorable Elijah E. Cummings

March 13, 2019

Page 5

During the hearing, CNN journalist Dana Bash rebutted Cohen's testimony on live television. She stated, "the one potential problem that I thought Michael Cohen has is when he was asked if he wanted a job in the White House, and he said no. Our reporting [shows] . . . he very much wanted a job in the White House."¹⁸ Another CNN journalist, Nathan McDermott, tweeted, "Good point by @DanaBashCNN that when Cohen was asked in the hearings whether he wanted a job in the White House and he said 'no' he contradicted mountains of reporting that show he did, in fact, want one."¹⁹

Cohen lied about not seeking a pardon

Cohen made an additional false statement to this Committee when he testified under oath: "I have never asked for, nor would I accept, a pardon from President Trump."²⁰ Last week, however, Lanny Davis, Cohen's media advisor and lawyer, contradicted Cohen's testimony. Davis stated that Cohen had "directed his attorney to explore possibilities of a pardon at one point with Trump lawyer Rudy Giuliani as well as other lawyers advising President Trump."²¹

On March 12, nearly two weeks after Cohen's testimony, his lawyer, Michael Monico, sent you a letter conceding that Cohen's statement about a pardon was not accurate and "could have been clearer" but stating that Cohen stood by his testimony.²² Monico asserted that Cohen wrote his statement about the pardon "in the context of [his] decision in June 2018 to leave the Trump Joint Defense Agreement"²³

This *ex post* assertion by Cohen's lawyers does not undo Cohen's intentionally false and misleading statement and is manifestly unpersuasive. Regardless of the context in which Cohen wrote this statement, Cohen *uttered* the statement under oath in the context of apologizing for all his criminal activities. Cohen's denial of ever seeking a pardon, which he made during his carefully crafted opening statement, contained no qualifiers about the context of his statement. It did not restrict his denial to the period after Cohen left the joint defense agreement. In fact, there is no mention whatsoever in Cohen's prepared testimony about the joint defense agreement. Simply put, Cohen's denial of ever seeking a pardon, as uttered under oath in his testimony, was absolute and unequivocal.

Although Cohen's attorneys now claim that Cohen did not mislead the Committee, it is clear—and Cohen's lawyers concede—that Cohen asked his legal representatives to seek a

¹⁸ CNN Newsroom (@CNNnewsroom), TWITTER (Feb. 27, 2019, 9:25 AM), <https://twitter.com/CNNnewsroom/status/1100809107026538496>.

¹⁹ Nathan McDermott (@natemcdermott), TWITTER (Feb. 27, 2019, 12:19 PM), <https://twitter.com/natemcdermott/status/1100807647710900224>.

²⁰ Cohen Hearing Transcript, *supra* note 2, at 28.

²¹ Rebecca Ballhaus et al., *Lawyer for Cohen Approached Attorneys About Pardon*, Wall St. J., (Mar. 6, 2019), <https://www.wsj.com/articles/attorney-says-cohen-directed-his-lawyer-to-seek-trump-pardon-contradicting-testimony-11551931412>.

²² Letter from Michael Monico to Elijah E. Cummings, Chairman, H. Comm. on Oversight & Reform (Mar. 12, 2019).

²³ *Id.*

The Honorable Elijah E. Cummings

March 13, 2019

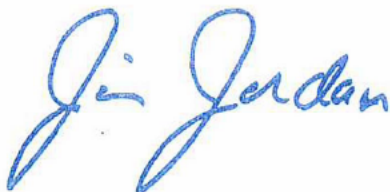
Page 6

pardon on his behalf. Therefore, in light of this undisputed evidence, Cohen's testimony under oath that he "*never* asked for . . . a pardon" cannot be true. Cohen's intentionally false statement under oath is material to the Committee's assessment of his credibility.

* * *

This Committee cannot stand idly by when a witness comes to a hearing, swears an oath to testify truthfully, and provides material testimony that appears on its face to be demonstrably false. Accordingly, we urge you to request from both Michael Cohen and the Department of Justice all documents and communications relating to Cohen's desire or attempts to obtain a position in the Trump Administration, as well as Cohen's efforts to seek a pardon for his crimes. We also encourage you to uphold the prerogatives of the Committee by joining our referral to the Department of Justice.

Thank you for your consideration of this request. We look forward to hearing back from you soon on this important matter.



Jim Jordan
Ranking Member

Sincerely,



Mark Meadows
Ranking Member
Subcommittee on Government Operations

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051

MINORITY (202) 225-5074

<http://oversight.house.gov>

June 7, 2019

The Honorable Elijah E. Cummings
Chairman
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We received your letter, dated May 22, 2019, in which you excused and legitimized Michael Cohen's perjury-laden testimony to our Committee.¹ Cohen was the first announced witness of your chairmanship, who you invited to testify during a made-for-cable-news hearing to attack President Trump for political gain. While your defense of Cohen's testimony is perhaps unsurprising, it ignores information that does not support your analysis and fails to address the totality of lies that Cohen uttered under oath.

You waited to review Cohen's testimony before the House Permanent Select Committee on Intelligence (HPSCI) to determine whether he lied before *our* Committee. Now that HPSCI has released the testimony—following our request—we believe it does not change our earlier conclusions.² Indeed, the HPSCI testimony only reveals new information that is unhelpful and unflattering to you: that Cohen has no independent evidence to support his accusations, and that you engaged in *ex parte* preparation sessions with Cohen to help him to appear more credible before our Committee.

Today marks 100 days since Cohen's testimony. We are deeply disappointed that you have declined to hold Cohen accountable, despite your forceful promises to do so and contrary to Vice Chair Katie Hill's expectation that you would.³ We can only assume that you worry that acknowledging Cohen's lies would undermine the investigations on which they are based and ultimately undercut your partisan attacks upon the President. We hope that you will reconsider your decision, put the institutional interests of the Committee ahead of your political goals, and do what you promised to do.

¹ Letter from Elijah E. Cummings, Chairman, H. Comm. on Oversight & Reform, to Jim Jordan, Ranking Member, H. Comm. on Oversight & Reform (May 22, 2019).

² Letter from Jim Jordan & Mark Meadows, H. Comm. on Oversight & Reform, to Adam B. Schiff & Devin G. Nunes, H. Perm. Select Comm. on Intel. (April 2, 2019).

³ Brett Samuels, *Oversight Dem: "I imagine" chairman will ask for investigation into Cohen for alleged perjury*, THE HILL (Mar. 10, 2019).

Cohen's HPSCI testimony shows that he lied about never seeking a pardon

Your exoneration of Cohen narrowly focuses on only one of Cohen's lies: "I have never asked for, nor would I accept, a pardon from President Trump."⁴ However, a straightforward reading of the sources cited in your May 22 letter—Cohen's attorneys' statements; Cohen's February 28 and March 6 HPSCI testimony; and Special Counsel Robert Mueller III's report—actually contradict your conclusion. These sources provide ample support that Cohen directed his attorneys to seek a pardon from the President, contrary to his sworn statement.

In all three sources Cohen admitted that he spoke, or directed his attorneys to speak, with the President's representatives about a pardon. The Special Counsel's report notes that "Cohen . . . recalled speaking with the President's personal counsel about pardons after the searches of his home and office had occurred . . ."⁵ In his testimony before HPSCI on March 6, Cohen admitted that he directed his then-attorney to discuss a pardon with President Trump's representatives and that he would have accepted it if offered. He testified:

Mr. Cohen: I asked Mr. [Stephen] Ryan [Cohen's former lawyer] to meet with Rudy Giuliani, and I don't recall if Jay [Sekulow] was a party to that, but it was to *explore the possibility of a pardon*, because that possibility was constantly being dangled in my face. *And, yes, I was 100 percent open to accepting it.* Anything to end this.⁶

When asked specifically to reconcile his denial to our Committee about ever seeking a pardon with his testimony to HPSCI, his response was nonsense. He claimed that his written statement to our Committee, which he later uttered aloud publicly under oath—"I have never asked for . . . a pardon from President Trump"—was actually meant to be a statement in the present tense. He said:

Mr. Ratcliffe: Okay. Did you ever make public statements that you would never accept a pardon from President Trump?

Mr. Cohen: I did. Yes, I made that statement.

Mr. Ratcliffe: How do you reconcile that statement with the one you just made?

⁴ *Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 28 (Feb. 27, 2019); *Hearing with Michael Cohen, Former attorney for President Donald Trump: Hearing before the H. Comm. on Oversight & Reform*, 116th Cong. 19 (2019) (written testimony of Michael D. Cohen).

⁵ SPECIAL COUNSEL ROBERT S. MUELLER, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, 147, Vol. 2 (2019); see Letter from Elijah E. Cummings, Chairman, H. Comm. on Oversight & Reform, to Jim Jordan, Ranking Member, H. Comm. on Oversight & Reform (May 22, 2019).

⁶ *Deposition of Michael Cohen, Executive Session before the Perm. Select Comm. on Intel.*, 116th Cong. 115-116 (March 6, 2019) (emphasis added).

Mr. Cohen: Because I was talking about in the present tense, I wasn't talking about in the past tense when I was writing my statement.⁷

Following Cohen's March 6 HPSCI testimony, Cohen's lawyers began to spin his closed-door testimony about the pardon. On March 7, Cohen lawyer and media advisor Lanny Davis admitted that Cohen "directed his attorney to explore possibilities of a pardon at one point with Trump lawyer Rudy Giuliani as well as other lawyers advising President Trump."⁸ On March 12, a second Cohen attorney, Michael Monico, acknowledged that Cohen "asked his then attorney to discuss with another Trump attorney possible pardon options"⁹ Cohen's attorneys still maintained, however, that Cohen did not lie.

Cohen's spin is unconvincing and we are troubled that you have parroted it so readily. Cohen's denial of ever seeking a pardon was unequivocal and unambiguous. It contained no temporal constraints and no qualifications. Cohen's explanation that he was speaking in the present tense is unpersuasive because he specifically included the word "never," which by definition means at no time and under no conditions.¹⁰ Cohen included "never" in his written statement, which he testified that he spent considerable time crafting, meaning that his blanket denial was deliberate and willful.¹¹ Cohen's denial is material in that it goes directly to Cohen's credibility as a witness.

No reasonable person could hear an unequivocal denial containing the word "never" and believe the speaker was referring only to his current actions and state of mind. We are troubled that you could accept this absurd explanation.

Your exoneration of Cohen failed to address his other lies to the Committee

During the Committee's hearing, you warned that "if [Cohen] comes here today and he does not tell him the truth – tell us the truth, I will be the first one to refer that – those untruthful statements to DOJ."¹² We have identified at least seven problematic areas of Cohen's testimony

⁷ *Id.* at 116.

⁸ Andrew Desiderio, *Michael Cohen previously asked Trump attorneys about pardon, his lawyer says*, POLITICO (March 7, 2019).

⁹ Letter from Michael Monico, attorney to Michael Cohen, to Elijah Cummings, Chairman, H. Comm. on Oversight & Reform (March 12, 2019).

¹⁰ *See, e.g., Never*, Merriam-Webster Dictionary (11th ed. 2016).

¹¹ *Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 12 (Feb. 27, 2019) (statement of Michael Cohen) ("We were making edits all the way through the night."); Email from Lanny Davis, attorney to Michael Cohen, to H. Comm. on Oversight & Reform staff (Feb. 26, 2019 at 10:08 p.m.).

¹² *Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 12 (Feb. 27, 2019).

The Honorable Elijah E. Cummings

June 7, 2019

Page 4

that require investigation for potential perjury.¹³ However, your letter of May 22 failed to address Cohen’s other false statements, including but not limited to the following:

- Cohen’s repeated denials of wanting a job in the White House, which is contrary to court documents submitted by the United States Attorney’s Office for the Southern District of New York;¹⁴
- Cohen’s assertion that he “never defrauded any bank,” despite pleading guilty to bank fraud;¹⁵ and
- Cohen’s denial of originating the twitter account, @WomenForCohen, which contrary to the assertion of the owner of an IT firm who recounted that Cohen directed him to create the account.¹⁶

Your refusal to address the entirety of Cohen’s false statements—and instead to focus only on the one statement that Cohen’s attorneys chose to address—speaks volumes. Clearly, you cannot defend all of Cohen’s reckless statements. Cohen has gone so far as to dispute assertions made by a federal judge in open court and to deny that he committed a crime to which he pled guilty.¹⁷ These false statements remain unaddressed and, left uncontested, they will continue to tarnish the Committee’s integrity and credibility.

Cohen’s HPSCI testimony shows that he cannot support his accusations with evidence

The transcripts of Cohen’s HPSCI testimony reveal he is incapable of supporting the accusations that he has levied against the President and the President’s advisors. In particular, Cohen could not provide any documentary evidence related to his accusations that Jay Sekulow helped Cohen craft his false statements to HPSCI in 2017.¹⁸ Cohen also admitted in his

¹³ See Letter from Jim Jordan & Mark Meadows, H. Comm. on Oversight & Reform, to William P. Barr, Att’y Gen., Dep’t of Justice (Feb. 28, 2019).

¹⁴ Compare Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform, 116th Cong. 96 (Feb. 27, 2019) with The Government’s Sentencing Memorandum at 25, United States v. Cohen, 18-cr-602 (S.D.N.Y. Dec. 7, 2018).

¹⁵ Compare Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform, 116th Cong. 49 (Feb. 27, 2019) with Plea Agreement at 3 n.2, United States v. Michael Cohen, 18-cr-602 (S.D.N.Y. Aug. 21, 2018).

¹⁶ Compare Hearing with Michael Cohen, Former Attorney for President Donald Trump: Hearing Before the H. Comm. on Oversight & Reform, 116th Cong. 35 (Feb. 27, 2019) with Michael Rothfeld, *Cohen Hired IT Firm to Rig Early CNBC, Drudge Polls to Favor Trump*, WALL STREET J. (Jan. 17, 2019).

¹⁷ Compare Statement of Michael Cohen, United States v. Cohen, Nos. 18-cr-602, 18-cr-850, at 27 (S.D.N.Y. Dec. 12, 2018) (sentencing hearing) (“...blind loyalty to this man that led me to choose a path of darkness over light.”) with, Statement of Judge William H. Pauley III, United States v. Cohen, Nos. 18-cr-602, 18-cr-850, at 31 (S.D.N.Y. Dec. 12, 2018) (sentencing hearing) (“Each of the crimes involved deception and each appears to have been motivated by personal greed and ambition.”) and The Government’s Sentencing Memorandum at 25, United States v. Cohen, 18-cr-602 (S.D.N.Y. Dec. 7, 2018) (“This was not a blind act of loyalty, as Cohen has also suggested.”); see Plea Agreement at 3 n.2, United States v. Michael Cohen, 18-cr-602 (S.D.N.Y. Aug. 21, 2018).

¹⁸ See Deposition of Michael Cohen, Executive Session before the Perm. Select Comm. on Intel., 116th Cong. 10 (March 6, 2019) (“Q Mr. Cohen, one thing that we did not receive from you were any written communications between you and Jay Sekulow. Were you able to find any? COHEN: I have not been able to locate, as of yet, and the search is continuing.”); Deposition of Michael Cohen, Executive Session before the Perm. Select Comm. on Intel.,

testimony to HPSCI that many of the exhibits Cohen presented to our Committee, such as President Trump's financial statements, were not in fact evidence of a crime:

Mr. Ratcliffe: Well, to be fair, Mr. Cohen, this is your statement which you gave to Congress. And I'm asking you why you submitted these documents. Do you believe - all I'm asking you -- again, this is not a trick question. Do you believe that these documents evidence some crime?

Mr. Cohen: I don't believe, sir, in my statement I reference the 2011 through 2013 financial statements as evidence of any crime.

Mr. Ratcliffe: That's what I'm asking.

Mr. Cohen: Right. The statement reads for itself.

Mr. Ratcliffe: You just submitted that for informational purposes.

Mr. Cohen: That's correct.

Mr. Ratcliffe: Okay. All right. So the next item, a copy of an article with Mr. Trump's handwriting on it that reported on the auction of a portrait of himself, that he arranged a bidder ahead of time and then reimbursed the bidder from the account for his nonprofit charitable foundation, with the picture now hanging in one of his country clubs. Did you submit that because you believe it's in evidence of some crime by Mr. Trump? And if so, what crime would that be related to?

Mr. Cohen: Well, I did it, again, for informational purposes. Plus, could be issues regarding the foundation, improper usage of the foundation.

Mr. Ratcliffe: Okay. And, finally, the last item that you submitted were copies of letters that you wrote at Mr. Trump's direction that threatened his high school, colleges, and the College Board not to release his grades or SAT scores. Again, was that submitted because you believe it's

116th Cong. 10 (Feb. 28, 2019) ("MR. QUIGLEY: Who else might corroborate the allegations you've made this week? MR. COHEN: Well, the conversations, unfortunately, between Jay Sekulow and I were just the two of us.").

The Honorable Elijah E. Cummings
June 7, 2019
Page 6

evidence of some crime, or was it just for informational purposes?

Mr. Cohen: Informational.

Although Cohen admitted the documents he provided to the Committee were not evidence of a crime—but instead just meant to be “informational”—you still used them as the basis for your unprecedented and unilateral subpoena to Mazars USA LLP (Mazars) for President Trump’s sensitive, personal financial documents. In a memorandum justifying your subpoena to Mazars, you boldly alleged that “the President may have engaged in illegal conduct before and during his tenure in office”¹⁹—although Cohen very clearly said that the information he provided the Committee was not evidence of a crime.

Cohen’s HPSCI testimony shows that Cohen coordinated with Oversight Committee Democrats on his testimony

Finally, we learned through the release of these HPSCI transcripts that Cohen engaged in extensive and exclusive strategy sessions with Oversight Committee Democrats before his testimony to our Committee to preemptively address Cohen’s credibility problems.²⁰ This information just reinforces our longstanding concerns that Cohen’s testimony was not legitimate oversight but merely an episode of political theater proposed and produced by a prominent Democrat operative.

It is disappointing you shut out minority participation from your pre-hearing meetings with Cohen. This exclusion is especially disappointing in light of our letter, dated January 11, 2019, in which we urged you to conduct a bipartisan transcribed interview with Cohen before the hearing.²¹ Instead of choosing to hold a bipartisan interview with Cohen, you chose to meet alone with him to discuss how Republicans could question Cohen’s credibility. These actions are not indicative of the serious, fact-based oversight that you promised.

* * *

Your entire course of conduct with respect to Michael Cohen has been deeply troubling. You allowed a prominent Democrat operative to use the Committee for an orchestrated partisan attack on the President. You declined to follow up on your promises to hold Cohen accountable for his lies to the Committee. You declined to hold a Committee vote on Cohen’s lies. You deferred action on Cohen’s lies until you reviewed his HPSCI testimony, but you never requested access to HPSCI’s transcripts. You admitted to considering writing a letter of

¹⁹ Memorandum from Elijah E. Cummings to Members of the H. Comm. on Oversight & Reform, *Notice of Intent to Issue Subpoena to Mazars USA LLP* (April 12, 2019).

²⁰ See *Deposition of Michael Cohen, Executive Session before the Perm. Select Comm. on Intel.*, 116th Cong. 78 (March 6, 2019).

²¹ Letter from Jim Jordan & Mark Meadows, H. Comm. on Oversight & Reform, to Elijah E. Cummings, Chairman, H. Comm. on Oversight & Reform (Jan. 11, 2019).

The Honorable Elijah E. Cummings

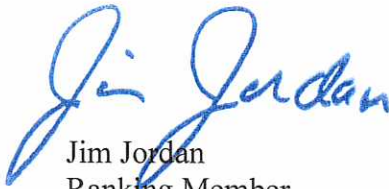
June 7, 2019

Page 7

commendation on behalf of Cohen to reduce his prison sentence.²² You admitted to speaking on the phone with Cohen before he began his prison sentence, but you have not informed the Committee about the substance of your phone call.²³

You may consider this matter “closed” because you want it to go away. But respectfully, you invited Michael Cohen before the Committee and you must live with the consequences. We warned you about the dangers of showcasing the testimony of a convicted liar. The stain of Cohen’s testimony will continue to tarnish the Committee’s reputation and that of your chairmanship until you accept the overwhelming evidence that he lied and act to hold him accountable.

Sincerely,



Jim Jordan
Ranking Member



Mark Meadows
Ranking Member
Subcommittee on Government Operations

²² Manu Raju (@mkraju), Twitter, (April 9, 2019, 11:58 AM)
<https://twitter.com/mkraju/status/1115690562303094784?s=11>.

²³ Manu Raju (@mkraju), Twitter, (May 7, 2019, 4:03 PM),
<https://twitter.com/mkraju/status/1125899040288329731>.

Congress of the United States
Washington, DC 20515

March 20, 2023

Mr. Alvin L. Bragg, Jr.
District Attorney
New York County
One Hogan Place
New York, NY 10013

Dear Mr. Bragg:

You are reportedly about to engage in an unprecedented abuse of prosecutorial authority: the indictment of a former President of the United States and current declared candidate for that office. This indictment comes after years of your office searching for a basis—any basis—on which to bring charges, ultimately settling on a novel legal theory untested anywhere in the country and one that federal authorities declined to pursue. If these reports are accurate, your actions will erode confidence in the evenhanded application of justice and unalterably interfere in the course of the 2024 presidential election. In light of the serious consequences of your actions, we expect that you will testify about what plainly appears to be a politically motivated prosecutorial decision.

The New York County District Attorney's Office has been investigating President Trump since at least 2018, looking for some legal theory on which to bring charges.¹ The facts surrounding the impending indictment have “been known for years.”² Michael Cohen, President Trump's disgraced former lawyer, pleaded guilty over four years ago to charges based on the same facts at issue in the impending indictment.³ By July 2019, however, federal prosecutors determined that no additional people would be charged alongside Cohen.⁴ Now, in the words of one legal scholar, you are attempting to “shoehorn[]” the same case with identical facts into a new prosecution, resurrecting a so-called “zombie” case against President Trump.⁵ Even the *Washington Post* quoted “legal experts” as calling your actions “unusual” because “prosecutors have repeatedly examined the long-established details but decided not to pursue charges.”⁶

¹ Andrew Feinberg, *New York prosecutors warn Trump of possible indictment, report says*, THE INDEPENDENT (Mar. 10, 2023).

² Mark Berman et al., *The prosecutor, the ex-president and the ‘zombie’ case that came back to life*, WASH. POST (Mar. 17, 2023).

³ Shawna Chen, *Timeline: The probe into Trump's alleged hush money payments to Stormy Daniels*, AXIOS (Mar. 18, 2023).

⁴ *Id.*; see Barrett et al., *supra* note 2.

⁵ Jonathan Turley, *Get ready for Manhattan DA's made-for-TV Trump prosecution: high on ratings, but short on the law*, THE HILL (Mar. 18, 2023); Berman et al., *supra* note 2.

⁶ Berman et al., *supra* note 2.

Mr. Alvin L. Bragg, Jr.
March 20, 2023
Page 2

The legal theory underlying your reported prosecution appears to be tenuous and untested.⁷ Bringing charges for falsifying business records is ordinarily a misdemeanor subject to a two-year statute of limitations,⁸ which would have expired long ago. State law, however, allows a district attorney to “elevate nominal misdemeanor conduct” to a felony charge if the “intent to defraud includes an intent to commit another crime or to aid or conceal the commission thereof.”⁹ Such a showing would extend the statute of limitations to five years¹⁰—which would likely expire soon and thus explains your rush to indictment. The only potential speculated crime that could be alleged here would be a violation of campaign finance law, according to one scholar, a charge that the Justice Department has already declined to bring.¹¹

In addition to the novel and untested legal theory, your star witness for this prosecution has a serious credibility problem—a problem that you have reportedly recognized.¹² This case relies heavily on the testimony of Michael Cohen, a convicted perjurer with a demonstrable prejudice against President Trump.¹³ Cohen pleaded guilty to lying to Congress in 2018.¹⁴ In 2019, when he testified before Democrats on the House Oversight Committee to aid their fruitless investigation into President Trump, Cohen lied again—six times.¹⁵ Cohen has been vocal about his deeply personal animus toward President Trump.¹⁶ Under these circumstances, there is no scenario in which Cohen could fairly be considered an unbiased and credible witness.

The inference from the totality of these facts is that your impending indictment is motivated by political calculations. In January 2022, soon after you took office, you expressed doubts about President Trump’s case and suspended the investigation.¹⁷ This decision caused two of your top investigators, Carey Dunne and Mark Pomerantz, to resign in protest and publicly denounce your work.¹⁸ Pomerantz, in particular, heavily criticized you for declining to bring charges at that time,¹⁹ and “Dunne and others” are now “weighing ways” to bar President Trump from holding future office.²⁰ Pomerantz has published a book in the past month

⁷ Turley, *supra* note 5.

⁸ *Id.*

⁹ N.Y. Penal Law § 175.10.

¹⁰ Turley, *supra* note 5; Jeremy Saland, *First Degree Falsifying Business Records: NY Penal Law 175.10*, SALAND LAW PC (page last visited Mar. 19, 2023).

¹¹ *Id.*

¹² Berman et al., *supra* note 2.

¹³ Christopher Lopez, *Progressive DA Alvin Bragg’s case against Trump hinges on witnesses with ‘credibility problems’*: *Andy McCarthy*, FOX NEWS (Mar. 19, 2023); Marisa Schultz, *Jim Jordan, Mark Meadows ask Justice Department to probe Cohen for perjury*, N.Y. POST (Feb. 28, 2019).

¹⁴ *Michael Cohen pleads guilty to lying to Congress*, ASSOC. PRESS (Nov. 29, 2018).

¹⁵ Letter from Jim Jordan & Mark Meadows, H. Comm. on Oversight & Reform, to William P. Barr, Att’y Gen., Dep’t of Justice (Feb. 28, 2019).

¹⁶ See, e.g., Nicholas Fandos & Maggie Haberman, *In Congressional Testimony, Cohen Plans to Call Trump a ‘Con Man’ and a ‘Cheat’*, N.Y. TIMES (Feb. 26, 2019).

¹⁷ Shayna Jacobs et al., *Prosecutor who resigned over stalled Trump probe says ex-president committed felonies*, WASH. POST (Mar. 23, 2022).

¹⁸ *Id.*

¹⁹ *Read the Full Text of Mark Pomerantz’s Resignation Letter*, N.Y. TIMES (Mar. 23, 2022).

²⁰ Shayna Jacobs, *Lawyers who investigated Trump form group to oppose anti-democratic policies*, WASH. POST (Jan. 11, 2023).

Mr. Alvin L. Bragg, Jr.
March 20, 2023
Page 3

excoriating you for not aggressively prosecuting President Trump.²¹ The *Washington Post* reported that you were “deeply stung” by this criticism.²²

The facts of this matter have not changed since 2018 and no new witnesses have emerged.²³ The Justice Department examined the facts in 2019 and opted not to pursue further prosecutions at that time. Even still, according to reporting, the investigation “gained some momentum this year,” and your office “convened a new grand jury in January to evaluate the issue.”²⁴ The only intervening factor, it appears, was President Trump’s announcement that he would be a candidate for President in 2024.²⁵

Your decision to pursue such a politically motivated prosecution—while adopting progressive criminal justice policies that allow career “criminals [to] run [] the streets” of Manhattan²⁶—requires congressional scrutiny about how public safety funds appropriated by Congress are implemented by local law-enforcement agencies. In addition, your apparent decision to pursue criminal charges where federal authorities declined to do so requires oversight to inform potential legislative reforms about the delineation of prosecutorial authority between federal and local officials. Finally, because the circumstances of this matter stem, in part, from Special Counsel Mueller’s investigation,²⁷ Congress may consider legislative reforms to the authorities of special counsels and their relationships with other prosecuting entities. Accordingly, to advance our oversight, please produce the following documents and information for the period January 1, 2017, to the present:

1. All documents and communications between or among the New York County District Attorney’s Office and the U.S. Department of Justice, its component entities, or other federal law enforcement agencies referring or relating to your office’s investigation of President Donald Trump;
2. All documents and communications sent or received by former employees Carey Dunne and Mark Pomerantz referring or relating to President Donald Trump; and
3. All documents and communications referring or relating to the New York County District Attorney Office’s receipt and use of federal funds.

In addition, your testimony is necessary to advance our oversight and to inform potential legislative reforms. We therefore ask that you testify in a transcribed interview about these

²¹ MARK POMERANTZ, *PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT* (2023).

²² Berman et al., *supra* note 2.

²³ *Id.*

²⁴ *Id.*

²⁵ Max Greenwood, *Trump announces 2024 run for president*, THE HILL (Nov. 15, 2022).

²⁶ Alyssa Guzman, *Priorities, eh? Woke DA Alvin Bragg who’s set to indict Trump is one of America’s most controversial prosecutors after charging self-defense shopkeeper with murder and sending soft-on-crime memo*, DAILY MAIL (Mar. 18, 2023); Andrea Cavallier, *REVEALED: Woke Manhattan DA Alvin Bragg has downgraded over HALF of felony cases to misdemeanors as criminals are free to roam streets of the Big Apple*, DAILY MAIL (Nov. 27, 2022).

²⁷ Ben Protess et al., *How Michael Cohen turned against President Trump*, N.Y. Times (Apr. 21, 2019).

Mr. Alvin L. Bragg, Jr.

March 20, 2023

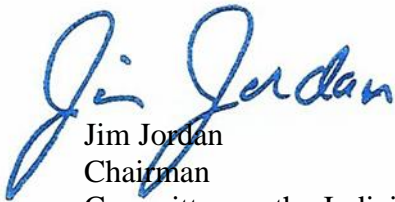
Page 4

matters as soon as possible. Please provide this information and contact Committee staff to schedule your transcribed interview as soon as possible but not later than 10:00 a.m. on March 23, 2023.

Pursuant to Rule X of the Rules of the House of Representatives, the Committee on the Judiciary has jurisdiction over criminal justice matters in the United States. The Committee on House Administration has jurisdiction over matters concerning federal elections. The Committee on Oversight and Accountability may examine “any matter” at any time.

If you have any questions about this request, please contact Committee staff at (202) 225-6906. Thank you for your prompt attention to this matter.

Sincerely,



Jim Jordan
Chairman
Committee on the Judiciary



Bryan Steil
Chairman
Committee on House Administration



James Comer
Chairman
Committee on Oversight and Accountability

cc: The Honorable Jerrold Nadler, Ranking Member
Committee on the Judiciary

The Honorable Joseph Morelle, Ranking Member
Committee on House Administration

The Honorable Jamie Raskin, Ranking Member
Committee on Oversight and Accountability

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-6906
judiciary.house.gov

March 22, 2023

Mr. Carey R. Dunne
Former Manhattan Special Assistant District Attorney
The Law Office of Carey R. Dunne, PLLC
114 E. 95th St.
New York, NY 10128

Dear Mr. Dunne:

New York County District Attorney Alvin Bragg is reportedly about to engage in an unprecedented abuse of prosecutorial authority: the indictment of a former President of the United States and current declared candidate for that office. This indictment comes after years of the District Attorney's office aggressively pursuing charges, with you and other special prosecutors leading the investigation into every facet of President Trump's finances.¹ Last year, you resigned from the office over Bragg's initial reluctance to move forward with charges in 2022, Bragg is now attempting to "shoehorn[]" the same case with identical facts into a new prosecution.² Based on your unique role in this matter, we request your cooperation with our oversight of this politically motivated prosecutorial decision.

The New York County District Attorney's Office has been investigating President Trump since at least 2018, looking for some legal theory on which to bring charges.³ The facts surrounding the impending indictment have "been known for years."⁴ Michael Cohen, President Trump's disgraced former lawyer, pleaded guilty over four years ago to charges based on the same facts at issue in the impending indictment.⁵ By July 2019, however, federal prosecutors determined that no additional people would be charged alongside Cohen.⁶

¹ Ben Protess et al., *How the Manhattan DA's investigation into President Donald Trump unraveled*, N.Y. TIMES (March 5, 2022); Shayna Jacobs et al., *Prosecutors in Trump probe quit after new DA seems to abandon plan to seek indictment of former president*, WASH. POST (Feb. 24, 2022).

² Jonathan Turley, *Get ready for Manhattan DA's made-for-TV Trump prosecution: high on ratings, but short on the law*, THE HILL (Mar. 18, 2023); Mark Berman et al., *The prosecutor, the ex-president and the 'zombie' case that came back to life*, WASH. POST (Mar. 17, 2023).

³ Andrew Feinberg, *New York prosecutors warn Trump of possible indictment, report says*, THE INDEPENDENT (Mar. 10, 2023).

⁴ Berman et al., *supra* note 2.

⁵ Shawna Chen, *Timeline: The probe into Trump's alleged hush money payments to Stormy Daniels*, AXIOS (Mar. 18, 2023).

⁶ *Id.*; see Berman et al., *supra* note 2.

Mr. Carey R. Dunne
March 22, 2023
Page 2

In January 2022, soon after Bragg took office, he expressed doubts about President Trump's case and suspended the investigation.⁷ This decision caused you and your colleague, Mark Pomerantz, to resign in protest.⁸ Your unrelenting pursuit of President Trump has followed you into the private sector. Following your resignation from Bragg's office, you and Pomerantz started a law firm dedicated to "weighing ways" to bar President Trump from holding future office.⁹ Just this month, Pomerantz published a book excoriating Bragg for not aggressively prosecuting President Trump.¹⁰ The *Washington Post* reported that Bragg was "deeply stung" by criticism from you and Pomerantz.¹¹

It now appears that your efforts to shame Bragg have worked as he is reportedly resurrecting a so-called "zombie" case against President Trump using a tenuous and untested legal theory.¹² Even the *Washington Post* quoted "legal experts" as calling Bragg's actions "unusual" because "prosecutors have repeatedly examined the long-established details but decided not to pursue charges."¹³ In addition, Bragg's star witness—Michael Cohen—has a serious credibility problem as a convicted perjurer and serial fabricator with demonstrable prejudice against President Trump.¹⁴ Under these circumstances, there is no scenario in which Cohen could fairly be considered an unbiased and credible witness.

The inference from the totality of these facts is that Bragg's impending indictment is motivated by political calculations. The facts of this matter have not changed since 2018 and no new witnesses have emerged.¹⁵ The Justice Department examined the facts in 2019 and opted not to pursue further prosecutions at that time. Even still, according to reporting, the investigation "gained some momentum this year," and Bragg's office "convened a new grand jury in January to evaluate the issue."¹⁶ The only intervening factor, it appears, was President Trump's announcement that he would be a candidate for President in 2024.¹⁷

Your actions, both as a special prosecutor and since leaving the District Attorney's office, cast serious doubt on administration of fair and impartial justice in this matter. In light of this unprecedented and overzealous investigation, Congress has a keen interest in understanding the relevant facts to inform potential legislation to improve the functioning and fairness of our criminal justice system and to better delineate prosecutorial authority between federal and local

⁷ Shayna Jacobs et al., *Prosecutor who resigned over stalled Trump probe says ex-president committed felonies*, WASH. POST (Mar. 23, 2022).

⁸ *Id.*

⁹ Shayna Jacobs, *Lawyers who investigated Trump form group to oppose anti-democratic policies*, WASH. POST (Jan. 11, 2023).

¹⁰ MARK POMERANTZ, *PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT* (2023).

¹¹ Berman et al., *supra* note 2.

¹² Turley, *supra* note 5.

¹³ Berman et al., *supra* note 2.

¹⁴ Christopher Lopez, *Progressive DA Alvin Bragg's case against Trump hinges on witnesses with 'credibility problems': Andy McCarthy*, FOX NEWS (Mar. 19, 2023); Marisa Schultz, *Jim Jordan, Mark Meadows ask Justice Department to probe Cohen for perjury*, N.Y. POST (Feb. 28, 2019); *Michael Cohen pleads guilty to lying to Congress*, ASSOC. PRESS (Nov. 29, 2018).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ Max Greenwood, *Trump announces 2024 run for president*, THE HILL (Nov. 15, 2022).

Mr. Carey R. Dunne
March 22, 2023
Page 3

officials. In addition, because the circumstances of this matter stem, in part, from Special Counsel Mueller's investigation,¹⁸ Congress may consider legislative reforms to the authorities of special counsels and their relationships with other prosecuting entities. Accordingly, to advance our oversight, please produce the following documents and information in your personal possession for the period January 1, 2017, to the present:

1. All documents and communications between or among the New York County District Attorney's Office and the U.S. Department of Justice, its component entities, or other federal law enforcement agencies referring or relating to New York County District Attorney's investigation of President Donald Trump;
2. All documents and communications between or among you and the New York County District Attorney's Office referring or relating to President Donald Trump; and
3. All documents and communications between or among you and representatives of the New York County District Attorney's Office referring or relating to your appointment and role as a Special Assistant District Attorney for New York County.

In addition, your testimony is necessary to advance our oversight and to inform potential legislative reforms. We therefore ask that you testify in a transcribed interview about these matters as soon as possible. Please provide this information and contact Committee staff to schedule your transcribed interview as soon as possible but not later than 10:00 a.m. on March 27, 2023.

Further, this letter serves as a formal request to preserve all existing and future records and materials relating to the topics addressed in this letter. You should construe this preservation notice as an instruction to take all reasonable steps to prevent the destruction or alteration, whether intentionally or negligently, of all documents, communications, and other information, including electronic information and metadata, that are or may be responsive to this congressional inquiry. This instruction includes all electronic messages sent using your official and personal accounts or devices, including records created using text messages, phone-based message applications, or encryption software.

The Committee on the Judiciary has jurisdiction over criminal justice matters in the United States and matters involving threats to civil liberties pursuant to Rule X of the Rules of the House of Representatives.¹⁹ If you have any questions about this request, please contact Committee staff at (202) 225-6906. Thank you for your prompt attention to this matter.

Sincerely,



Jim Jordan
Chairman

¹⁸ Ben Protess et al., *How Michael Cohen turned against President Trump*, N.Y. TIMES (Apr. 21, 2019).

¹⁹ Rules of the U.S. House of Representatives, R. X (2023).

Mr. Carey R. Dunne

March 22, 2023

Page 4

cc: The Honorable Jerrold Nadler, Ranking Member

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-6906
judiciary.house.gov

March 22, 2023

Mr. Mark F. Pomerantz
Former New York County Special Assistant District Attorney
Free & Fair Litigation Group
128 E. Broadway, Unit 793
New York, NY 10002

Dear Mr. Pomerantz:

New York County District Attorney Alvin Bragg is reportedly about to engage in an unprecedented abuse of prosecutorial authority: the indictment of a former President of the United States and current declared candidate for that office. This indictment comes after years of the District Attorney's office aggressively pursuing charges, including by appointing you as an unpaid "special assistant district attorney" to lead the investigation into every facet of President Trump's finances.¹ Last year, you resigned from the office over Bragg's initial reluctance to move forward with charges, shaming Bragg in your resignation letter—which was subsequently leaked—into bringing charges.² Based on your unique role in this matter, and your subsequent public statements prejudicing the impartiality of any prosecution, we request your cooperation with our oversight of this politically motivated prosecutorial decision.

The New York County District Attorney's Office has been investigating President Trump since at least 2018, looking for some legal theory on which to bring charges.³ The facts surrounding the impending indictment have "been known for years."⁴ Michael Cohen, President Trump's disgraced former lawyer, pleaded guilty over four years ago to charges based on the

¹ William K. Rashbaum et al., *A former federal prosecutor has joined the Manhattan D.A.'s team investigating the Trump family business*, N.Y. TIMES (Feb. 19, 2021); Ben Protess et al., *How the Manhattan DA's investigation into President Donald Trump unraveled*, N.Y. TIMES (March 5, 2022).

² *Read the Full Text of Mark Pomerantz's Resignation Letter*, N.Y. TIMES (Mar. 23, 2022) [hereinafter "Pomerantz Letter"].

³ Andrew Feinberg, *New York prosecutors warn Trump of possible indictment, report says*, THE INDEPENDENT (Mar. 10, 2023).

⁴ Mark Berman et al., *The prosecutor, the ex-president and the 'zombie' case that came back to life*, WASH. POST (Mar. 17, 2023).

Mr. Mark F. Pomerantz

March 22, 2023

Page 2

same facts at issue in the impending indictment.⁵ By July 2019, however, federal prosecutors determined that no additional people would be charged alongside Cohen.⁶

In January 2022, soon after Bragg took office, he expressed doubts about President Trump's case and suspended the investigation.⁷ This decision caused you and your colleague, Carey Dunne, to resign in protest.⁸ You penned a scathing resignation letter in which you baselessly accused President Trump of "numerous felony violations," and asserted it would be "a grave failure of justice" if Bragg did not pursue charges.⁹ You urged Bragg to hold President Trump "fully accountable for his crimes," asserting that Bragg's decision "will doom any future prospects" for prosecution.¹⁰ Your resignation letter found its way into the *New York Times*, word-for-word, and your criticisms of Bragg's investigation were widely reported by news outlets.¹¹ Your unrelenting pursuit of President Trump followed you into the private sector as you and Dunne started a law firm dedicated to "weighing ways" to bar President Trump from holding future office.¹² Just this month, you published a book excoriating Bragg for not aggressively prosecuting President Trump, laying bare the office's internal deliberations about the investigation and your personal animus toward President Trump.¹³

It now appears that your efforts to shame Bragg have worked as he is reportedly resurrecting a so-called "zombie" case against President Trump using a tenuous and untested legal theory.¹⁴ Even the *Washington Post* quoted "legal experts" as calling Bragg's actions "unusual" because "prosecutors have repeatedly examined the long-established details but decided not to pursue charges."¹⁵ In addition, Bragg's star witness—Michael Cohen—has a serious credibility problem as a convicted perjurer and serial fabricator with demonstrable prejudice against President Trump.¹⁶ Under these circumstances, there is no scenario in which Cohen could fairly be considered an unbiased and credible witness.

The inference from the totality of these facts is that Bragg's impending indictment is motivated by political calculations. The facts of this matter have not changed since 2018 and no new witnesses have emerged.¹⁷ The Justice Department examined the facts in 2019 and opted not

⁵ Shawna Chen, *Timeline: The probe into Trump's alleged hush money payments to Stormy Daniels*, AXIOS (Mar. 18, 2023).

⁶ *Id.*; see Berman et al., *supra* note 4.

⁷ Shayna Jacobs et al., *Prosecutor who resigned over stalled Trump probe says ex-president committed felonies*, WASH. POST (Mar. 23, 2022).

⁸ *Id.*

⁹ Pomerantz Letter, *supra* note 2.

¹⁰ *Id.*

¹¹ *Id.*

¹² Shayna Jacobs, *Lawyers who investigated Trump form group to oppose anti-democratic policies*, WASH. POST (Jan. 11, 2023).

¹³ MARK POMERANTZ, *PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT* (2023).

¹⁴ Berman et al., *supra* note 4.

¹⁵ *Id.*

¹⁶ Christopher Lopez, *Progressive DA Alvin Bragg's case against Trump hinges on witnesses with 'credibility problems': Andy McCarthy*, FOX NEWS (Mar. 19, 2023); Marisa Schultz, *Jim Jordan, Mark Meadows ask Justice Department to probe Cohen for perjury*, N.Y. POST (Feb. 28, 2019); *Michael Cohen pleads guilty to lying to Congress*, ASSOC. PRESS (Nov. 29, 2018).

¹⁷ Berman et al., *supra* note 4.

Mr. Mark F. Pomerantz
March 22, 2023
Page 3

to pursue further prosecutions at that time. Even still, according to reporting, the investigation “gained some momentum this year,” and Bragg’s office “convened a new grand jury in January to evaluate the issue.”¹⁸ The only intervening factor, it appears, was President Trump’s announcement that he would be a candidate for President in 2024.¹⁹

Your actions, both as a special prosecutor and since leaving the District Attorney’s office, cast serious doubt on the administration of fair and impartial justice in this matter. Your words in the *New York Times* have unfairly disparaged President Trump, an innocent and uncharged man, as a felon to millions of *Times* readers. Your book again unfairly disparaged President Trump, and now opens the door to examination about the District Attorney’s office commitment to evenhanded justice. In light of this unprecedented and overzealous partisan investigation, Congress has a keen interest in these facts to inform potential legislation to improve the functioning and fairness of our criminal justice system, and to better delineate prosecutorial authority between federal and local officials. In addition, because the circumstances of this matter stem, in part, from Special Counsel Mueller’s investigation,²⁰ Congress may consider legislative reforms to the authorities of special counsels and their relationships with other prosecuting entities.

Accordingly, to advance our oversight, please produce the following documents and information in your personal possession for the period January 1, 2017, to the present:

1. All documents and communications between or among the New York County District Attorney’s Office and the U.S. Department of Justice, its component entities, or other federal law enforcement agencies referring or relating to New York County District Attorney’s investigation of President Donald Trump;
2. All documents and communications between or among you and representatives of the New York County District Attorney’s Office referring or relating to President Donald Trump; and
3. All documents and communications between or among you and representatives of the New York County District Attorney’s Office referring or relating to your appointment and role as a Special Assistant District Attorney for New York County.

In addition, your testimony is necessary to advance our oversight and to inform potential legislative reforms. We therefore ask that you testify in a transcribed interview about these matters as soon as possible. Please provide this information and contact Committee staff to schedule your transcribed interview as soon as possible but not later than 10:00 a.m. on March 27, 2023.

Further, this letter serves as a formal request to preserve all existing and future records and materials relating to the topics addressed in this letter. You should construe this preservation

¹⁸ *Id.*

¹⁹ Max Greenwood, *Trump announces 2024 run for president*, THE HILL (Nov. 15, 2022).

²⁰ Ben Protess et al., *How Michael Cohen turned against President Trump*, N.Y. TIMES (Apr. 21, 2019).

Mr. Mark F. Pomerantz

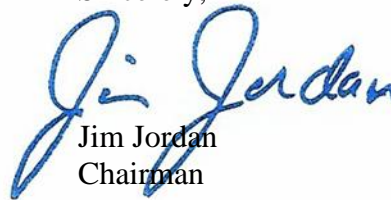
March 22, 2023

Page 4

notice as an instruction to take all reasonable steps to prevent the destruction or alteration, whether intentionally or negligently, of all documents, communications, and other information, including electronic information and metadata, that are or may be responsive to this congressional inquiry. This instruction includes all electronic messages sent using your official and personal accounts or devices, including records created using text messages, phone-based message applications, or encryption software.

The Committee on the Judiciary has jurisdiction over criminal justice matters in the United States and matters involving threats to civil liberties pursuant to Rule X of the Rules of the House of Representatives.²¹ If you have any questions about this request, please contact Committee staff at (202) 225-6906. Thank you for your prompt attention to this matter.

Sincerely,

A handwritten signature in blue ink that reads "Jim Jordan". The signature is written in a cursive, flowing style.

Jim Jordan
Chairman

cc: The Honorable Jerrold Nadler, Ranking Member

²¹ Rules of the U.S. House of Representatives, R. X (2023).



ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

LESLIE B. DUBECK
GENERAL COUNSEL

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000

Final Report 3937

March 23, 2023

By email

The Honorable Jim Jordan
Chairman, House Committee on the Judiciary

The Honorable Bryan Steil
Chairman, House Committee on House Administration

The Honorable James Comer
Chairman, House Committee on Oversight and Accountability

Dear Chairman Jordan, Chairman Steil, and Chairman Comer:

The District Attorney of New York County is investigating allegations that Donald Trump engaged in violations of New York State penal law. The investigation is one of thousands conducted by the Office of the District Attorney in its long history of pursuing justice and protecting New Yorkers. The investigation has been conducted consistently with the District Attorney's oath to faithfully execute the laws of the State of New York. The District Attorney pledged that the DA's Office would "publicly state the conclusion of our investigation—whether we conclude our work without bringing charges, or move forward with an indictment."¹ He stands by that pledge. And if charges are brought at the conclusion, it will be because the rule of law and faithful execution of the District Attorney's duty require it.

Your letter dated March 20, 2023 (the "Letter"), in contrast, is an unprecedented inquiry into a pending local prosecution. The Letter only came after Donald Trump created a false expectation that he would be arrested the next day² and his lawyers reportedly urged you to intervene.³ Neither fact is a legitimate basis for congressional inquiry.

¹ Statement by Manhattan District Attorney Alvin Bragg on Ongoing Investigation Concerning the Trump Organization (April 7, 2022), available at: <https://www.manhattanda.org/statement-by-manhattan-district-attorney-alvin-bragg-on-ongoing-investigation-concerning-the-trump-organization/>.

² *Trump says 'illegal leaks' indicate he'll be arrested Tuesday*, FoxNews, March 18, 2023, available at: <https://www.foxnews.com/politics/trump-says-illegal-leaks-indicate-arrested-tuesday>.

³ Shane Goldmacher, et al., *For the G.O.P., a Looming Trump Indictment Takes Center Stage*, N.Y. Times (March 20, 2023) (quoting a letter from Joseph Tacopina, a lawyer for Donald Trump, to Chairman Jordan, encouraging Congress to investigate the District Attorney).

In New York, the District Attorney is a constitutional officer charged with “the responsibility to conduct all prosecutions for crimes and offenses cognizable by the courts of the county in which he serves.” *People v Di Falco*, 44 N.Y.2d 482, 486 (1978); see also *Matter of Haggerty v. Himelein*, 89 N.Y.2d 431, 436 (1997); *Matter of Schumer v. Holtzman*, 60 N.Y.2d 46, 52 (1983). These are quintessential police powers belonging to the State, and your letter treads into territory very clearly reserved to the states. It suggests that Congress’s investigation is being “conducted solely for the personal aggrandizement of the investigators or to ‘punish’ those investigated,” and is, therefore, “indefensible.” *Watkins v. United States*, 354 U.S. 178, 187 (1957).

As articulated below, the District Attorney is obliged by the federal and state constitutions to protect the independence of state law enforcement functions from federal interference. The DA’s Office therefore requests an opportunity to meet and confer with committee staff to better understand what information the DA’s Office can provide that relates to a legitimate legislative interest and can be shared consistent with the District Attorney’s constitutional obligations.

Compliance with the Letter Would Interfere with Law Enforcement

The Letter seeks non-public information about a pending criminal investigation, which is confidential under state law. CPL § 190.25(4)(a) (“Grand jury proceedings are secret”); Penal Law § 215.70 (prosecutor’s disclosure of grand jury evidence is a felony unless “in the proper discharge of his official duties or upon written order of the court”); *Sanchez v. City of New York*, 201 A.D.2d 325, 326 (1st Dept. 1994) (witness statements to the District Attorney’s Office protected by the public interest privilege); Public Officers Law § 87(2)(e) (shielding materials “compiled for law enforcement purposes” from public disclosure where disclosure would “interfere with law enforcement investigations” or “disclose confidential information relating to a criminal investigation”).⁴

These confidentiality provisions exist to protect the interests of the various participants in the criminal process—the defendant, the witnesses, and members of the grand jury—as well as the integrity of the grand jury proceeding itself. Like the Department of Justice, as a prosecutor exercising sovereign executive powers, the District Attorney has a constitutional obligation to “protect the government’s ability to prosecute fully and fairly,” to “independently and impartially uphold the rule of law,” to “protect witnesses and law enforcement,” to “avoid flight by those implicated in our investigations,” and to “prevent additional crimes.”⁵

⁴ That the investigation relates to a former President does not change this analysis. Even Donald Trump has conceded that he is not immune from local criminal prosecution. See *Trump v. Vance*, 591 U.S. ___, 140 S. Ct. 2412, 2426-27 (2020) (noting that the President “concedes—consistent with the position of the Department of Justice—that state grand juries are free to investigate a sitting President with an eye toward charging him after the completion of his term”).

⁵ Letter from Assistant Attorney General Carlos Uriarte to Chairman Jordan, dated January 20, 2023, at page 3-4. (Available at <https://www.politico.com/f/?id=00000185-d087-dde8-a9af-d4afeba70000>).

Consistent with these constitutional obligations, the DA's Office is cognizant of DOJ's "[l]ongstanding" policy of not providing Congress with non-public information about investigations.⁶

With regard to pending federal investigations, "Congress seems generally to have been respectful of the need to protect material contained in open criminal investigative files. There is almost no precedent for Congress attempting to subpoena such material, and even fewer examples of the DOJ actually producing such documents."⁷

Requests Regarding the Exercise of State Police Powers Violate New York's Sovereignty

The Letter's requests are an unlawful incursion into New York's sovereignty. Congress's investigative jurisdiction is derived from and limited by its power to legislate concerning federal matters. *See, e.g., Eastland v. U. S. Servicemen's Fund*, 421 U.S. 491, 503-05 (1975); *Barenblatt v. United States*, 360 U.S. 109, 111-12 (1959); *Kilbourn v. Thompson*, 103 U.S. 168, 195-96 (1880).

The Constitution limits Congress's powers to those specifically enumerated; and the Tenth Amendment ensures that any unenumerated powers are reserved to the States. *New York v. United States*, 505 U.S. 144, 155-56 (1992). It is therefore generally understood that a Congressional committee may not "inquire into matters which are . . . reserved to the States." Charles W. Johnson, *et al.*, *House Practice: A Guide to the Rules, Precedents, and Procedures of the House* at 254 (GPO 2017)⁸; *see also Watkins*, 354 U.S. at 187 ("The power of the Congress to conduct investigations . . . comprehends probes into departments of the *Federal Government* . . .") (emphasis added).⁹

Among the powers reserved to the states, "[p]erhaps the clearest example of traditional state authority is the punishment of local criminal activity." *Bond v. United States*, 572 U.S. 844, 858 (2014). Thus, federal interference with state law enforcement "is peculiarly inconsistent with our federal framework." *Cameron v. Johnson*, 390 U.S. 611, 618 (1968); *see also Printz v. United*

⁶ *Id.* at 3.

⁷ Todd David Peterson, *Congressional Oversight of Open Criminal Investigations*, 77 *Notre Dame L. Rev.* 1373, 1410 (2002); *see also* Alissa M. Dolan & Todd Garvey, *CRS Report for Congress: Congressional Investigations of the Department of Justice, 1920-2012: History, Law, and Practice*, 2 (Nov. 5, 2012) (available at <https://sgp.fas.org/crs/misc/R42811.pdf>) ("Department [of Justice] rarely releases—and committees rarely subpoena—material relevant to open criminal investigations.").

⁸ Available at <https://www.govinfo.gov/content/pkg/GPO-HPRACTICE-115/pdf/GPO-HPRACTICE-115.pdf>.

⁹ Consistent with this general understanding, this type of inquiry appears to be unprecedented. The only precedent is one aimed at an ongoing state *civil* investigation that was never enforced. *See* Lemos, et al. Letter to House Committee on Science & Technology (Sept. 13, 2016) (scholarly review of subpoenas from the House Committee on Science & Technology to state Attorneys General regarding pending *civil* investigations, and stating: "To our knowledge, Congress has *never* before attempted to use its investigatory authority to interfere with an ongoing state investigation."), available at page 814 of <https://docs.house.gov/meetings/SY/SY00/20160914/105259/HHRG-114-SY00-20160914-SD004.pdf>.

States, 521 U.S. 898, 931 n.15 (1997) (Tenth Amendment limits federal power over local law enforcement). Invoking these principles of comity, equity, and federalism, the Supreme Court held, in *Younger v. Harris*, that federal courts may not interfere in pending state criminal prosecutions absent extraordinary circumstances. 401 U.S. 37 (1971). This holding reflects a “continuance of the belief that the National Government will fare best if the States and their institutions are left free to perform their separate functions in their separate ways.” *Id.* at 44.

Against this history, it is clear that Congress cannot have any legitimate legislative task relating to the oversight of local prosecutors enforcing state law. To preserve the Constitution’s federalist principles, the District Attorney is duty bound by his constitutional oath to New York’s sovereign interest in the exercise of police powers reserved to the States under the Tenth Amendment.

Congressional Review of a Pending Criminal Investigation Usurps Executive Powers

Congress is not the appropriate branch to review pending criminal matters. As the Supreme Court noted in *Watkins*, “Congress [is not] a law enforcement or trial agency. These are functions of the executive and judicial departments of government.” 354 U.S. at 187. “[T]he power [of Congress] to investigate must not be confused with any of the powers of law enforcement; those powers are assigned under our Constitution to the Executive and the Judiciary.” *Quinn v. United States*, 349 U.S. 155, 161 (1955).

If a grand jury brings charges against Donald Trump, the DA’s Office will have an obligation, as in every case, to provide a significant amount of discovery from its files to the defendant so that he may prepare a defense. The Letter’s allegation that the DA’s Office is pursuing a prosecution for political purposes is unfounded, and regardless, the proper forum for such a challenge is the Courts of New York, which are equipped to consider and review such objections. In addition, review by the U.S. Supreme Court would be available to the extent any criminal case raises federal issues. That is the mechanism afforded to every defendant in a criminal case. Congress has no role to play in that review, especially as to a pending *state* criminal proceeding. *See Younger*, 401 U.S. at 43-45.

Federal Funding is an Insufficient Basis to Justify These Unconstitutional Requests

The Letter indicates that its requests may be related to a review of federal public safety funds. But the Letter does not suggest any way in which either the District Attorney’s testimony about his prosecutorial decisions or the documents and communications of former Assistant District Attorneys on a pending criminal investigation would shed light on that review.

Nonetheless, to assist Congress in understanding the ways in which the DA’s Office has used federal funds, we are preparing and will submit a letter describing its use of federal funds.

* * *

We trust that you appreciate the importance of our federal system, state law enforcement activities, and the critical need to maintain the integrity and independence of state criminal law enforcement from federal interference. While the DA's Office will not allow a Congressional investigation to impede the exercise of New York's sovereign police power, this Office will always treat a fellow government entity with due respect. Therefore, again, we request a meet and confer to understand whether the Committee has any legitimate legislative purpose in the requested materials that could be accommodated without impeding those sovereign interests. We simply expect that our office also be treated "in a manner consistent with [New York's] status as a residuary sovereign[] and joint participant[] in the governance of the Nation." *Alden v. Maine*, 527 U.S. 706, 748 (1999) (Kennedy, J.).

Respectfully Submitted,



Leslie B. Dubeck
General Counsel

cc: Honorable Jerrold Nadler, Ranking Member, Committee on the Judiciary
Honorable Joseph Morelle, Ranking Member, Committee on House Administration
Honorable Jamie Raskin, Ranking Member, Committee on Oversight and Accountability
Majority Staff, Committee on the Judiciary
Minority Staff, Committee on the Judiciary

Congress of the United States
Washington, DC 20515

March 25, 2023

Mr. Alvin L. Bragg, Jr.
District Attorney
New York County
One Hogan Place
New York, NY 10013

Dear Mr. Bragg:

Our Committees are conducting oversight of your reported effort to indict a former President of the United States and current declared candidate for that office. On March 20, 2023, we wrote to you requesting that you voluntarily cooperate with our oversight by providing relevant documents and testimony.¹ We received a reply letter sent on your behalf dated March 23, 2023, which set forth several purported reasons for why you could not cooperate with our investigation.²

Notably, your reply letter did not dispute the central allegations at issue—that you, under political pressure from left-wing activists and former prosecutors in your office, are reportedly planning to use an alleged federal campaign finance violation, previously declined by federal prosecutors, as a vehicle to extend the statute of limitations on an otherwise misdemeanor offense and indict for the first time in history a former President of the United States. Moreover, you are apparently attempting to *upgrade* a misdemeanor charge to a felony using an untested legal theory at the same time when you are simultaneously downgrading felony charges to misdemeanors in a majority of other cases in your jurisdiction.³

Contrary to the central argument set forth in your letter, this matter does not simply involve *local* or *state* interests. Rather, the potential criminal indictment of a former President of the United States by an elected local prosecutor of the opposing political party (and who will face the prospect of re-election) implicates substantial *federal* interests, particularly in a jurisdiction where trial-level judges also are popularly elected. If state or local prosecutors are able to engage in politically motivated prosecutions of Presidents of the United States (former or current) for personal acts, this could have a profound impact on how Presidents choose to

¹ Letter from Rep. Jim Jordan, H. Comm. on the Judiciary, et al., to Mr. Alvin L. Bragg, Jr., Manhattan District Attorney (Mar. 20, 2023).

² Letter from Leslie B. Dubeck, Gen. Counsel, N.Y. Co. District Att’y Off., to Rep. Jim Jordan, H. Comm. on the Judiciary, et al. (Mar. 23, 2023) [hereinafter “Letter from Dubeck”].

³ See, e.g., Melissa Klein, *NYC Convictions Plummet, Downgraded Charges Surge under Manhattan DA Bragg*, N.Y. Post (Nov. 26, 2022).

Mr. Alvin L. Bragg, Jr.

March 25, 2023

Page 2

exercise their powers while in office. For example, a President could choose to avoid taking action he believes to be in the national interest because it would negatively impact New York City for fear that he would be subject to a retaliatory prosecution in New York City.

Likewise, because the federal government has a compelling interest in protecting the physical safety of former or current Presidents, any decision to prosecute a former or current President raises difficult questions concerning how to vindicate that interest in the context of a state or local criminal justice system. For these reasons and others, we believe that we now must consider whether Congress should take legislative action to protect former and/or current Presidents from politically motivated prosecutions by state and local officials, and if so, how those protections should be structured. Critically, due to your own actions, you are now in possession of information critical to this inquiry.

I. The Arguments in Defense of Your Unprecedented Prosecutorial Conduct Are Conclusory and Unconvincing.

The Supreme Court has recognized that Congress has a “broad and indispensable” power to conduct oversight, which “encompasses inquiries into the administration of existing laws, studies of proposed laws, and surveys in our social, economic or political system for the purpose of enabling Congress to remedy them.”⁴ In *Wilkinson v. United States*, the Supreme Court articulated a three-prong test to determine the legal sufficiency of a congressional subpoena: “(1) the Committee’s investigation of the broad subject matter area must be authorized by Congress; (2) the investigation must be pursuant to ‘a valid legislative purpose’; and (3) the specific inquiries involved must be pertinent to the broad subject matter areas which have been authorized by Congress.”⁵

A. The Committees Are Authorized to Conduct Such an Inquiry.

Contrary to your assertion otherwise, the Committees’ inquiry plainly satisfies this three-prong test. First, the Committee on the Judiciary is charged by the House of Representatives with upholding fundamental American civil liberties and with promoting fairness and consistency in our nation’s criminal justice system. In fact, Rule X of the Rules of the House of Representatives authorizes the Committee on the Judiciary to conduct oversight of criminal justice matters to inform potential legislation.⁶ In the Committees’ view, the circumstances of any prosecutorial decision to indict a former President of the United States on a novel and untested legal theory based on facts known for years and conduct previously uncharged by federal prosecutors, shortly after your former high-ranking employee has publicly criticized you for *not* making such an indictment, require an examination of the facts and potential consequences of this unprecedented decision. The Committee on the Judiciary has an interest in the fair and evenhanded application of justice at both the state and federal level.

⁴ See, e.g., *Trump v. Mazars LLP*, No. 19-715 at 11 (U.S. slip op. July 9, 2020) (internal quotation marks and citations omitted).

⁵ *Wilkinson v. United States*, 365 U.S. 399, 408-09 (1961); see *Ashland Oil, Inc. v. FTC*, 409 F. Supp. 297, 305 (D.D.C. 1976).

⁶ Rules of the U.S. House of Representatives, R. X(1)(5) (2023).

Mr. Alvin L. Bragg, Jr.
March 25, 2023
Page 3

B. The Inquiry Is on a Matter on Which Legislation Could be Had.

Second, the Committees' inquiry has an obvious legitimate legislative purpose and is "a subject on which legislation could be had."⁷ To begin with, as discussed above, Congress has a specific and manifestly important interest in preventing politically motivated prosecutions of current and former Presidents by elected state and local prosecutors, particularly those tried before elected state and local trial-level judges. Therefore, the Committee on the Judiciary, as a part of its broad authority to develop criminal justice legislation, must now consider whether to draft legislation that would, if enacted, insulate current and former presidents from such improper state and local prosecutions. These legislative reforms may include, for example, broadening the existing statutory right of removal of certain criminal cases from state court to federal court. Because your impending indictment of a former President is an issue of first impression, the Committees require information from your office to inform our oversight.

Moreover, as discussed above, your prosecutorial decision to indict a former President may cause a potential confrontation between federal and local law-enforcement authorities. Federal law requires the United States Secret Service to protect a former President.⁸ Therefore, your unprecedented prosecutorial decision raises the potential for conflict between the federal law-enforcement officials required to protect the former President and local law-enforcement officials required to enforce your indictment and exercise control of him throughout his presence in the local criminal justice system. Such a novel and potentially fraught collision of federal and local law-enforcement officials with the safety of a former President at stake is certainly a matter of interest for the Committees. The Committees' oversight is necessary to inform potential legislation that would address or remedy any potential conflicts between federal and local authorities.

In addition, the federal campaign finance charges you are reportedly attempting to use to upgrade a misdemeanor charge to a felony have previously been considered—and rejected—by federal prosecutors.⁹ In light of this fact, to bring uniformity to the law and prevent future attempts by state or local prosecutors to pursue politically motivated prosecutions related to campaign finance regulations applicable to federal elections, Congress may elect to consider legislation that broadens the preemption provision in the Federal Election Campaign Act. This reform could have the effect of better delineating the prosecutorial authorities of federal and local officials in this area and blocking the selective or politicized enforcement by state and local prosecutors of campaign finance restrictions pertaining to federal elections.

Furthermore, your reported decision to indict a former President requires congressional scrutiny about how federal public safety funds appropriated by Congress are implemented by

⁷ See, e.g., *Mazars*, No. 19-715 at 12 (internal quotation marks and citations omitted).

⁸ 18 U.S.C. § 3056.

⁹ Jonathan Turley, "America's Got Trump": *Get Ready for a Truly Made-for-TV Prosecution*, *Res Ipsa Loquitur – The Thing Itself Speaks* (Mar. 20, 2023) ("Although it may be politically popular, the case is legally pathetic. Bragg is struggling to twist state laws to effectively prosecute a federal case long ago rejected by the Justice Department . . .").

Mr. Alvin L. Bragg, Jr.

March 25, 2023

Page 4

local law-enforcement agencies and how limited resources are prioritized. Under your leadership, the New York County District Attorney’s Office has adopted and defended your progressive criminal justice policies, which includes “downgrad[ing] 52 percent of felony cases to misdemeanors.”¹⁰ Even with downgrading more than half of your felony cases to misdemeanors, your office’s conviction rate when prosecuting serious felony charges was reported to be just 51 percent.¹¹ Your conviction rate for misdemeanors also dropped sharply—from 53 percent to 28 percent.¹² Your policies have allowed career “criminals [to] run[] the streets” of Manhattan¹³—creating such a danger that a judge in your district has taken notice.¹⁴

To the extent that you are receiving federal funds and are choosing to prioritize apparent political prosecutions over commonsense public safety measures, the Committee on the Judiciary certainly may consider legislation to tie federal funds to improved public safety metrics. In fact, last year, a Judiciary Subcommittee heard testimony from the mother of an army veteran murdered in your district,¹⁵ who criticized your office’s handling of her son’s murder by offering plea deals to the defendants despite the fact that “the murder and their roles were caught on video”¹⁶ Her testimony crystallized the need for legislation to prevent dangerous criminals from running free. Additionally, if our oversight determines that improper partisan or political considerations are motivating your prosecutorial decisions, the Committee on the Judiciary may consider legislation to place conditions on federal funding for state and local law-enforcement jurisdictions to ensure that funds are not used to engage in discrimination on the basis of partisan affiliation or political beliefs.

Lastly, because the circumstances of this matter stem, in part, from Special Counsel Mueller’s investigation,¹⁷ Congress may consider legislative reforms to the authorities of special counsels and better delineate their relationships with other prosecuting entities.

¹⁰ Andrea Cavallier, *REVEALED: Woke Manhattan DA Alvin Bragg has downgraded over HALF of felony cases to misdemeanors as criminals are free to roam streets of the Big Apple*, DAILY MAIL (Nov. 28, 2022); Georgett Roberts and Melissa Klein, *Manhattan DA Alvin Bragg surprised by ‘push back’ – defends policies*, N.Y. Post (Jan. 8, 2022).

¹¹ *Numbers show the grim consequences of Manhattan DA Alvin Bragg’s pro-crime principles*, N.Y. Post (Nov. 27, 2022).

¹² *Id.*

¹³ Alyssa Guzman, *Priorities, eh? Woke DA Alvin Bragg who’s set to indict Trump is one of America’s most controversial prosecutors after charging self-defense shopkeeper with murder and sending soft-on-crime memo*, DAILY MAIL (Mar. 18, 2023); Cavallier, *supra* note 10.

¹⁴ Joe Marino and Bruce Golding, *Ex-con would have faced ‘long time in jail’ if not for new Manhattan DA: judge*, N.Y. Post (Jan. 12, 2022) (A career criminal “accused of threatening a drug store worker with a knife was told in court that he should “feel lucky” he got busted after new Manhattan District Attorney Alvin Bragg took office “Based on your record, you would have faced a long period of time in jail if convicted,” [Manhattan Criminal Court Judge Jay] Weiner said during the court proceeding”)

¹⁵ *Reimagining Public Safety in the COVID-19 Era, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 117th Cong. (Mar. 8, 2022) (testimony from Madeline Brame).

¹⁶ Jack Morphet and Gabrielle Fonrouge, *Mother of slain Army vet Hason Correa rips Manhattan DA Alvin Bragg for giving plea deals in case*, N.Y. Post (June 10, 2022).

¹⁷ Ben Protess et al., *How Michael Cohen turned against President Trump*, N.Y. Times (Apr. 21, 2019).

Mr. Alvin L. Bragg, Jr.
March 25, 2023
Page 5

C. The Requests Are Pertinent to the Committees' Inquiry.

The Committees' inquiry satisfies *Wilkinson's* third prong of pertinence to the oversight. Federal courts have interpreted this prong broadly, requiring "only that the specific inquiries be reasonably related to the subject matter under investigation."¹⁸ The information sought by the Committees will allow us to assess the extent to which your reported effort to indict a former President and current declared candidate for that office is politically motivated and whether Congress should therefore draft legislative reforms to, among other things, protect former and current Presidents from politically motivated prosecutions.

II. Your State Law-Based Defenses Are Insufficient.

Your conclusory claim that our constitutional oversight responsibilities will interfere with law enforcement is misplaced and unconvincing. As a threshold matter, whether your office is, in fact, fairly enforcing the law or abusing prosecutorial discretion to engage in a politically motivated indictment of a former President is a serious matter that, as discussed above, implicates significant federal interests. The Committees require information from the New York County District Attorney's Office to advance our oversight over the very matter that you claim is a basis to obstruct our investigation.

In support of your broad claim that compliance with the Committees' requests for documents and a transcribed interview would interfere with law enforcement, you note two New York State statutes that prohibit the disclosure of grand jury materials. The Committees' information requests, however, relate to numerous areas of inquiry that in no way implicate grand jury materials or seek information that would be confidential under New York law. For example, the request for your office's use of federal funds has no connection to any grand jury proceedings. Similarly, the vast majority of the questions that the Committees intend to ask you in an interview also would not implicate grand jury secrecy. Moreover, to the extent that questions are asked that you believe you are not permitted to answer, you would retain the ability to decline to answer or to assert an applicable privilege. Likewise, you remain free to decline to produce certain responsive documents on the basis of appropriate privileges or statutes that preclude production, provided you provide the Committees with a detailed privilege log that will enable us to review and evaluate your claims. The laws cited in your letter do not establish a basis for a complete refusal to cooperate. At best, they provide arguments that may be asserted on either a question-by-question or a document-by-document basis.

Furthermore, your invocation of certain New York laws as precluding you from complying with our oversight request is, at a minimum, overbroad. For example, New York's Freedom of Information Law (Public Officers Law § 87(2)) provides that agencies *may* decline to make certain records available for *public* inspection; it neither requires them to do so nor directly speaks to formal requests from congressional committees. Thus, that statutory provision does not preclude you from providing us with records that were "compiled for law enforcement

¹⁸ MORTON ROSENBERG, *WHEN CONGRESS COMES CALLING: A STUDY ON THE PRINCIPLES, PRACTICES, AND PRAGMATICS OF LEGISLATIVE INQUIRY* 18 (2017).

Mr. Alvin L. Bragg, Jr.

March 25, 2023

Page 6

purposes.”¹⁹ Indeed, the statute in question states that even when an agency receives a request from a member of the public, as opposed to congressional committees, a “denial of access shall not be based solely on the category or type of such record and shall be valid only when there is a particularized and specific justification for such denial.”²⁰

III. The Inquiry Does Not Intrude on Federalism Powers Because Congress Is Exercising Its Core Authority to Legislate.

Your letter raises unfounded and unpersuasive objections to our oversight based on federalism—arguing, in part, that our “requests are an unlawful incursion into New York’s sovereignty.”²¹ You go on to note that “the District Attorney is duty bound by his constitutional oath to New York’s sovereign interest in the exercise of police powers reserved to the States under the Tenth Amendment.”²² Contrary to your assertions, this inquiry does not infringe on New York’s sovereignty.

To begin with, your argument hinges on your assertion that “Congress cannot have any legitimate legislative task relating to the oversight of local prosecutors enforcing state law.” But this claim is simply wrong; as discussed at length above, this matter involves substantial federal interests. Moreover, the cases that you cite, *Younger v. Harris*, 401 U.S. 37 (1971), and *Cameron v. Johnson*, 390 U.S. 611 (1968), involve the question of when federal courts can enjoin prosecutions of state law. And needless to say, our oversight requests do no such thing; they would not block you from conducting any prosecution. Rather, we are simply seeking information to carry out constitutional duties.

Finally, our oversight requests do not implicate what is commonly referred to as the anti-commandeering principle.²³ In establishing the anti-commandeering principle in *New York v. United States*, the Supreme Court concluded that Congress cannot compel states to enact, enforce, or administer federal policies.²⁴ Unlike the matter before the Court in *New York*, our requests here simply do not compel the state “to enact, enforce, or administer federal policies.”²⁵ Rather, the Committees are merely seeking information pertaining to a matter that is directly within the purview of our jurisdiction and is necessary to inform potential legislative reforms.

IV. The Inquiry Does Not Usurp Executive Powers

In your reply letter, you cited the Supreme Court of the United States in *Watkins v. United States* as saying, “Congress [is not] a law enforcement or trial agency.”²⁶ We agree. The Committees do not seek to step into the shoes of the Executive Branch or usurp its powers.

¹⁹ Public Officers Law § 87(2)(e).

²⁰ *Id.* at § 87(2).

²¹ Letter from Dubeck, *supra* note 2.

²² *Id.*

²³ The Committee’s oversight does not involve the federal spending power. As such, the anti-coercion principle cannot be reasonably implicated.

²⁴ 505 U.S. 144, 188 (1992).

²⁵ *Id.*

²⁶ Letter from Dubeck, *supra* note 2 (citing *Watkins v. United States*, 354 U.S. 178, 187 (1957)).

Mr. Alvin L. Bragg, Jr.
 March 25, 2023
 Page 7

Rather, as explained, we are exercising the broad powers afforded Congress by the Constitution to conduct oversight to inform potential legislative reforms. This power

encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes. It includes surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them. It comprehends probes into departments of the Federal Government to expose corruption, inefficiency or waste.²⁷

Indeed, as the Supreme Court has recognized, Congress retains broad authority to conduct oversight of ongoing civil and criminal investigations. In *Sinclair v. United States*, the Supreme Court noted that the pendency of litigation does not stop Congress’s ability to investigate, stating:

It may be conceded that Congress is without authority to compel disclosures for the purpose of aiding the prosecution of pending suits; but the authority of that body, directly or through its committees, to require pertinent disclosures in aid of its own constitutional power is not abridged because the information sought to be elicited may also be of use in such suits.²⁸

The Court has further noted that “a congressional committee . . . engaged in legitimate legislative investigation need not grind to a halt whenever responses to its inquiries might potentially be harmful to a witness in some distinct proceeding . . . or when crime or wrongdoing is exposed.”²⁹ Phrased another way, the Committees’ oversight will in no way “stop [your] prosecution or set limits on the management of a particular case.”³⁰ Accordingly, your refusal to cooperate with our oversight inquires on this basis is therefore unavailing.

V. Your Offer to Provide Information About Your Office’s Use of Federal Funds Is Insufficient

While we appreciate your offer to submit a letter detailing the District Attorney’s Office’s use of federal funds, and we look forward to that submission, such a letter alone does not satisfy our oversight requests or preclude the Committees from proceeding with them. For example, as we have explained in detail, the Committee on the Judiciary is examining whether legislative reforms are necessary to insulate former and current Presidents from politically motivated prosecutions by state and local officials. And while your letter regarding your office’s use of federal funds will not shed meaningful light on that question, we expect that your response to our other information requests will do so.

²⁷ *Id.*

²⁸ 279 U.S. 263, 295 (1929).

²⁹ *Hutcheson v. United States*, 369 U.S. 599, 617 (1962).

³⁰ See MORTON ROSENBERG, CONGRESSIONAL RESEARCH SERVICE, INVESTIGATIVE OVERSIGHT: AN INTRODUCTION TO THE LAW, PRACTICE AND PROCEDURE OF CONGRESSIONAL INQUIRY (1995).

Mr. Alvin L. Bragg, Jr.

March 25, 2023

Page 8

Accordingly, we reiterate the requests in our March 20 letter and ask that you comply in full as soon as possible but no later than March 31, 2023. We trust the information in this letter satisfies your request to “understand whether the Committee has any legitimate legislative purpose”³¹ Thank you for your attention to this matter.

Sincerely,



Jim Jordan
Chairman
Committee on the Judiciary



Bryan Steil
Chairman
Committee on House Administration



James Comer
Chairman
Committee on Oversight and Accountability

cc: The Honorable Jerrold Nadler, Ranking Member
Committee on the Judiciary

The Honorable Joseph Morelle, Ranking Member
Committee on House Administration

The Honorable Jamie Raskin, Ranking Member
Committee on Oversight and Accountability

³¹ Letter from Dubeck, *supra* note 2.

THE LAW OFFICE OF CAREY R. DUNNE, PLLC

By email

March 27, 2023

The Honorable Jim Jordan
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Jordan:

I am in receipt of your letter dated March 22, 2023 (“the Committee Letter”), requesting that I provide to the House Committee on the Judiciary (“the Committee”) certain documents and information relating to my tenure at the Office of the New York County District Attorney (“the Office”).¹ I understand you sent a similar request directly to the Office on March 20, 2023, and that the Office responded to that letter on March 23, 2023.

Any information I have regarding the Office’s investigations, communications, and decision-making is derivative of my work as an attorney for the Office. The Office has directed me until further notice to decline to provide the Committee with the requested information and materials, and to instead refer the Committee to the Office for any further response. (A copy of the Office’s letter to me is attached.) As you know, the Office has deemed your request to be constitutionally infirm on federalism and other grounds, and improperly intrusive into an ongoing criminal investigation. The Office also asserts that the attorney-client privilege, the work product doctrine, and other legal protections are implicated by your requests. As the legal holder of such privileges, that is the Office’s prerogative. As a former attorney for the office, I will comply with its direction, and I respectfully refer the Committee to the Office for any further response.

Sincerely,



Carey R. Dunne

cc: The Honorable Jerrold Nadler, Ranking Member
Leslie Dubeck, General Counsel, Office of the New York County District Attorney

¹ To correct a misunderstanding in the Committee Letter: I served from January 1, 2017 to December 31, 2021 as General Counsel to the Office; I then served from January 1, 2022 to February 24, 2022 as a Special Assistant District Attorney.



ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

LESLIE B. DUBECK
GENERAL COUNSEL

**DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 336-9000**

Final Report 3951

March 25, 2023

By email

Mr. Carey R. Dunne
Former Assistant District Attorney
& General Counsel, New York County
New York, NY

Dear Mr. Dunne:

I am writing regarding the House Judiciary Committee (HJC) request of March 22, 2023, that you provide documents and information relating to your employment at the Office of the District Attorney of New York County (the "DA's Office"), which are similar to requests sent to the DA's Office on March 20, 2023.

The HJC's requests raise significant concerns about federalism, state sovereignty, the limits on congressional power, and the purpose and legality of the HJC's inquiry. In addition, the documents and information requested are protected from disclosure for many reasons, including because they relate to an ongoing criminal investigation, and are subject to the attorney client privilege, work product doctrine, and other legal protections.

For these reasons, the DA's Office has asked the HJC to provide additional information regarding their inquiries. To protect the DA's Office's interests and privileges, and until further notice, the DA's Office instructs you, as a former employee and attorney of the DA's Office, to not provide any information or materials relating to your work in the DA's Office in response to HJC's request. In addition, please direct HJC to communicate with the DA's Office regarding the request.

Sincerely,

A handwritten signature in black ink that reads "Leslie B. Dubeck".

Leslie B. Dubeck
General Counsel

MARK F. POMERANTZ

% Free & Fair Litigation Group
128 East Broadway, Unit 793
New York, NY 10002

March 27, 2023

BY E-MAIL

The Honorable Jim Jordan
2138 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Jordan:

This responds to your March 22, 2023 letter to me, which seeks certain documents and testimony relating to my employment at the New York County District Attorney's Office ("DANY").

After receiving your letter, I received a letter from Leslie Dubeck, General Counsel at DANY. Through that letter (copy attached), DANY has instructed me to not provide any information or materials in response to your request. At the present time, and in light of the ongoing discussions between DANY and the Committee, I will act in a manner consistent with the instructions I have received from DANY. Further, please note that DANY has asked that all communications regarding your request be directed to them.

Sincerely,



Mark F. Pomerantz

cc: The Honorable Jerrold Nadler, Ranking Member
Leslie Dubeck, General Counsel, DANY

Enclosure



DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000

Final Report 3953

ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

LESLIE B. DUBECK
GENERAL COUNSEL

March 25, 2023

By email

Mr. Mark F. Pomerantz
Former Special Assistant District Attorney,
New York County
New York, NY

Dear Mr. Pomerantz:

I am writing regarding the House Judiciary Committee (HJC) request of March 22, 2023, that you provide documents and information relating to your employment at the Office of the District Attorney of New York County (the "DA's Office"), which are similar to requests sent to the DA's Office on March 20, 2023.

The HJC's requests raise significant concerns about federalism, state sovereignty, the limits on congressional power, and the purpose and legality of the HJC's inquiry. In addition, the documents and information requested are protected from disclosure for many reasons, including because they relate to an ongoing criminal investigation, and are subject to the attorney client privilege, work product doctrine, and other legal protections.

For these reasons, the DA's Office has asked the HJC to provide additional information regarding their inquiries. To protect the DA's Office's interests and privileges, and until further notice, the DA's Office instructs you, as a former employee and attorney of the DA's Office, to not provide any information or materials relating to your work in the DA's Office in response to HJC's request. In addition, please direct HJC to communicate with the DA's Office regarding the request.

Sincerely,

A handwritten signature in black ink, appearing to read "Leslie B. Dubeck".

Leslie B. Dubeck
General Counsel

ONE HUNDRED EIGHTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6216
(202) 225-6906
judiciary.house.gov

April 6, 2023

Mr. Mark F. Pomerantz
Former New York County Special Assistant District Attorney
Free & Fair Litigation Group
128 E. Broadway, Unit 793
New York, NY 10002

Dear Mr. Pomerantz:

The Committee on the Judiciary is conducting oversight of the New York County District Attorney's unprecedented indictment of a former President of the United States and current declared candidate for that office. On March 22, 2023, we requested that you voluntarily cooperate with our oversight by providing relevant documents and testimony pertaining to your role as a special assistant district attorney leading the investigation into the former President's finances.¹ We received a reply letter dated March 27, 2023, stating that, at the instruction of the New York County District Attorney's Office, you would not cooperate with our oversight.² You enclosed a copy of a letter from the New York County District Attorney's Office directing you not to cooperate.³

The Supreme Court has recognized that Congress has a "broad and indispensable" power to conduct oversight, which "encompasses inquiries into the administration of existing laws, studies of proposed laws, and surveys in our social, economic or political system for the purpose of enabling Congress to remedy them."⁴ Rule X of the Rules of the House of Representatives authorizes the Committee on the Judiciary to conduct oversight of criminal justice matters to inform potential legislation.⁵ Congress has a specific and manifestly important interest in preventing politically motivated prosecutions of current and former Presidents by elected state

¹ Letter from Rep. Jim Jordan, H. Comm. on the Judiciary, to Mr. Mark F. Pomerantz, Former N.Y. Co. Special Assistant District Att'y (Mar. 22, 2023).

² Letter from Mr. Mark F. Pomerantz, Former N.Y. Co. Special Assistant District Att'y, to Rep. Jim Jordan, H. Comm. on the Judiciary (Mar. 27, 2023).

³ Letter from Leslie B. Dubeck, Gen. Counsel, N.Y. Co. District Att'y Off., to Mr. Mark F. Pomerantz, Former N.Y. Co. Special Assistant District Att'y (Mar. 25, 2023).

⁴ See, e.g., *Trump v. Mazars LLP*, No. 19-715 at 11 (U.S. slip op. July 9, 2020) (internal quotation marks and citations omitted).

⁵ Rules of the U.S. House of Representatives, R. X(1)(5) (2023).

Mr. Mark F. Pomerantz

April 6, 2023

Page 2

and local prosecutors, particularly in jurisdictions—like New York County—where the prosecutor is popularly elected and trial-level judges lack life tenure. Among other things, if state or local prosecutors are able to engage in politically motivated prosecutions of Presidents of the United States (current or former) for personal acts, this could have a profound impact on how Presidents choose to exercise their powers while in office. For example, a President could choose to avoid taking action he believes to be in the national interest because it would negatively impact New York City for fear that he would be subject to a retaliatory prosecution in New York City.

As a result, the New York County District Attorney’s unprecedented prosecutorial conduct requires oversight to inform the consideration of potential legislative reforms that would, if enacted, insulate current and former Presidents from such politically motivated state and local prosecutions. These potential legislative reforms may include, among other things, broadening the existing statutory right of removal of certain criminal cases from state court to federal court. The local prosecution of a former President also raises the potential for conflict between the federal law-enforcement officials required by federal law to protect a former President and local law-enforcement officials required to enforce an indictment and exercise control of him throughout his presence in the local criminal justice system. The Committee may consider legislative reforms to address or remedy this potential conflict. In addition, the New York County District Attorney’s Office has acknowledged that it used federal forfeiture funds in its investigations of President Trump, including during your tenure in that office and during the time when former President Trump was in office and a candidate for re-election.⁶ The Committee may therefore consider legislation to enhance reporting requirements concerning the use of federal forfeiture funds or to prohibit the use of federal forfeiture funds to investigate a current or former President or presidential candidate.

Based on your unique role as a special assistant district attorney leading the investigation into President Trump’s finances, you are uniquely situated to provide information that is relevant and necessary to inform the Committee’s oversight and potential legislative reforms. Although the New York County District Attorney’s Office has directed you not to cooperate with our oversight, you have already discussed many of the topics relevant to our oversight in a book you wrote and published in February 2023,⁷ as well as in several public interviews to promote your book.⁸ As a result, you have no basis to decline to testify about matters before the Committee that you have already discussed in your book and/or on a prime-time television program with an

⁶ See Letter from Leslie B. Dubeck, Gen. Counsel, N.Y. Co. District Att’y Off., to Rep. Jim Jordan, H. Comm. on the Judiciary 4 (Mar. 31, 2023) (“[O]f the federal forfeiture money that the Office helped collect, approximately \$5,000 was spent on expenses incurred relating to the investigation of Donald J. Trump or the Trump Organization. These expenses were incurred between October 2019 and August 2021.”).

⁷ MARK POMERANTZ, PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT (2023).

⁸ See, e.g., Rachel Maddow Show, *Trump case ‘cried out for federal investigation’*: Pomerantz, MSNBC (Feb. 7, 2023) (“As I mentioned in the book, this case cried out for federal investigation . . . I don’t know why there was never an intensive federal investigation of Trump’s finances.”); 60 Minutes, *Mark Pomerantz on investigating Donald Trump*, CBS NEWS (Feb. 5, 2023) (“[Bragg] did not say to slow down. He never said, ‘I don’t wanna be rushed. There’s not enough time. I need more time to study the facts.’ He said, ‘Okay. You need a decision? You get a decision.’ And the decision was no. ‘You’re not going forward.’”).

Mr. Mark F. Pomerantz

April 6, 2023

Page 3

audience in the millions, including on the basis of any purported duty of confidentiality or privilege interest.

Your book discloses various details about the New York County District Attorney's Office's investigation of President Trump, including internal deliberations about the investigation. Indeed, you discuss how members of the Office viewed the credibility of a key witness in the case, and you note their concerns about the case's dim prospects. For example, in your book, you recount a "mini-revolt" that occurred following an internal Office meeting on September 21, 2021, about the investigations into President Trump.⁹ You offer details about a disagreement between you and the Office's Major Economic Crimes Bureau Chief, Julieta Lozano, about Michael Cohen's credibility as a witness in the investigation.¹⁰ You also complain about concerns expressed by Chris Conroy, the Office's Investigative Division Chief, during a meeting on November 12, 2021.¹¹ According to you, Conroy "spoke about his misgivings" about the Trump investigation, which stemmed from a recent case involving financial and accounting fraud charges that mirrored the charges that the Office was considering pursuing against President Trump.¹² That case apparently ended poorly for the New York County District Attorney's Office.¹³ Like Lozano, Conroy also expressed concerns about Cohen's viability as a witness.¹⁴ You accuse other lawyers of being "relentlessly negative, dwelling on all the difficulties and issues with the case, and refusing to acknowledge the positives" during an internal meeting on December 10, 2021, referring to your former colleagues as "conscientious objectors" merely for opining that the case was "weak" and pointing to its "many fatal flaws."¹⁵ You ultimately dismiss their concerns about the investigation by suggesting that they were either too lazy to do the work, did not know the evidence, or were somehow afraid of bringing charges against President Trump.¹⁶

Your book, described as a "300-page exercise in score-settling and scorn,"¹⁷ also reveals the extent to which the New York County District Attorney's Office's investigation of President Trump appears to have been politically motivated. Specifically, you describe your eagerness to investigate President Trump, writing that you were "delighted" to join an unpaid group of lawyers advising on the Trump investigations, and joking that salary negotiations had gone "great" because you would have paid to join the investigation.¹⁸ You frivolously compare President Trump to mob boss John Gotti,¹⁹ and claim that the District Attorney's Office was "warranted in throwing the book" at President Trump because, in your view, he "had become a master of breaking the law in ways that were difficult to reach."²⁰ You explain that this "collective weight" of President Trump's conduct over the years "left no doubt in [your] mind

⁹ POMERANTZ, *supra* note 7, at 159.

¹⁰ *Id.*

¹¹ *Id.* at 171.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.* at 191–92, 194.

¹⁶ *Id.* at 160, 171–72.

¹⁷ Lloyd Green, *People vs Donald Trump review: Mark Pomerantz pummels Manhattan DA*, THE GUARDIAN (Feb. 11, 2023).

¹⁸ POMERANTZ, *supra* note 7, at 6, 21–22.

¹⁹ *Id.* at 108–09.

²⁰ *Id.* at 112.

Mr. Mark F. Pomerantz

April 6, 2023

Page 4

that [President] Trump deserved to be prosecuted.”²¹ In other words, as a special assistant district attorney, you seem, for reasons unrelated to the facts of this particular investigation, to have been searching for any basis on which to bring criminal charges.²²

Although you claim that you were “able to put aside [your] personal feelings about [President] Trump” during the investigation, the depth of your personal animosity towards him is apparent in your writing. You wrote of President Trump:

I saw him as a malignant narcissist, and perhaps even a megalomaniac who posed a real danger to the country and the ideals that mattered to me. His behavior made me angry, sad, and even disgusted.²³

You additionally “marveled at the thought” of being “at the center of what might become one of the most consequential criminal cases ever brought.”²⁴ You reflect on your “only similar experience,” which you indicated was the “indictment of Osama bin Laden and other members of al Qaeda for the bombing of the United States embassies in Kenya and Tanzania.”²⁵ Drawing a parallel between these two vastly different matters speaks volumes about the mindset that you brought to the investigation of President Trump.

These perceptions appear to have colored your work as a special assistant district attorney, to the point that you even resigned because the investigation into President Trump was not proceeding fast enough for your liking.²⁶ In your resignation letter, you prejudged the results of the District Attorney’s investigation, writing that “Donald Trump is guilty of numerous felony violations,” and vowing not to be a “passive participant” to “a grave failure of justice.”²⁷ Your public resignation reportedly left District Attorney Bragg “deeply stung,” and caused him to issue an “unusual” public statement “emphasizing that the investigation into Trump and his business was far from over.”²⁸ Your book also contributed to the “political pressure” on District Attorney Bragg to bring charges against former President Trump.²⁹

²¹ *Id.* at 112–13.

²² See also Rachel Maddow Show, *Watch Rachel Maddow Highlights: Feb. 6*, YOUTUBE (Feb. 6, 2023) (“[W]e were trying to work quickly. Bringing a racketeering case, particularly one that includes [other crimes], it’s such a big ball of wax that, ultimately, we decided, you know what, let’s focus on a smaller, more contained set of charges. That’s when we started to focus on the financial statements.”).

²³ POMERANTZ, *supra* note 7, at 176.

²⁴ *Id.* at 194–95.

²⁵ *Id.*

²⁶ *Read the Full Text of Mark Pomerantz’s Resignation Letter*, N.Y. TIMES (Mar. 23, 2022).

²⁷ *Id.*

²⁸ Mark Berman et al., *The prosecutor, the ex-president and the ‘zombie’ case that came back to life*, WASH. POST (Mar. 17, 2023).

²⁹ Luc Cohen, *Trump charges follow criticism of Manhattan prosecutor for not acting sooner*, REUTERS (Mar. 31, 2023).

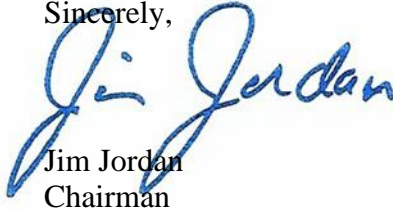
Mr. Mark F. Pomerantz

April 6, 2023

Page 5

Accordingly, for these reasons, and in light of your disregard of our earlier voluntary request, please find attached a subpoena compelling your appearance for a deposition.

Sincerely,

A handwritten signature in blue ink that reads "Jim Jordan". The signature is written in a cursive style with a large, looping "J" and "J" at the beginning and end.

Jim Jordan
Chairman

cc: The Honorable Jerrold Nadler, Ranking Member

Enclosure

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 4/19/2023

ALVIN L. BRAGG, JR., *in his official capacity as
District Attorney for New York County,*

Plaintiff,

-against-

JIM JORDAN, *in his official capacity as Chairman
of the Committee on the Judiciary,* COMMITTEE
ON THE JUDICIARY OF THE UNITED STATES
HOUSE OF REPRESENTATIVES, and MARK F.
POMERANTZ,

Defendants.

1:23-cv-3032 (MKV)

OPINION AND ORDER
DENYING TEMPORARY
RESTRAINING ORDER

MARY KAY VYSKOCIL, United States District Judge:

The request by Manhattan District Attorney Alvin L. Bragg Jr. for a temporary restraining order, enjoining enforcement of the subpoena issued to Mark F. Pomerantz by the Committee on the Judiciary of the United States House of Representatives, chaired by Congressman Jim Jordan, is DENIED. The subpoena was issued with a “valid legislative purpose” in connection with the “broad” and “indispensable” congressional power to “conduct investigations.” It is not the role of the federal judiciary to dictate what legislation Congress may consider or how it should conduct its deliberations in that connection. Mr. Pomerantz must appear for the congressional deposition. No one is above the law.

BACKGROUND

On April 6, 2023, the Committee on the Judiciary of the United States House of Representatives (the “Committee”) issued a subpoena, directing Mark F. Pomerantz (“Pomerantz”), a former *pro bono* employee of the Office of the District Attorney for New York County (“DANY”), to appear on April 20, 2023 “to testify at a deposition touching matters of

inquiry committed to [the Committee].” Exhibit 1 (“Ex. 1”) to the Declaration of Theodore J. Boutrous, Jr. (“Boutrous Dec.”) [ECF No. 12-1]. The subpoena does *not* request that Pomerantz produce any documents. *See* Ex. 1.

The subpoena was accompanied by a letter from the Chairman of the Committee, Jim Jordan (“Jordan”). *See* Ex. 1. The letter requests Pomerantz’s appearance due to his “unique role as a special assistant district attorney leading the investigation into President Trump’s finances.” Ex. 1 at 2. It further explains that Pomerantz has “already discussed many of the topics relevant to [the Committee’s] oversight in a book [that Pomerantz] wrote and published in February 2023, as well as in several public interviews to promote [his] book.”¹ Ex. 1 at 2 (citations omitted). Jordan notes that DANY has “acknowledged that it used federal forfeiture funds in its investigations of President Trump,”² and that the Committee was considering “potential legislative reforms,” such as “broadening the existing statutory right of removal of certain criminal cases from state court to federal court.” Ex. 1 at 2.

The book referenced in Jordan’s letter is *People vs. Donald Trump: An Inside Account*, written by Pomerantz and published in early 2023. *See* M. Pomerantz, *People vs. Donald Trump: An Inside Account* (2023) (“*Inside Account*”). As its subtitle indicates, the book recounts Pomerantz’s *insider* insights, mental impressions, and his front row seat to the investigation and deliberative process leading up to the DANY case against former President and current presidential candidate Donald Trump. Among Pomerantz’s observations:

- Within DANY, the case against Trump arising out of payment of so-called “hush money” to Stephanie Clifford was referred to as the “zombie” case. *Id.* at 200.
- The facts surrounding the payments “did not amount to much in legal terms. Paying hush money is not a crime under New York State law, even if the payment

¹ *See* Exhibits E–O to the Declaration of Todd B. Tatelman [ECF Nos. 32-5 to 32-15].

² *See* Exhibit 19 to the Boutrous Dec. [ECF No. 12-20].

was made to help an electoral candidate.” *Id.* at 40.

- “[C]reating false business records is only a misdemeanor under New York law.” *Id.* at 40.
- “[T]here appeared to be no [felony] state crime in play.” *Id.* at 40–41.
- “[T]o charge Trump with something other than a misdemeanor, DANY would have to argue that the intent to commit or conceal a federal crime had converted the falsification of the records into a felony. No appellate court in New York had ever upheld (or rejected) this interpretation of the law.” *Id.* at 41.
- The statutory language (under which Trump was charged) is “ambiguous.” *Id.* at 40.
- “[T]here was a big risk that felony charges would be dismissed before a jury could even consider them.” *Id.* at 41.
- “[T]he Trump investigation should have been handled by the U.S. Department of Justice, rather than by the Manhattan district attorney’s office.” *Id.* at 240.
- “[F]ederal prosecutors would not have to torture or massage [statutory] language to charge Trump with a violation,” as DANY would have to do. *Id.* at 240.
- *Federal prosecutors previously looked into the Clifford “hush money payment” and did not move forward with the prosecution. Id.* at 242 (emphasis added); *see also id.* at 39.
- There is a statute of limitations issue with the DANY case against Trump. *Id.* at 240–41.
- Numerous DANY prosecutors were skeptical about the prosecution of Trump and were referred to internally at DANY as “conscientious objectors.” *Id.* at 194.
- The invoices and requests for payment from Michael Cohen in connection with the Clifford payments, in a supposed effort to “camouflage” reimbursements, were made “throughout 2017 (*after* Trump’s inauguration as president).” *Id.* at 39 (emphasis added) (parenthetical in original).
- The DANY prosecution team discussed “Michael Cohen’s credibility” as being one of “the difficulties in the case.” *Id.* at 203.
- *At one point, Bragg “commented that he ‘could not see a world’ in which [DANY] would indict Trump and call Michael Cohen as a prosecution witness.” Id.* at 227 (emphasis added).

- While Pomerantz acknowledged Bragg’s right to make prosecutorial decisions, Pomerantz viewed himself as more experienced and qualified than Bragg. *Id.* at 218–19. Pomerantz makes a point that he was “finishing law school when Alvin was a toddler.” *Id.* at 208.
- Pomerantz resigned from his *pro bono* position at DANY when it became clear to him that President Trump would not be indicted. *Id.* at 248–51; *see also* Exhibit C (“Ex. C”) to the Declaration of Todd B. Tatelman (“Tatelman Dec.”) [ECF No. 32-3]. Pomerantz “told the DA that he was responsible for a ‘grave failure of justice’ because he would not authorize Trump’s indictment.” *Inside Account* at 1.
- Ultimately in March 2023, Bragg did, of course, indict President Trump, “bring[ing] the ‘zombie’ theory back from the dead once again.” *Id.* at 209.

Jordan and the Committee first tried to acquire information from Pomerantz and DANY voluntarily. *See, e.g.*, Exhibit 2 (“Ex. 2”) to the Boutrous Dec. [ECF No. 12-2]; Exhibit 11 (“Ex. 11”) to the Boutrous Dec. [ECF No. 12-12]; Exhibit 58 (“Ex. 58”) to the Boutrous Dec. [ECF No. 12-61]. While the DANY General Counsel offered to “meet and confer” with the Committee “to understand whether [it] ha[d] any legitimate legislative purpose in the requested materials,” DANY declined to provide information and instructed Pomerantz not to comply with the Committee’s requests. Exhibit 10 (“Ex. 10”) to the Boutrous Dec. at 5 [ECF No. 12-11]; Exhibit 12 (“Ex. 12”) to the Boutrous Dec. [ECF No. 12-13]; *see also* Exhibit 19 (“Ex. 19”) to the Boutrous Dec. [ECF No. 12-20].

On April 11, 2023, Manhattan District Attorney Alvin L. Bragg, Jr. (“Plaintiff” or “Bragg”)—one of five local district attorneys for the five boroughs in the City of New York—filed a 50-page Complaint in this Court, naming Jordan, the Committee, and Pomerantz as defendants. *See* Complaint [ECF No. 1] (“Compl.”). Bragg simultaneously filed a motion, brought on by an *ex parte* proposed order to show cause, seeking a temporary restraining order and a preliminary injunction (1) enjoining Jordan and the Committee from enforcing the subpoena served on Pomerantz and (2) enjoining Pomerantz from complying with the subpoena, *see*

Proposed Order to Show Cause With Emergency Relief [ECF No. 7]; *see also* Memorandum of Law in Support [ECF No. 8] (“Pl. Mem.”). Plaintiff later filed the Declaration of Theodore J. Boutrous, Jr., accompanied by over 60 exhibits. *See* Boutrous Dec.

The first 35 pages of the Complaint have little to do with the subpoena at issue and are nothing short of a public relations tirade against former President and current presidential candidate Donald Trump. The same is true of the vast majority of the exhibits accompanying the Boutrous Declaration. Of note, the Complaint acknowledges that DANY used federal forfeiture funds in investigating President Trump and/or the Trump Organization. Compl. ¶ 78. Moreover, Bragg concedes that DANY was aware that Pomerantz was writing a book about the Trump investigation and asked to review the manuscript pre-publication. Compl. ¶ 90. Pomerantz declined. Compl. ¶ 90; Pl. Mem. 21–22. At heart, the Complaint simply includes two requests for declaratory and injunctive relief directed at the congressional inquiry. The reality is that, as framed, this action is merely a motion to quash a subpoena dressed up as a lawsuit.

The motion for a temporary restraining order was filed without notice to Defendants and before Defendants even were served with the Complaint. *See* Certificate of Service [ECF No. 17]; Waiver of Service [ECF No. 18]. In this Court, Local Civil Rule 6.1(d) dictates that any party seeking an *ex parte* order must submit an “affidavit of good and sufficient reasons why a procedure other than by notice of motion is necessary, and stating whether a previous application for similar relief has been made.” No such affidavit was submitted here. Accordingly, the Court issued an Order, declining to enter the proposed order to show cause, directing service on Defendants not only of the motion (with all supporting papers), but also of the Complaint by which this case was initiated, setting a briefing schedule to allow Defendants to be heard, and scheduling a hearing for today to address the motion for a temporary restraining order. *See* Order [ECF No. 13].

Jordan and the Committee filed an opposition brief. *See* Opposition Brief [ECF No. 27]

(“Def. Mem.”). They argue that Bragg cannot establish a likelihood of success on the merits because Jordan and the Committee are immune from suit under the Speech or Debate Clause of Article I of the United States Constitution. Def. Mem. 5–14. Defendants further argue that the subpoena has at least two valid legislative purposes. First, they contend that the Committee is considering the viability of legislation to protect former Presidents and presidential candidates from politically motivated prosecutions by local district attorneys, such as by permitting those cases to be removed to federal court, out of a concern that such prosecutions “could have a profound impact on how Presidents choose to exercise their powers while in office.” Def. Mem. 3. Second, Defendants argue that the Committee is permissibly investigating DANY’s use of federal forfeiture funds in the investigation of President Trump, which could potentially influence the outcome of the 2024 presidential election. Def. Mem. 8–9.

Pomerantz filed a “response” to Bragg’s motion. *See* Pomerantz Response [ECF No. 30] (“Pomerantz Res.”); *see also* Declaration of Mark F. Pomerantz [ECF No. 31] (“Pomerantz Dec.”). Pomerantz describes himself as a “nominal[]” defendant. Pomerantz Dec. ¶ 1. He does not oppose Bragg’s motion and, instead, joins in the request for an injunction. *See* Pomerantz Dec. ¶ 1 (“I have no objection to the relief that the District Attorney has requested. I consent to that relief, and indeed urge this Court to grant it.”).³ It appears that Pomerantz is content to largely allow Bragg to speak for him. *See* Pomerantz Res. 1 (“These are matters for the District Attorney . . . to argue.”); *id.* at 5 (“We defer to the papers filed by the District Attorney on this motion to articulate why the subpoena threatens New York’s sovereign power.”). Indeed, Bragg’s counsel, Theodore J. Boutros, Jr., filed a waiver of service on behalf of Pomerantz. *See* Waiver of Service [ECF No. 18].

³ Unless otherwise noted, references to “Defendants” in this Opinion refer only to Jordan and the Committee.

The day before the scheduled hearing, Bragg filed an eleventh hour reply brief, not authorized by the Court’s Scheduling Order given the compressed time frame in which Plaintiff’s motion was brought on. The reply largely rehashes the same arguments made in the moving brief and, for the first time, addresses the Speech or Debate Clause. *See* Reply Brief [ECF No. 41-1] (“Reply”). The reply brief was accompanied by a supplemental declaration attaching sixteen largely irrelevant exhibits, consisting of a hodge-podge of social media postings, news articles, television interviews, pleadings from unrelated lawsuits, and a transcript from the arraignment in the Trump prosecution. *See* Exhibits 60–72 to the Second Boutrous Declaration [ECF Nos. 41-2 to 41-5].

The Court is in receipt of several unsolicited amicus briefs. An assemblage of former members of Congress, former prosecutors, former government attorneys, and academics filed an amicus brief with the consent of Bragg. *See* Letter Motion to File Amicus Brief [ECF No. 34]; Amicus Brief [ECF No. 37] (“First Amicus”). Amici argue that the Committee lacked authority to issue the subpoena and echo Bragg’s refrain that the subpoena will “interfere with an ongoing criminal prosecution . . . brought by a state prosecutor.” First Amicus 1. A separate group of former state and federal prosecutors filed another amicus brief, again with the consent of Bragg. *See* Letter Motion to File Amicus Brief [ECF No. 40] (“Second Amicus”). These amici assert that the subpoena “seriously challenges . . . the prosecutorial process.” Second Amicus 2.⁴

Bragg and his two sets of amici attack what they describe as federal interference in his criminal prosecution. Pl. Mem. 1; First Amicus 3; Second Amicus 3. There is no question that New York, a sovereign state in our federal system, has authority to enforce its criminal laws through its local prosecutors. The Court is mindful of potential federalism concerns. However,

⁴ The Court also received a “friend of the court letter” from James H. Brady, dated April 17, 2023. *See* Letter [ECF No. 38]. The Court has reviewed and considered all of the unsolicited submissions.

the Court rejects the premise that the Committee’s investigation will interfere with DANY’s ongoing prosecution. The subpoena of Pomerantz, who was a private citizen and public commentator at the time Bragg indicted Trump, will not prevent or impede the criminal prosecution that is proceeding in New York state court.

ANALYSIS

I. Bragg Has Sufficiently Alleged Article III Standing

A threshold issue in this matter is whether Bragg has standing to maintain this action since the challenged subpoena is not addressed to Bragg or his office. *See All. For Env’t Renewal, Inc. v. Pyramid Crossgates Co.*, 436 F.3d 82, 85 (2d Cir. 2006) (“[A] district court must generally. . . establish that it has federal constitutional jurisdiction, including a determination that the plaintiff has Article III standing, before deciding a case on the merits.”). The subpoena was issued to Pomerantz—not to Bragg. *See* Ex. 1. Pomerantz has not filed suit. Although he is named as a defendant, Pomerantz “asks this Court to grant [Bragg’s] motion.” Pomerantz Res. 1.

Bragg, as the party invoking federal jurisdiction, bears the burden of establishing standing. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). The Supreme Court has “established that the ‘irreducible constitutional minimum’ of standing consists of three elements.” *Id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). “The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Id.*

Where a plaintiff seeks to enjoin a subpoena issued to a third party and has “no alternative means to vindicate [his] rights,” a plaintiff satisfies his burden of establishing standing. *U.S. Servicemen’s Fund v. Eastland*, 488 F.2d 1252, 1260 (D.C. Cir. 1973), *rev’d on other grounds*, 421 U.S. 491 (1975); *see also Trump v. Deutsche Bank AG*, 943 F.3d 627, 635 (2d Cir. 2019), *rev’d on other grounds sub nom.*, 140 S. Ct. 2019 (2020) (“[T]here is no dispute that Plaintiffs had

standing in the District Court to challenge the lawfulness of the Committees' subpoenas by seeking injunctive relief against the Banks as custodians of the documents.”).

Bragg's stated interest in the subpoena is his claim that permitting Pomerantz to appear will undermine the pending criminal case against President Trump, intrude on the grand jury proceedings, and violate grand jury secrecy laws, among other things. These assertions are all without merit. Since Pomerantz was not at DANY when the grand jury indicted President Trump (and therefore has no information on that subject), *see* Pomerantz Res. 2, the only arguably valid interest Bragg has (to the extent it is not waived, *see infra* Section II.D) is in maintaining the confidentiality of deliberations within the office he now leads.

Determining whether Bragg has any “alternative means to vindicate” his rights is made difficult where, as here, the Court cannot predict what questions will be asked—or whether any rights of Bragg will be implicated. In that vein, Defendants contend that Bragg “has no standing whatsoever to stop Pomerantz from appearing before the Committee to answer . . . questions” that “do not involve purportedly privileged material in any way.” Def. Mem. 18.

The Court concludes that Bragg sufficiently alleges standing. Jordan's letter to Pomerantz references “the New York County District Attorney's unprecedented prosecutorial conduct” and Pomerantz's “unique role as a special assistant district attorney.” *See* Ex. 1 at 2. These areas of inquiry at least arguably implicate Bragg's interests. Because “general factual allegations of injury resulting from the defendant's conduct may suffice” at the *pleading* stage, the Court concludes that Bragg has established Article III standing sufficient to survive this *even earlier* stage of litigation. *Lujan*, 504 U.S. at 561; *cf. U.S. Servicemen's Fund*, 488 F.2d at 1260; *Deutsche Bank*, 943 F.3d at 635.

II. Bragg Is Not Entitled to a Temporary Restraining Order

A. Legal Standard

In the Second Circuit, the same legal standard governs the issuance of preliminary injunctions and temporary restraining orders. *See, e.g., 3M Co. v. Performance Supply, LLC*, 458 F. Supp. 3d 181, 191 (S.D.N.Y. 2020). To obtain either, Bragg must show: (1) a likelihood of success on the merits, (2) a likelihood of irreparable injury, (3) the balance of hardships tips in his favor, and (4) that the public interest would not be disserved by the issuance of an injunction. *See Benihana, Inc. v. Benihana of Tokyo, LLC*, 784 F.3d 887, 895 (2d Cir. 2015).⁵ Like a preliminary injunction, a temporary restraining order is “an extraordinary remedy never awarded as of right.” *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008).

Where a party seeking a temporary restraining order fails to establish a likelihood of success on the merits, “there is no need to address the other prongs of the analysis.” *Oneida Nation of New York v. Cuomo*, 645 F.3d 154, 164 (2d Cir. 2011). For the reasons outlined below, Bragg has not demonstrated a likelihood of success on the merits.

B. The Subpoena Serves a Valid Legislative Purpose and Is Not Ultra Vires or Otherwise Unconstitutional

Congressional committees have constitutional authority to conduct investigations and issue subpoenas because “each House has power ‘to secure needed information’ in order to legislate.” *Trump v. Mazars USA, LLP*, 140 S. Ct. 2019, 2031 (2020) (quoting *McGrain v. Daugherty*, 273 U.S. 135, 161 (1927)); *see Eastland v. U.S. Servicemen’s Fund*, 421 U.S. 491, 504 (1975). This “power of inquiry—with process to enforce it—is an *essential* and *appropriate* auxiliary to the

⁵ The Second Circuit has previously instructed that a district court may also grant a preliminary injunction when there are “sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly in the movant’s favor” and “irreparable harm in the absence of the injunction.” *Kelly v. Honeywell Int’l, Inc.*, 933 F.3d 173, 184 (2d Cir. 2019). Neither party contends that this standard should apply here.

legislative function.” *McGrain*, 273 U.S. at 174 (emphasis added). “The power of the Congress to conduct investigations is inherent in the legislative process.” *Watkins v. United States*, 354 U.S. 178, 187 (1957).

Of course, this power is not limitless. “[T]here is no congressional power to expose for the sake of exposure.” *Id.* at 200. Nor may Congress issue subpoenas “for the purpose of ‘law enforcement,’” because that power is assigned “to the Executive and the Judiciary.” *Mazars*, 140 S. Ct. at 2032 (quoting *Quinn v. United States*, 349 U.S. 155, 161 (1955)). However, the Supreme Court has described the congressional power of inquiry as “broad” and “indispensable.” *Watkins*, 354 U.S. at 187, 215. Indeed, without its investigative powers, “Congress would be shooting in the dark, unable to legislate ‘wisely or effectively.’” *Mazars*, 140 S. Ct. at 2031 (quoting *McGrain*, 273 U.S. at 175).

Congress may conduct inquiries “into the administration of existing laws, studies of proposed laws, and [particularly relevant here,] ‘surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them.’” *Mazars*, 140 S. Ct. at 2031 (quoting *Watkins*, 354 U.S. at 187). Importantly, a congressional subpoena is valid only if it is “related to, and in furtherance of, a legitimate task of the Congress.” *Watkins*, 354 U.S. at 187. The subpoena must serve a “valid legislative purpose,” *Quinn*, 349 U.S. at 161, and “concern[] a subject on which ‘legislation could be had,’” *Eastland*, 421 U.S. at 506 (quoting *McGrain*, 273 U.S. at 177). The role of a court in evaluating a congressional subpoena is strictly limited to determining only whether the subpoena is “plainly incompetent or irrelevant to any lawful purpose . . . in the discharge of [the Committee’s] duties.” *McPhaul v. United States*, 364 U.S. 372, 381 (1960) (emphasis added) (quoting *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (1943)).

Jordan and the Committee have identified several valid legislative purposes underlying the subpoena. *See* Def. Mem. 15–17. First, they reference the Committee’s interest in investigating the use of federal forfeiture funds in connection with DANY’s investigation of President Trump. *See* Def. Mem. 8, 17; *see also* Ex. 1 at 2; Exhibit V (“Ex. V”) to the Tatelman Dec. [ECF No. 32-22]. There can be no doubt that Congress may permissibly investigate the use of federal funds, particularly where the result of the investigation might prompt Congress to pass legislation changing how such funds are appropriated or may be spent. *See Sabri v. United States*, 541 U.S. 600, 608 (2004) (“The power to keep a watchful eye on expenditures and on the reliability of those who use public money is bound up with congressional authority to spend in the first place.”); U.S. Const. art. I, § 8, cl. 1. DANY has conceded that it used federal forfeiture funds in its investigation of President Trump. *See* Ex. 19; Compl. ¶¶ 78, 81. Defendants represent that the Committee is considering legislation to prohibit the use of federal forfeiture funds to investigate a current or former President. Def. Mem. at 8; Ex. V. This purpose, standing alone, is clearly sufficient to justify the subpoena and thereby to end this Court’s inquiry. On the record at the hearing on the motion for emergency relief, Bragg’s counsel conceded that the investigation of DANY’s use of federal funds is a valid legislative purpose.

Second, Defendants identify the possibility of legislative reforms to insulate current and former presidents from state prosecutions, such as by removing criminal actions filed against them from state to federal court. *See* Def. Mem. 8–9. Congress, of course, has authority to consider, and to investigate, this potential legislative reform. *See Watkins*, 354 U.S. at 187 (“The [investigative] power of the Congress . . . encompasses inquiries concerning the administration of existing laws as well as *proposed or possibly needed* statutes.” (emphasis added)); U.S. Const. art. I, § 8, cl. 18 (defining the congressional power “[t]o make all laws which shall be necessary and proper for carrying into execution the foregoing powers”). And Congress also has authority to

investigate legislative reforms to prevent local prosecutions that could potentially interfere with federal elections. *See Mazars*, 140 S. Ct. at 2031 (It is legitimate for Congress to conduct “inquiries into the administration of existing laws” and “proposed laws” that seek to address problems “in our social, economic or political system.”). Although Bragg speculates that any such legislation would be unconstitutional, *see* Pl. Mem. 15, that issue is for another day. The Court will not, and indeed cannot, block congressional investigation into *hypothetical* future legislation based on Bragg’s speculation that such legislation would not pass constitutional muster. *See Nashville, C. & St. L. Ry. v. Wallace*, 288 U.S. 249, 262 (1933) (courts may not make “abstract determination[s] . . . of the validity of a statute”).⁶

C. *The Subpoena Does Not Implicate the Sovereign Interests of New York*

Bragg suggests that these are not the Committee’s *true* objectives. Instead, he contends that the subpoena is *actually* intended “to undermine and obstruct New York’s criminal case against Mr. Trump and [to] retaliate against the District Attorney.” Pl. Mem. 7. The Court cannot passively accept this contention. The Court is required to presume that a congressional committee’s stated legislative object is “the real object.” *McGrain*, 273 U.S. at 178 (When it appears that Congress is investigating on a subject matter in aid of legislating, “the presumption should be indulged that this was the real object.”). Moreover, even if Bragg’s hypotheses about the Committee’s *real* motivations were correct, they are irrelevant. “It is not a court’s ‘function’ to invalidate a congressional investigation that serves a legislative purpose.” *Comm. on Ways & Means, U.S. House of Representatives v. U.S. Dep’t of the Treasury*, 575 F. Supp. 3d 53, 69 (D.D.C. 2021), *aff’d sub nom.*, 45 F.4th 324 (D.C. Cir. 2022) (quoting *Watkins*, 354 U.S. at 200). Indeed, the Supreme Court has instructed that “[s]o long as Congress acts in pursuance of its

⁶ Plaintiffs make much of *Kilbourn v. Thompson*, 103 U.S. 168 (1880). *See* Pl. Mem. 7–8. But the Court concluded there that the subpoena was “clearly judicial” in nature. 103 U.S. at 192. The same is not true here.

constitutional power, the Judiciary *lacks authority to intervene on the basis of the motives which spurred the exercise of that power.*” *Barenblatt v. United States*, 360 U.S. 109, 132 (1959) (emphasis added). Whatever motives may underlie the Committee’s subpoena, its “inquiry may fairly be deemed within its province.” *Tenney v. Brandhove*, 341 U.S. 367, 378 (1951). That is sufficient to resolve this inquiry.⁷

Plaintiff next urges this Court to apply the “heightened standard of review” outlined by the Supreme Court in *Trump v. Mazars USA, LLP*, 140 S. Ct. 2019 (2020). Pl. Mem. 13. In *Mazars*, the Supreme Court outlined a four-part analysis relevant in assessing “a subpoena *directed at the President’s personal information.*” 140 S. Ct. at 2035 (emphasis added). Because “[c]ongressional subpoenas for the President’s personal information implicate[d] weighty concerns regarding the separation of powers,” the Supreme Court instructed courts considering such subpoenas to: (1) “carefully assess whether the asserted legislative purpose warrants the significant step of involving *the President* and his papers,” (2) “insist on a subpoena no broader than reasonably necessary to support Congress’s legislative objective,” (3) “be attentive to the nature of the evidence offered by Congress to establish that a subpoena advances a valid legislative purpose,” and (4) “be careful to assess the burdens imposed *on the President* by a subpoena.” *Id.* at 2035–36 (emphasis added). The Court did not, as Bragg suggests, indicate that the four *Mazars* factors apply *whenever* someone argues that a subpoena “implicat[es] significant separation-of-powers concerns.” Pl. Mem. 13. In any event, the same separation of powers concerns are *not* implicated here. The congressional subpoena in *Mazars* was directed at materials pertaining to the *sitting President of the United States*. In contrast, here, the subpoena was issued to a *private*

⁷ Bragg notes that there is “no prior case in which Congress has attempted to subpoena a state prosecutor for the purpose of extracting information about an ongoing state prosecution.” Pl. Mem. 12 (emphasis omitted). Defendants do not dispute this characterization or cite to any such case. However, there also is no prior case in which a former President of the United States has been criminally charged in a state trial court, suggesting *both* parties swim in untested waters.

citizen who is *no longer* employed by *any* state government and who has written a book and spoken extensively about the subject matter of the congressional inquiry. The Court is not persuaded that *Mazars* applies to this case.⁸

Even assuming that *Mazars* were applicable, the Court would reach the same conclusion. With respect to the first factor, Bragg does not demonstrate that the subpoena issued to Pomerantz—a private citizen—will occasion a “constitutional confrontation.” *Mazars*, 140 S. Ct. at 2035 (quoting *Cheney v. U.S. Dist. Ct. for D.C.*, 542 U.S. 367, 389 (2004)). Congress has the power to compel individuals to testify. *See Watkins*, 354 U.S. at 187–88 (“It is unquestionably the duty of all citizens to cooperate with the Congress in its efforts to obtain the facts needed for intelligent legislative action. It is their unremitting obligation to respond to subpoenas, to respect the dignity of the Congress and its committees and to testify fully with respect to matters within the province of proper investigation.”); *Quinn*, 349 U.S. at 160–61 (“There can be no doubt as to the power of Congress, by itself or through its committees, to investigate matters and conditions relating to contemplated legislation. . . . Without the power to investigate—including of course the authority to compel testimony, either through its own processes or through judicial trial—Congress could be seriously handicapped in its efforts to exercise its constitutional function wisely and effectively.” (citations omitted)). Indeed, courts have even compelled individuals *actively* employed by the executive branch (who at least arguably hold executive privilege, and some of whom are attorneys obligated to protect privileged information) to appear for congressional depositions. *See, e.g., Meadows v. Pelosi*, No. 1:21-CV-03217 (CJN), 2022 WL 16571232 at *8–13 (D.D.C. Oct. 31, 2022) (dismissing challenge by White House Chief of Staff to a congressional

⁸ Despite having discussed *Mazars* in his moving brief, Bragg seeks a second chance at arguing its applicability in his reply brief, contending that the case broadly governs subpoenas “seeking a current or former president’s information.” Reply 8. That is clearly incorrect. In any event, the subpoena does *not* seek a current or former president’s information—it seeks *Pomerantz*’s testimony. *See* Ex. 1.

subpoena requesting his appearance for a deposition); *Comm. on Judiciary, U.S. House of Representatives v. Miers*, 558 F. Supp. 2d 53, 106 (D.D.C. 2008) (“[The former White House counsel] is not excused from compliance with the Committee’s subpoena by virtue of a claim of executive privilege that may ultimately be made. Instead, she must appear before the Committee to provide testimony, and invoke executive privilege where appropriate.”); *Comm. on Judiciary of U.S. House of Representatives v. McGahn*, 968 F.3d 755, 764 (D.C. Cir. 2020) (“The subpoena power is potent. Each House of Congress is specifically empowered to compel testimony from witnesses and the production of evidence in service of its constitutional functions, and the recipient of a subpoena is obligated by law to comply.”). If those individuals could permissibly be deposed, the same is certainly true here.

Second, the subpoena seeks only Pomerantz’s *testimony* (not any documents or materials). Jordan specifically noted that “*many* of the topics relevant to [the Committee’s oversight]” were discussed—voluntarily and extensively—by Pomerantz in his book, as well as in several public interviews. Ex. 1 at 2 (emphasis added). The subpoena is not, as Bragg contends, an “overbroad fishing expedition.” Pl. Mem. 17.

Third, Bragg criticizes Defendants’ “flimsy evidence” of a valid legislative purpose. Pl. Mem. 17 (internal quotation marks omitted); *see also* Pomerantz Res. 3. But Defendants provide evidence that the Committee is investigating the use of federal forfeiture funds, *see* Ex. V, and considering the viability of legislation to protect former Presidents from politically motivated state prosecutions, *see* Exhibit W to the Tatelman Dec. [ECF No. 32-23].⁹ Bragg suggests this evidence

⁹ Although Pomerantz contends that he has “little if anything to say that will advance the purported legislative purpose,” Pomerantz Res. at 5, it is not this Court’s role to prescribe the most effective manner for congressional inquiry. *See Eastland*, 421 U.S. at 509 (“The very nature of the investigative function—like any research—is that it takes the searchers up some ‘blind alleys’ and into nonproductive enterprises. To be a valid legislative inquiry there need be no predictable end result.”).

is insufficient but his conclusory assertions do not move the needle where, as here, *he* has the burden of demonstrating entitlement to an “extraordinary remedy.” *Winter*, 555 U.S. at 24.

Bragg and Pomerantz insist that Pomerantz’s testimony cannot advance any valid legislative purpose because, in essence, everything Pomerantz is prepared to say is already in his book and he does not have information about DANY’s use of federal funds. Pl. Mem. 11, 22 (“[T]he Committee already has his book.”); Pomerantz Res. 2; Reply 5. Bragg and Pomerantz are not entitled to unilaterally narrow the universe of acceptable inquiry to the information and mental impressions that Pomerantz decided to sell in the pages of his book. *See Eastland*, 421 U.S. at 509; *McGahn*, 968 F.3d at 764. If Pomerantz does not have any information about DANY’s use of federal funds, he may say so if asked at his deposition.

Finally, Bragg’s suggestion that the subpoena “would substantially burden both the New York criminal justice system itself and the District Attorney’s Office” is without merit. Pl. Mem. 18. Pomerantz is a *former* prosecutor. He is not involved in the state prosecution in any way. Bragg provides no reason to conclude that a deposition of a former employee would interfere with DANY or any of its ongoing prosecutions. The pending prosecution will move forward in the ordinary course regardless of whether the Committee deposes Pomerantz. Further, Pomerantz was not even employed with DANY at the time President Trump was indicted. Pomerantz admits as much. Pomerantz Dec. ¶ 4. He has stated that the materials in his book would “have no bearing on the litigation of [the criminal prosecution of President Trump]” and would “not prejudice any investigation or prosecution of Donald Trump.” *Inside Account* at 278–79. Moreover, Pomerantz emphasizes that he “was *not* involved in the decision to bring the pending indictment against Mr. Trump.” Pomerantz Res. 5 (emphasis added). Bragg therefore does not satisfy his burden of demonstrating that the subpoena poses a threat “to a state executive officer, a state judicial proceeding, [or] our federal system itself.” Pl. Mem. 14. The Court is further unmoved by Bragg’s

purported concern at the prospect of “inject[ing] partisan passions into a forum where they do not belong.” Pl. Mem. 19. By bringing this action, Bragg is engaging in precisely the type of political theater he claims to fear.

While the Court need not decide the ultimate merits of Bragg’s claims at this stage, serious constitutional infirmities are evident with respect to a lawsuit against Defendants Jordan and the Committee. *See* Def. Mem. 5–9. The Speech or Debate Clause states: “for any Speech or Debate in either House,” Senators and Representatives “shall not be questioned in any other Place.” U.S. Const. art. I, § 6, cl. 1. Although the Clause speaks only of “Speech or Debate,” it has been interpreted to protect all “legislative acts.” *See Doe v. McMillan*, 412 U.S. 306, 312 (1973) (citation omitted). The Clause provides individual members of Congress *and* congressional committees broad immunity from civil suits. *See Eastland*, 421 U.S. at 501–03; *Doe*, 412 U.S. at 313; *see also Harlow v. Fitzgerald*, 457 U.S. 800, 807 (1982); *Supreme Ct. of Virginia v. Consumers Union of U.S., Inc.*, 446 U.S. 719, 731–33 (1980). Because Jordan and the Committee are likely immune, Defendants contend that they are necessary parties who cannot be joined and that, under Federal Rule of Civil Procedure 19, the action cannot be maintained. *See* Def. Mem. 10–14. Bragg disagrees.¹⁰ The Court need not resolve this issue, but the distinct possibility of immunity weighs against concluding that Bragg has shown a likelihood of success on the merits. In all events, Bragg confirms in his reply brief that the Court must consider whether there is a “legitimate legislative purpose” for the subpoena he seeks to quash. Reply 3. As explained above, Jordan and the Committee clearly have identified a legitimate legislative purpose, and accordingly the Court will not issue a temporary restraining order.

¹⁰ Despite pervasive discussion of the Speech or Debate Clause in the relevant case law and governing authority, Bragg neglected to mention the Clause whatsoever in his moving brief. However, Bragg seeks an opportunity to address this “material issue[.]” in his unauthorized reply brief. *See* Letter Motion for Leave to File Reply [ECF No. 41].

D. *To the Extent They Have Not Been Waived, the Claimed Privileges Are Not Jeopardized by the Subpoena*

Plaintiff's assertion that the subpoena "seeks grand jury material" and "documents and communications protected by the attorney-client privilege and work product doctrine" does not salvage his motion. Pl. Mem. 20. As an initial matter, the subpoena does *not*, as Plaintiff suggests, "seek[]" any "material," "documents," or "communications." Pl. Mem. 20. The subpoena *only* seeks Pomerantz's *testimony*. See Ex. 1. Although Bragg assumes that the questioning will stray into impermissible territory, the Court declines Bragg's invitation to blindly speculate about what questions might *hypothetically* be posed to Pomerantz at the deposition. See *Nat'l Org. for Marriage, Inc. v. Walsh*, 714 F.3d 682, 687 (2d Cir. 2013) ("A claim is not ripe if it depends upon 'contingent future events that may not occur as anticipated, or indeed may not occur at all.'" (quoting *Thomas v. Union Carbide Agr. Prods. Co.*, 473 U.S. 568, 580–81 (1985)); *Ass'n of Car Wash Owners Inc. v. City of New York*, 911 F.3d 74, 85 (2d Cir. 2018) ("[F]ederal courts may not give an opinion advising what the law would be upon a hypothetical state of facts." (citing *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 241 (1937) (internal quotation marks omitted))).

Bragg's throw-everything-at-the-wall approach to privilege is unpersuasive. As an initial matter, Bragg concedes that "Jordan represents that he *does not* seek information protected by New York's grand jury secrecy laws." Pl. Mem. 20 (emphasis added). Although Bragg vaguely asserts that the Committee's "inquiry *could* [still] include questions about grand jury matters," this Court will not quash a subpoena based solely on Bragg's seemingly endless string of "what ifs." Pl. Mem. 21 (emphasis added). Even if grand jury secrecy *were* implicated by the subpoena, Bragg's argument makes little sense because Pomerantz was not involved in securing the grand jury indictment. Pomerantz Dec. ¶ 3. Indeed, at the time Pomerantz left DANY, "there [had] been no New York state criminal prosecution of Donald Trump." *Inside Account* at 278. And even

assuming Pomerantz *did* have some relevant information about the grand jury, Pomerantz is clearly aware that he “cannot disclose details about grand jury proceedings” since he professes that he authored his book in such a way that his “account of the investigation did not violate the grand jury secrecy requirement.” *Id.* at 195, 277.¹¹

With respect to Bragg’s various other claims of privilege,¹² the Court is unpersuaded that judicial intervention is needed to ensure that any privilege that might exist is preserved. Pomerantz is impressively credentialed. He had a long and successful career: he graduated from the University of Michigan Law School, served as a law clerk for a distinguished federal judge, clerked at the United States Supreme Court, was a law professor, worked as a federal prosecutor for the United States Attorney’s Office for the Southern District of New York, and as a criminal defense attorney for many years, including as a senior partner at a prominent New York City law firm (Paul, Weiss, Rifkind, Wharton & Garrison). *See Inside Account* at 3–4. In short, Pomerantz is a very experienced, sophisticated, and extremely capable attorney. Moreover, the Committee’s procedural rules permit two additional lawyers to accompany Pomerantz to the deposition. *See* Rules of Procedure of the Committee on the Judiciary, R. XI(k)(3) (2023) (“Rule XI”).¹³ This

¹¹ The Court notes that the secrecy of the grand jury proceedings in the pending criminal case was compromised before an indictment was even announced. *See* Kara Scannell *et al.*, *Donald Trump indicted by Manhattan grand jury on more than 30 counts related to business fraud*, CNN (Mar. 31, 2023, 7:35 AM), <https://www.cnn.com/2023/03/30/politics/donald-trump-indictment/index.html>.

¹² Specifically, Bragg contends that attorney-client privilege, attorney work product protection, law enforcement privilege, informant’s privilege, public interest privilege, and deliberative process privileges are all implicated. Pl. Mem. 21–22. Although Bragg pays lip service to these other so-called privileges, his primary concern appears to be the possibility that Pomerantz might be asked to disclose the “internal deliberations” of DANY, which is a question of work product. *See* Pl. Mem. 21. Work product protection is not absolute, but rather offers a *qualified* protection to “documents and tangible things that are prepared in anticipation of litigation or for trial.” Fed. R. Civ. P. 26(b)(3). Of course, this is precisely what Pomerantz lays out in *People vs. Donald Trump: An Inside Account*.

¹³ Although the rules only permit “personal, nongovernmental attorneys” to accompany Pomerantz, *see* Rule XI, this Court has no authority to rewrite the Committee’s rules. *See Exxon Corp. v. F.T.C.*, 589 F.2d 582, 590 (D.C. Cir. 1978) (“[W]e are sympathetic to appellants’ concern for safeguarding highly confidential information worth millions of dollars, but for this court on this record to establish any such requirement would clearly involve an unacceptable judicial intrusion into the internal operations of Congress.”).

Court is confident that Pomerantz and his counsel are fully knowledgeable about the privilege and confidentiality obligations he owes to DANY and, indeed, are duty bound to ensure they are maintained.¹⁴ See Model Rules of Pro. Conduct 1.6 (duty of confidentiality); 1.9 (duties to former clients) (Am. Bar Ass’n 2023); see also *Inside Account* at 279 (noting that Pomerantz “overcame [his] angst” about “describing the inner dialogue of the investigation” because “the Trump investigation was in a class of its own”). The “recipients of legislative subpoenas . . . have long been understood to retain common law and constitutional privileges with respect to certain materials, such as attorney-client communications and governmental communications protected by executive privilege.” *Mazars*, 140 S. Ct. at 2032.

Pomerantz is now represented by a team of capable lawyers from his former firm Paul, Weiss. See Notices of Appearance [ECF Nos. 28, 29]. Bragg provides no reason to assume those accomplished lawyers would not also be fully knowledgeable about Pomerantz’s ethical obligations with respect to privilege and confidentiality. Accordingly, the deposition should proceed in the normal course, question by question, and Pomerantz is free to object, personally or through his counsel, and decline to answer any questions when (and if) appropriate. See *Miers*, 558 F. Supp. 2d at 106–07. Indeed, Defendants confirm that “[t]o the extent that questions are asked that Pomerantz believes he is not permitted to answer, he would retain the ability to decline to answer or to assert an applicable privilege.” Def. Mem. 19.

Bragg expresses concern that the Committee’s rules permit “a partisan decisionmaker” to “overrule privilege objections” at the deposition and “order a witness to answer a question.” Pl.

¹⁴ Pomerantz has made it abundantly clear that he will seek to comply with Bragg’s instructions and to invoke privilege. See Pomerantz Res. 4 (“The District Attorney . . . instructed Mr. Pomerantz, in writing, to provide no information to the [Committee] in response to the subpoena.”); see also Pomerantz Dec. ¶ 6 (“[I]f I were to testify, I believe that the District Attorney would instruct me to assert the various claims of privilege he has identified in his moving papers.”). This claimed deference to the District Attorney’s command is a surprising about-face, particularly given that Pomerantz previously *declined* the District Attorney’s request to review his book manuscript before publication. See Compl. ¶ 90.

Mem. 23. The Court cannot decide, before-the-fact, “what information or answers [Pomerantz] may validly be required to give or the validity of any objections he might make.” *Sanders v. McClellan*, 463 F.2d 894, 903 (D.C. Cir. 1972); *see also Ansara v. Eastland*, 442 F.2d 751, 753 (D.C. Cir. 1971) (noting that “courts [should] avoid use of extraordinary remedies that involve ‘needless friction’ with a coordinate branch of the government” where “the plaintiffs [sought] relief that would precede and seek to relate to the conduct of a *future* legislative hearing” (emphasis added) (citation omitted)). But in the event that this situation does arise, Pomerantz has avenues for judicial review. *See, e.g., Watkins*, 354 U.S. at 214–16; *United States v. House of Representatives of U.S.*, 556 F. Supp. 150, 152 (D.D.C. 1983) (“[C]onstitutional claims and other objections to congressional investigatory procedures may be raised as defenses in a criminal prosecution.”).

Pomerantz complains that he is in a “legally untenable position” because he will be forced to make a choice between “legal or ethical consequences” or “potential criminal and disciplinary exposure.” Pomerantz Res. 4–5. The Court, again, is unable to surmise whether Pomerantz will *actually* face such a dilemma. In addition, the Court notes that Pomerantz is in this situation because *he* decided to inject himself into the public debate by authoring a book that he has described as “appropriate and in the public interest.” *Inside Account* at 280.

Finally, Bragg cannot seriously claim that any information *already published* in Pomerantz’s book and discussed on prime-time television in front of millions of people is protected from disclosure as attorney work product (or otherwise). *See* Pl. Mem. 21–22. On the record at the hearing on the motion for emergency relief, Bragg’s counsel admitted that Pomerantz’s book did not preserve the confidences of the District Attorney’s Office. While Bragg maintains that Pomerantz’s inappropriate disclosures cannot waive DANY’s privilege, such a claim is belied by DANY’s inaction in response to Pomerantz’s *known plan* to publish a book about DANY’s

investigation into President Trump. If that information *ever* was protected from disclosure as attorney work product,¹⁵ the protection has been *waived* by DANY. Bragg concedes that he was aware of Pomerantz’s intention to publish the book *before* it was published. Compl. ¶ 90. Although Bragg contends that he “diligently sought to protect [the privilege],” he merely “remind[ed] Mr. Pomerantz of his obligations not to disclose confidential or privileged information and request[ed] the opportunity for prepublication review.” Pl. Mem. 21. By Bragg’s own admission, Pomerantz *declined* the request for pre-publication review and proceeded to publish the book anyway. Pl. Mem. 21–22. There is no evidence that DANY took *any action* before the book was published—such as seeking to enjoin publication or distribution.¹⁶ Similarly, after publication, DANY *again* took no action. It did not request a gag order, seek an injunction, pursue Pomerantz for money damages, refer Pomerantz for an ethics inquiry, or even raise any concerns about the publication with Pomerantz. This repeated inaction constitutes acquiescence to the disclosure of any otherwise privileged information. *See, e.g., Cruz v. Coach Stores, Inc.*, 196 F.R.D. 228, 230 (S.D.N.Y. 2000) (privilege waived where “Coach raised no objection when . . . Jaspán Associates . . . publicly filed a copy of the [purportedly privileged document and Coach] . . . neither sought its sealing by the Court nor raised any objection with Jaspán Associates.”); *von Bulow by Auersperg v. von Bulow*, 114 F.R.D. 71, 76 (S.D.N.Y. 1987) (“An attorney’s disclosure of communications with his client will constitute a waiver of the attorney-client privilege if the

¹⁵ Pomerantz seemingly contends it was not, as he has publicly stated that he is “confident that all of [his] actions with respect to the Trump investigation, including the writing of [his] forthcoming book, are consistent with [his] legal and ethical obligations.” Compl. ¶ 90; *see also Inside Account* at 279–80 (“The public debate about Trump’s conduct, his unique public status, the circumstances under which my work ended, and the extensive news coverage about the progress of the investigation convinced me that writing this book was appropriate and in the public interest.”).

¹⁶ At the hearing on the motion for emergency relief, the Court repeatedly pressed Bragg to describe what, if any steps, DANY took to preserve its privilege after it became aware that Pomerantz intended to publish a book. In response to that questioning, Bragg’s counsel represented for the first time that at some point, she copied the City’s Department of Investigation on an email containing the letter that DANY sent to Pomerantz reminding him of his ethical obligations to DANY.

client has . . . acquiesced in the disclosure.”). Because Bragg has *never* claimed that any information in the book was privileged, he may not do so now simply because it is convenient.

In sum, the Court is unwilling to hypothesize about, and prophylactically rule on, the permissibility of questions that may—or may not—arise at the deposition of Pomerantz. Bragg has not shown a likelihood of success on the merits. The Court therefore need not address the other prongs of the temporary restraining order analysis. *See Oneida*, 645 F.3d at 164.¹⁷

CONCLUSION

For the foregoing reasons, the motion for a temporary restraining order enjoining the subpoena to depose Mr. Pomerantz and enjoining Mr. Pomerantz from appearing is DENIED.

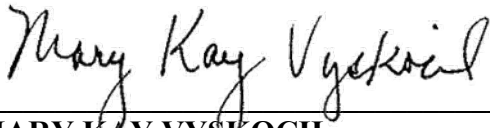
In our federalist system, elected state and federal actors sometimes engage in political dogfights. Bragg complains of political interference in the local DANY case, but Bragg does not operate outside of the political arena. Bragg is presumptively acting in good faith. That said, he is an elected prosecutor in New York County with constituents, some of whom wish to see Bragg wield the force of law against the former President and a current candidate for the Republican presidential nomination. Jordan, in turn, has initiated a political response to what he and some of his constituents view as a manifest abuse of power and nakedly political prosecution, funded (in part) with federal money, that has the potential to interfere with the exercise of presidential duties and with an upcoming federal election. The Court does not endorse either side’s agenda. The sole question before the Court at this time is whether Bragg has a legal basis to quash a congressional subpoena that was issued with a valid legislative purpose. He does not.

¹⁷ In his Complaint, Bragg seeks a declaratory judgment that any *future* subpoenas served by Jordan or the Committee on Bragg or “any of his current or former employees or officials” are “invalid, unconstitutional, *ultra vires*, and/or unenforceable” and a “permanent and preliminary injunction enjoining enforcement of any such [future] subpoena.” Compl. ¶ 127; *see* Compl. ¶ 20. To be clear, Bragg seeks this declaratory judgment for theoretical *future* subpoenas which Jordan or the Committee may issue against him or others. On the record at the hearing on the motion for emergency relief, Bragg’s counsel represented that he is not seeking such a declaratory judgment at this time.

The parties are encouraged to speak with one another to reach a mutually agreeable compromise regarding how the deposition of Mr. Pomerantz will proceed. This Court will retain jurisdiction over this dispute and any ancillary claims arising out of the inquiry by the Committee relating to the use of federal funds in a manner that may influence the 2024 presidential election. In other words, Bragg may not file successive proceedings under a different index number if and when the Committee in fact issues another subpoena that he finds objectionable or if there are issues with respect to the Pomerantz deposition. The parties are HEREBY ORDERED to file a joint status report within 30 days of the date of this Order.

SO ORDERED.

Date: April 19, 2023
New York, NY



MARY KAY VYSKOCIL
United States District Judge

COMMITTEE ON THE JUDICIARY,
U.S. HOUSE OF REPRESENTATIVES,
WASHINGTON, D.C.

DEPOSITION OF: MARK F. POMERANTZ

Friday, May 12, 2023

Washington, D.C.

The deposition in the above matter was held in room 2141, Rayburn House Office Building, commencing at 10:06 a.m.

Present: Representatives Jordan, Armstrong, Bishop, Gaetz, Hageman, Issa, Stefanik, Goldman, Plaskett, and Schiff.

Appearances:

For the COMMITTEE ON THE JUDICIARY:

[REDACTED], GENERAL COUNSEL

[REDACTED], DEPUTY GENERAL COUNSEL

[REDACTED], SENIOR ADVISOR

[REDACTED], STAFF DIRECTOR

[REDACTED], DEPUTY COMMUNICATIONS DIRECTOR

[REDACTED], COUNSEL

[REDACTED], CHIEF COUNSEL FOR OVERSIGHT

[REDACTED], COUNSEL

[REDACTED], DIGITAL DIRECTOR

[REDACTED], MINORITY CHIEF OVERSIGHT COUNSEL

[REDACTED], MINORITY INTERN

[REDACTED], MINORITY CHIEF COUNSEL

AND DEPUTY STAFF DIRECTOR

[REDACTED], MINORITY OVERSIGHT COUNSEL

For the SUBCOMMITTEE ON THE CONSTITUTION

AND LIMITED GOVERNMENT:

[REDACTED], MINORITY PROFESSIONAL STAFF MEMBER

For the DISTRICT ATTORNEY'S OFFICE, NEW YORK COUNTY:

MYLAN L. DENERSTEIN, PARTNER, GIBSON DUNN

LESLIE DUBECK, GENERAL COUNSEL

For the WITNESS:

ROBERTO FINZI, PARTNER

JACOB ROSEN, LITIGATION ASSOCIATE

THEODORE V. WELLS, JR., PARTNER

PAUL, WEISS

1285 AVENUE OF THE AMERICAS

NEW YORK, NY 10019-6064

Mr. [REDACTED] We'll go on the record now.

Good morning. This is a deposition of Mr. Mark Pomerantz, formerly of the District Attorney's Office of New York County.

Chairman Jordan has requested this as part of the committee's oversight of the unprecedented indictment of a former President of the United States and a current declared candidate for that office.

The committee's oversight of the New York County District Attorney's unprecedented prosecutorial conduct will inform the consideration of potential legislative reforms that would, if enacted, insulate current and former Presidents from politically motivated State and local prosecutions.

These potential reforms may include, among other things, legislation to enhance reporting requirements concerning the use of Federal forfeiture funds or to prohibit the use of Federal funds to investigate a current or former President or current Presidential candidate and broadening the existing statutory right of removal of certain criminal cases from State to Federal court.

Because of Mr. Pomerantz's former role as a Special Assistant District Attorney that led the investigation into President Trump's finances, he is uniquely situated to provide information that is relevant and necessary to inform the committee's oversight and potential legislative reforms.

On April 6th of this year, Chairman Jordan issued a subpoena for Mr. Pomerantz to testify at a deposition. I'd like to mark that as exhibit 1.

[Pomerantz Exhibit No. 1

Was marked for identification.]

Mr. [REDACTED] Would the witness please state your name for the record, sir?

The Witness. Yes. My name is Mark F. Pomerantz.

Mr. [REDACTED]. And you're joined here today by personal counsel.

Mr. Wells, I'll have you introduce yourself and your colleagues.

Mr. Wells. Yes. My name is Ted Wells. I'm with the Paul, Weiss law firm.

I'm here today with my partner, Roberto Finzi, and my associate, Jacob Rosen.

Mr. [REDACTED]. And we're also joined here today by Ms. Dubeck from the New York County District Attorney's Office. We'll have Ms. Dubeck introduce herself.

Ms. Dubeck. I'm Leslie Dubeck. I'm the general counsel of the New York County District Attorney's Office.

Mr. [REDACTED]. And I understand you're also joined by one of your colleagues?

Ms. Dubeck. Oh, yes. Mylan Denerstein from the Gibson Dunn firm.

Mr. [REDACTED]. My name is [REDACTED]. I'm with Chairman Jordan's House Judiciary Committee staff.

I'm going to have the staffers introduce themselves first, and then we'll allow the members to introduce themselves, starting with my colleague, Ms. Nabity.

Ms. [REDACTED] [REDACTED] with Chairman Jordan's committee staff.

Ms. [REDACTED] [REDACTED] with Chairman Jordan.

Ms. [REDACTED] [REDACTED] chief oversight counsel for the House Judiciary Democratic staff.

Ms. [REDACTED] [REDACTED] House Judiciary Democrat staff.

Ms. [REDACTED] [REDACTED] with the House Judiciary Democrats.

Mr. [REDACTED] [REDACTED] House Judiciary Democrats.

Ms. [REDACTED] [REDACTED] with the House Judiciary Committee Democrats.

Mr. [REDACTED]. We're also joined by some of our members. I'll have them introduce themselves as well.

Chairman Jordan. Jim Jordan, Fourth District of Ohio.

Ms. Stefanik. Elise Stefanik, 21st District of New York, House Republican
Conference chair.

Mr. Armstrong. Kelly Armstrong, North Dakota.

Mr. Gaetz. Matt Gaetz, First District of Florida.

Mr. Bishop. Dan Bishop, North Carolina.

Mr. [REDACTED] And some members may come in after the proceedings begin, and depending on where we are, we may or may not have them introduces themselves. But certainly if they're going to ask any questions of you, we'll be sure to have introductions.

I'd like to go over the ground rules and guidelines that we will follow during today's deposition.

The committee will conduct the deposition in accordance with Rule XI of the Committee on the Judiciary's Rules of Procedure of the 118th Congress as well as the House rules.

Our questioning will proceed in rounds. The majority will ask questions first for 1 hour, and then the minority will have an opportunity to ask questions for an equal period of time if they choose. We will alternate back and forth until there are no more questions and the interview is over.

We ordinarily take a short break at the end of each hour, and the provision of breaks is totally up to you, sir. You let us know if you need a break, more breaks or less breaks. And you may also ask us to go off the record so you can confer with your counsel.

As you can see, we have an official reporter here taking down everything to make a written record, so we ask that you give verbal responses to all the questions.

Do you understand that?

The Witness. I do.

Mr. [REDACTED] Sometimes the court reporters need us to go back because we're talking over one another. Usually it's our fault. So we may have to go back and repeat a question.

We will only have one staffer asking you a question per round. However, the members can jump in. And ordinarily on our side we like to make sure we have at least 15 or 20 minutes of every hour that we turn it to our members.

We want you to answer our questions in the most complete and truthful manner as possible, so we will take our time. If you have any questions or don't understand one of our questions, please let us know. Our questions will cover a cover a wide range of topics, so if you need clarification at any point just say so.

If you don't know the answer to a question or do not remember -- of course, it's best not to guess -- please give us your best recollection. And it's okay to tell us if you learned information from someone else. The Federal Rules of Evidence aren't applicable here. Just indicate how you came to know the information. And if there are things you don't know or can't remember, just say so.

By law you are required to answer questions from Congress truthfully. Do you understand that?

The Witness. I understand that.

Mr. [REDACTED] Witnesses that knowingly provide false testimony could be subject to criminal prosecution for perjury. Do you understand that?

The Witness. I do.

Mr. [REDACTED] And, of course, as I indicated before we went on the record, I mean no disrespect by mentioning that. You are a veteran lawyer and somebody who obviously has great understanding of how this process works.

Finally, I'd like to make a note that under the deposition rules, the content of what we discuss here today is confidential. And until the chairman and ranking member sort out what portions of the testimony or all the testimony is going to be released, under the House rules it's confidential. Obviously, you're not a party to the House rules, but I mention that for our members and staff.

At this time the court reporter will swear the witness in.

The Reporter. Please raise your right hand.

Do you solemnly declare and affirm, under the penalty of perjury, that the testimony you're about to give will be the truth, the whole truth, and nothing but the truth?

The Witness. I do.

Mr. [REDACTED] [REDACTED] do you have any welcoming remarks?

Ms. [REDACTED] We don't have any.

Mr. [REDACTED] Okay. And before we start our questions, Mr. Wells or Mr. Pomerantz, do you have any remarks you'd like to make to kick things off?

The Witness. I do have a statement.

Mr. [REDACTED] Okay. Take your time.

The Witness. I am here because I respect the rule of law. I've spent my working life in service to the rule of law. And the rule of law requires a witness to appear for testimony in response to a subpoena. So I am present as required.

What I do not respect is the use of the committee's subpoena power to compel me to participate in an act of political theater.

This deposition is for show. I do not believe for a moment that I am here to assist a genuine effort to enact legislation or to conduct legislative oversight.

We are gathered here because Donald Trump's supporters would like to use these

proceedings to attempt to obstruct and undermine the criminal case pending against him and to harass, intimidate, and discredit anyone who investigates or charges him.

Fortunately, I do not have to cooperate with the cynical histrionics that this deposition represents. Although the rule of law compels me to be here, it does not require that I play a substantive role in a theatrical production. Under the law, I can decline to answer your questions for several reasons.

First, I have been instructed by the Manhattan District Attorney's Office that I should maintain that office's claims of privilege and confidentiality in order to protect the integrity of the pending prosecution and continuing investigation of Donald Trump. I intend to honor the District Attorney's request, and I will not answer questions to which the District Attorney objects.

Although I have written and spoken publicly about the Trump investigation, I did so before any criminal charges were brought against Mr. Trump.

Now that a grand jury has indicted him, the circumstances have changed. With formal charges now pending, the rule of law is best served if the merits of the case against Mr. Trump are litigated before the court that is hearing that case.

This is neither the time nor the place for me to answer questions about the investigation or the pending indictment over the objection of the prosecutors. The charges against Mr. Trump should be heard and decided by a judge and a jury before politicians second-guess their merits or the decision to bring them.

That's how our system works. Those who claim that they respect the rule of law should wait for the courts to do their work.

Second, the rule of law also affords me a personal privilege not to answer your questions. Under the Fifth Amendment to the Constitution, no person may be compelled to be a witness against himself or herself in a possible criminal case.

Shortly before the publication of my book, the District Attorney's Office warned me that I could face criminal liability if, among other things, I disclosed grand jury material or violated a provision of the New York City Charter dealing with the misuse of confidential information.

When we were before the United States District Court on April 19th of this year, a lawyer for the Manhattan District Attorney's Office said that my book, quote, "exposed me to criminal liability," close quote.

While I am certain that I broke no laws, I am not required to answer questions if my answers might be used against me in a criminal prosecution. The Fifth Amendment is a protection for all citizens, including those who have done nothing wrong.

Therefore, and on the advice of counsel, I will invoke my rights under the Fifth Amendment and I will not answer any questions that could conceivably be used against me in a criminal case.

Finally, the rule of law permits me to refuse to answer questions that are not pertinent to a legitimate legislative function or that seek information that is protected by the First Amendment's guarantee of freedom of speech. Under the Due Process Clause of the Fifth Amendment, I cannot be punished for refusing to answer such questions.

There may be other privileges, such as the attorney-client privilege or the work product privilege, that are available to me with respect to certain questions.

For all these reasons, I will not be answering questions that relate to my work in the District Attorney's Office, my book, or public statements I have made in the past.

It gives me no joy to invoke my legal rights, but I am glad that the law allows me not to cooperate with this performance of political theater.

As an American, I am privileged to have the legal rights that I assert today, and I am hopeful that I live in a country that will continue to respect them.

Mr. [REDACTED] On that note, I would just remark for the record that we, the Congress, recognizes constitutional-based privileges but not common law based-privileges. And as we represented to the Second Circuit, the committee will consider any invocation of privilege and accompanying explanation on an individualized question-by-question basis.

So even though it might get repetitive, we are going to ask for an explanation for each objection and then consider your explanation.

The chairman may rule -- he may overrule the objection, and in that instance we would instruct you to answer the question. At the end of the process, we'll maybe tally up the questions that haven't been answered and offer you a chance to change your mind. And if we do need to bring you back or pursue additional proceedings, we will -- we'll write you a letter, and we'll proceed on that basis.

Mr. Wells. Can I reply?

Mr. [REDACTED] Certainly, sir.

Mr. Wells. Today is not the day to debate the merits of explanations for asserting privileges. He will assert the privilege, the committee members may rule on the privilege, the record will be made, but we are not going to debate the merits. That is for a court if we ever get in front of a court.

So I have no problem if you're making a ruling. The record will be made and we'll move on to the next question. But we are not going to debate the legitimacy of any particular privilege so the record will be clear with respect to his assertions.

Mr. [REDACTED] Fair enough sir. I hope I didn't indicate to you that I wanted to have a debate with you on the record.

Mr. Wells. No. I'm responding to the phrase "explanations."

Mr. [REDACTED] Well, explanation --

Mr. Wells. If I misunderstood what you meant, we can --

Mr. [REDACTED] I think by explanation, it's the nature of the -- is it based on the Fifth Amendment or is it based on what the District Attorney's Office has told you.

Mr. Wells. That's very common.

Mr. [REDACTED] That's what we're looking for.

Mr. Wells. Yes, that's very common.

Mr. [REDACTED] We're not looking for the case citations and so forth.

With that, I'll begin my hour. Hopefully this will be a productive hour and find some questions that you want to answer.

I'll note it's 10:21. I'll be referring, sir, to your book. If you need a copy, we can provide you one.

EXAMINATION

BY MR. [REDACTED]

Q On page 1 of your book, you state that when you joined the Trump investigation you got countless emails and telephone calls from friends and colleagues urging me to go get him.

Was that statement accurate?

A Mr. [REDACTED] I acknowledge writing the book, but I'm not going to expand beyond what is contained in the book for the reasons reflected in my opening statement.

Q But surely you can concur that the statement was accurate?

A I think I can concur that you have read accurately from the book, which speaks for itself.

Q Okay.

A I'm not disputing your --

Q But your book's accurate, right?

A I'm not going to expand beyond acknowledging that I wrote this book.

Q But you didn't put anything intentionally false in the book, correct?

A I'm not going to answer your question.

Q Okay. What did you --

A One way or the other.

Q Okay. What did you understand your friends and colleagues to mean when they were urging you to go get him?

A Again, I'm not going to go beyond what is stated in the book, and I assert my rights as reflected in the statement that I made at the outset.

Q And how did you respond to your friends and colleagues when they urged you to go get him?

A I'm not going to answer your questions for the reasons stated.

Chairman Jordan. Did they really say "go get him"?

The Witness. Again, Mr. Chairman, I'm not going to respond beyond what is printed in the book.

Chairman Jordan. Did they not say "go get him"?

The Witness. I'm not going to answer your question.

BY MR. [REDACTED]

Q What was your opinion of President Trump at the time that you joined the District Attorney's Office?

A I refuse to answer your question on the basis of the rights that are outlined in the statement that I made.

Q What was your opinion of President Trump's actions as President and the policies of the Trump administration at the time you joined the District Attorney's Office?

A For the reasons indicated in my statement, I'm not going to answer your

question.

Q On page 129 of your book it states: "Nor was there any conversation about politics, about the 2020 election, the Stop the Steal shenanigans, or whether Trump needed to be prosecuted because his behavior as President was repugnant to us or others."

Sir, was the behavior of the President repugnant to you?

A Mr. [REDACTED] I respect your right to ask the question, and I hope you'll respect my right not to answer it for the reasons stated. And I refuse to answer it.

Mr. [REDACTED] We're marking as exhibit 2 some remarks of Justice Jackson.

[Pomerantz Exhibit No. 2

Was marked for identification.]

BY MR. [REDACTED]

Q Are you familiar with this speech that the Attorney General at the time and subsequently Supreme Court Justice Jackson made at the Second Annual Conference of U.S. Attorneys in April of 1940?

A I'm confident I wasn't present. But I'm not going to answer your question whether I'm familiar with the speech from having later become aware of it.

Q Okay. Are you aware that it says in the second sentence: "The prosecutor has more control over life, liberty, and reputation than any other person in America. His discretion is tremendous. He can have citizens investigated and, if he is that kind of person, he can have this done to the tune of public statements and veiled or unveiled intimations."

Are you familiar with that?

A I see it in the exhibit that you've handed me.

Q And do you agree with that statement of Justice Jackson?

A I'm not going to answer your question.

Q Justice Jackson -- Attorney General Jackson at the time -- further stated: "While the prosecutor at his best is one of the most beneficial forces in our society, when he acts from malice or other base motives, he is one of the worst."

Do you agree with that statement, sir?

A I'm not going to answer your question, Mr. [REDACTED] for the reasons indicated in my statement.

Q "There is a most important reason why the prosecutor should have, as nearly as possible, a detached and impartial view of all the groups in his community. Law enforcement is not automatic. It isn't blind. One of the greatest difficulties of the

position is that he must pick his cases, because no prosecutor can even investigate all of the cases in which he receives complaints.

"What every prosecutor is practically required to do is to select the cases for prosecution and to select those in which the offense is the most flagrant, the public harm the greatest, and the proof the most certain.

"If the prosecutor is obliged to choose his cases, it follows that he can choose his defendants. Therein is the most dangerous power of the prosecutor: that he will pick people that he thinks he should get, rather than pick cases that need to be prosecuted."

Are you familiar with that statement from the former Attorney General?

A I see it in the statement, yes.

Q And do you agree with that?

A I'm not going to answer your question.

Q "With the law books filled with a great assortment of crimes, a prosecutor stands a fair chance of finding at least a technical violation of some act on the part of almost anyone. In such a case, it is not a question of discovering the commission of a crime and then looking for the man who has committed it, it's a question of picking the man and then searching the law books, or putting the investigators to work, to pin some offense on him."

Do you agree that's a concern?

A I agree that it is reflected in the statement. Beyond that, I'm not prepared to answer your question.

Q "It is in this realm in which the prosecutor picks some person whom he dislikes or desires to embarrass, or selects some group of unpopular persons and then looks for an offense, that the greatest danger of abuse of prosecuting power lies."

Do you agree with that?

A Again, Mr. [REDACTED] I see that in the statement, and I'm not prepared to respond to the question whether I agree or disagree with it.

Q Are you familiar with the American Bar Association's Criminal Justice Standards, specifically standard 3-1.6?

A For the reasons indicated in my statement, I'm not going to respond to your question.

Mr. [REDACTED] Okay. I'd like to mark this for the record.

[Pomerantz Exhibit No. 3

Was marked for identification.]

Mr. Finzi. 3?

Mr. [REDACTED] The standard --

Mr. Finzi. Sorry. Is it exhibit 3?

Mr. [REDACTED] Exhibit 3, yes. And we're looking at standard 3-1.6, improper bias prohibited.

Section (a): "The prosecutor should not manifest or exercise, by words or conduct, bias or prejudice based upon the race, sex, religion, national origin, disability, age, sexual orientation, gender identity, or socioeconomic status. A prosecutor should not use other improper considerations, such as partisan or political or personal considerations, in exercising prosecutorial discretion. A prosecutor should strive to eliminate implicit biases, and act to mitigate any improper bias or prejudice when credibly informed that it exists within the scope of the prosecutor's authority."

Is this type of ABA standard something that the New York County District Attorney's Office follows?

Ms. Dubeck. Objection.

The Witness. I'm not going to respond to your question for the reasons

indicated in my statement.

Mr. [REDACTED] "A prosecutor's office" -- this is section (b) -- "A prosecutor's office should be proactive in efforts to detect, investigate, and eliminate improper biases."

Do you think during your time at the New York County District Attorney's Office you were proactive in your efforts to detect, investigate, and eliminate bias?

Ms. Dubeck. Objection.

The Witness. I'm not going to respond to your question.

Mr. [REDACTED] Are you familiar with the Department of Justice's --

Chairman Jordan. What is the specific objection here? Is it -- you cited, I think, three in your opening statement. Which one are you asserting?

The Witness. As to this question, I am asserting all of the bases, both the objection of the District Attorney's Office, the rights indicated in the fifth paragraph of my statement, which refer to the Fifth Amendment guarantee against --

Chairman Jordan. You're asserting -- in your opening statement, you referenced the District Attorney's Office and you may have to assert your Fifth Amendment rights. Are you asserting those now?

The Witness. I am asserting those now.

Chairman Jordan. Okay.

Mr. Issa. Could we have that in the future? Because the record is not clear when you just lump them all together. I think we'd like to know whether it's the Fifth Amendment or specific each one, because if it goes to a judge later, the judge is going to say: Which one? We should have that clear on the record if it's one, two, three, or four different ones. I think the record should be clear.

Mr. Wells. That is a fair comment.

Paragraph 4 of the statement refers to the D.A.'s objections. Paragraph 5 refers

to the Fifth Amendment. And paragraph 6 refers to his First Amendment and due process objections.

Mr. Issa. So if you could just --

Mr. Wells. So We will identify.

Mr. Issa. -- state the paragraph each time --

Mr. Wells. We will.

Mr. Issa. -- that would be great.

Mr. Wells. Right.

Mr. Issa. Thank you. The number will be sufficient.

Chairman Jordan. And could we get a copy of the statement?

The Witness. Sure.

Mr. [REDACTED] And I'll stop briefly. I just want to welcome some of the new members have that have joined us, starting with Mr. Issa.

Do you want to introduce yourself for the record?

Mr. Issa. I'm Congressman Darrell Issa. I have been in a few of these before. I'm from California.

Mr. [REDACTED] And, Chairman Schiff, down at the end of the table?

Mr. Schiff. I don't have any questions.

Mr. [REDACTED] No. I'm just introducing you.

Mr. Schiff. Oh, I'm sorry. Adam Schiff from California.

Mr. [REDACTED] And Ms. Plaskett?

Ms. Plaskett. Good morning. Stacey Plaskett from the Virgin Islands.

Mr. [REDACTED] And, Mr. Goldman, I'm sorry, sir. How are you?

Mr. Goldman. Dan Goldman, New York.

The Witness. Good morning or afternoon.

Mr. Goldman. Well, it's still morning.

Mr. [REDACTED] Okay. I'm going to mark as exhibit 4 the Department of Justice -- part of the Justice Department manual -- prosecutor's manual, "Principles of Federal Prosecution."

[Pomerantz Exhibit No. 4

Was marked for identification.]

BY MR. [REDACTED]

Q Maybe I can get you to answer this question.

You served as a Federal prosecutor, correct?

A I did.

Q And on two separate stints?

A That's correct.

Q Would you be willing to identify for the record when that was?

A Yes. I served as an Assistant United States Attorney from 1978 until 1982, and then I returned to the United States Attorney's Office for the Southern District of New York in 1997 where I served as chief of the Criminal Division until mid-1999.

Q And after your time -- in between your time, you also have served as a partner at the Paul, Weiss law firm. Is that fair?

A It was after my time as chief of the Criminal Division that I was a partner at the Paul, Weiss law firm, from March of 2000 until I withdrew from the partnership at the end of 2012.

Q Okay. And have you been a partner at any other law firm?

A Yes.

Q And would you be able to answer that question?

A I can do my best with that.

I was a partner at a small criminal defense boutique known variously as Fischetti & Pomerantz, Fischetti, Pomerantz & Russo. There was one iteration, I think, Fischetti, Feigus & Pomerantz. I was a partner in that firm from 1984 to 1990.

From 1990 to 1997, I was a partner at a law firm then known as Rogers & Wells in New York City.

And for a period of a few months at the beginning of 2000, I was a partner in what had been the Rogers & Wells firm but was from that point forward, beginning January 1st, known as Clifford Chance -- I think it was known as Clifford, Chance, Rogers & Wells for a short period of time.

And I am now a founding principal of a law firm known as the Free and Fair Litigation Group.

Q And as I understand it, you graduated law school from Harvard? Is that correct?

A No. I graduated --

Q Your undergrad was Harvard?

A I graduated undergrad from Harvard. Then I went to law school at the University of Michigan.

Q Okay. Turning back to exhibit 4. During your time at the Justice Department or since you've been with the District Attorney's Office for New York County, are the "Principles of Federal Prosecution," the U.S. Attorneys' Manual, something that you consult or consider guidelines?

Ms. Dubeck. Objection to the extent you're asking him about his office at the D.A.'s Office.

The Witness. Could I have a moment?

Mr. [REDACTED] Of course.

We'll go off the record while the witness is conferring with his counsel.

[Discussion off the record.]

Mr. [REDACTED] Back on the record.

The Witness. Yes. Thank you.

On the advice of counsel, I will continue to assert my privilege, in particular the privilege referenced in the fifth paragraph of my opening statement, which is the privilege against self-incrimination.

Also, I believe there was an objection from Ms. Dubeck with respect to the position of the Manhattan District Attorney's Office. And as I indicated in the statement, I will honor that objection and refuse to answer.

So there are several bases for refusing to answer that question.

BY MR. [REDACTED]

Q Okay. So one of the bases is your Fifth Amendment against self-incrimination about whether the District Attorney's Office follows or relies on the U.S. Attorneys' Manual as a guideline?

A Yes.

Q Did I get that right?

A You did get that right, yes.

Q Okay.

A Thank you.

Mr. [REDACTED] And as I understand it, the District Attorney's office has objected to that question, whether the D.A.'s Office considers some of these standards?

Ms. Dubeck. To the extent you're asking about the D.A. Office's considerations, yes.

Mr. [REDACTED] Okay.

BY MR. [REDACTED]

Q What was the address of the District Attorney's Office in New York County?

A One Hogan Place, New York, New York.

Q And how frequently did you go to the office when you were a special district attorney? Did you have an office physically at that address?

A The office is located in several buildings around One Hogan Place. It's not all in one contiguous space of offices. There were several office premises.

Having clarified that, I'm not going to answer your question about how often I was physically at the offices of the Manhattan District Attorney.

Q Did you have your own desk there?

A Again, I'm not going to respond to your question.

Q On the basis of what?

A On the basis of the fifth paragraph of my statement. Conveniently, Mr.

[REDACTED] the fifth paragraph relates to the Fifth Amendment.

Q Okay. So really -- so I'm just being clear, and I don't mean to --

A I understand.

Q -- mean any disrespect, but asking the question whether you had a desk at the D.A.'s Office, you're asserting the Fifth Amendment?

Mr. Wells. I think that's what he said.

Mr. [REDACTED]. Okay. Fair enough. Again, I mean no disrespect, sir.

The Witness. Now I'm sure that that's what I said.

BY MR. [REDACTED]

Q In the book on page 1, you write: "He was responsible for a grave failure of justice."

Who is the "he" in that sentence?

A Well, the book speaks for itself. I don't think there's any ambiguity of the reference.

Q The reference is to the District Attorney Bragg?

A That's how the book reads.

Q Okay. In your book you go through a rather long list of investigative avenues the New York County District Attorney's Office pursued with respect to President Trump, and you refer to the Stormy Daniels matter as the "Zombie" case? Is that correct?

Ms. Dubeck. Objection.

Mr. [REDACTED] What's the basis of that objection?

Ms. Dubeck. To me?

Chairman Jordan. You're the one that objected.

Ms. Dubeck. That you are asking about confidential work of the D.A.'s Office.

Mr. [REDACTED] Well, I'm asking about the book. There's a whole chapter called "The 'Zombie' Case."

The witness can answer the question. I guess you're not going to answer it, but --

A Well, I'm perfectly happy to acknowledge that the book references the Zombie case, and I think you are correct that one of the chapters refers explicitly to the Zombie case. Yeah, chapter 5 and chapter 3. Chapter 3 refers to the Zombie case, and chapter 5 is entitled "The 'Zombie' Case Returns to the Grave."

BY MR. [REDACTED]

Q Okay.

A I'm not sure if I've answered your question, but the book certainly contains those references.

Q And was that a case, the Stormy Daniels payment, was that something that Robert Mueller looked into, to your knowledge, and considered investigating and prosecuting?

A I'm not going to answer that question.

Q On what basis? That's more of a history question, I think.

A Yes. Let me confer for a moment with counsel.

Mr. [REDACTED] Okay. We'll go off the record.

[Discussion off the record.]

The Witness. Yes. On the advice of counsel, I will assert my rights under the Fifth Amendment.

BY MR. [REDACTED]

Q Okay. And the facts of the Zombie case, in your words, were examined by the U.S. Attorney's Office in the Southern District of New York. Is that correct?

A To the extent the book references the facts embodied in your question, I refer you to the book. But I'm not going to elaborate beyond what's stated in the book.

Q Okay.

A I'm not denying what is written in the book obviously. But I'm not going to expand beyond what's written for the reasons indicated in my opening statement.

Q Okay. And do you know why the Southern District of New York's U.S. Attorney's Office decided not to prosecute President Trump on the facts of the Zombie case?

A I'm not going to answer that question on the basis of each of the paragraphs in my statement.

Q And you stated in your book that it was during the time frame of the spring and summer of 2019, is that correct, that the U.S. Attorney's office was examining the

facts of the Zombie case?

A I'm not going to respond to your statement beyond referencing what's in the book.

Q Okay. Are you invoking the Fifth Amendment for that particular one or --

A Yes.

Q And as I understand it, the next --

A I think also the fourth paragraph of my statement.

Q The fourth paragraph. Okay.

A Which references to --

Ms. Dubeck. To the extent you're asking for knowledge he obtained at the D.A.'s Office, I object.

BY MR. [REDACTED]

Q When did you join the D.A.'s Office? You can tell us that?

A I was sworn in as a special assistant district attorney on February 2nd, 2021.

Q Okay. So the facts I'm asking you about, you know, occurred before you became affiliated with the office?

A I think we can all acknowledge that 2019 occurred before 2021.

Q Right. But did --

A So I'm not taking issue with your statement.

Q Right. But did you learn about the fact that the U.S. Attorney's Office in the Southern District of New York decided -- looked at the Zombie case, the Stormy Daniels payments, and decided not to prosecute? Did you know that information before you came to the New York County District Attorney's Office?

A I'm not going to answer your question.

Q Based on?

A The Fifth Amendment.

Q Okay.

A And the fifth paragraph of my statement.

Q Before your tenure at the District Attorney's Office, in the fall of 2019, you write in your book the office examined the facts of the Zombie case, the Stormy Daniels payment, and commissioned an outside law firm to help the office analyze these questions.

Do you know what law firm that was?

Ms. Dubeck. Objection.

The Witness. Yeah. I refuse to answer on the basis of the fourth paragraph of my statement and the fifth paragraph of my statement.

Mr. [REDACTED]. Okay.

The Witness. I'm assuming that that's clear and you don't need me to elaborate further since you have the statement.

Mr. [REDACTED] The fourth iteration of the Zombie case, the Stormy Daniels payment, you were a key player in, am I correct, as I understand your book?

Ms. Dubeck. Objection.

The Witness. Again, I will invoke my rights not to answer the question for the reasons referenced in my statement.

Mr. [REDACTED] And so the fourth iteration of the Zombie case you studied whether there was a money laundering theory to pursue?

Ms. Dubeck. Objection.

The Witness. Same answer.

Mr. [REDACTED] Which one is that? Sorry.

The Witness. I was referencing the answer I gave to the just previous question

where I think I referenced both the fourth and fifth paragraph of my opening statement.

Mr. [REDACTED] And as I understand your book -- and hopefully you can correct me if I get this wrong -- but the legal theory there was President Trump -- I guess he was candidate Trump at this time -- was a victim of extortion. Is that correct?

Ms. Dubeck. Objection.

The Witness. Same answer as to the last question, if that's acceptable.

BY MR. [REDACTED]

Q Okay. No, but I'm just asking -- I'm just trying to understand this legal theory as you write in your book.

A I understand your question.

Q Okay.

A But for the reasons indicated, I'm not going to go beyond what's stated in the book.

Q Okay. So President Trump, under the fourth iteration of the Zombie case, President Trump as a victim of extortion could be prosecuted for money laundering. Is that -- do I have that understanding right?

Ms. Dubeck. Objection.

Mr. [REDACTED] Or is that the theory you were pursuing?

Ms. Dubeck. Objection.

The Witness. I'm not going to answer the question.

Chairman Jordan. Well, you say right here in the second paragraph on page 60: "In the Trump case, this meant that Clifford had not committed larceny by extortion until she or her lawyer received the hush money payment that Michael Cohen agreed to pay on Trump's behalf."

So you write it right here in the book, but you won't answer the question when

Mr. [REDACTED] describes exactly what you wrote in the book?

The Witness. Actually, I don't think [REDACTED] question embodied what was written in the book. But in any case, I'm asserting my privileges with respect to this question.

Chairman Jordan. Did you really write the book, Mr. Pomerantz?

The Witness. Yes.

Mr. [REDACTED] And then towards the end of your tenure at the District Attorney's Office, there was a -- as I understand it from your book, and you talk about this on page 61, then page 209 -- another attempt to prosecute the Stormy Daniels Zombie matter at the end of the investigation.

Can you tell us anything about that?

Ms. Dubeck. Objection.

The Witness. I won't answer that question, and I'm relying with respect to this question on all of the rights reflected in the statement.

BY MR. [REDACTED]

Q So, if I may, I'll just read on page 209. "Because we were now contemplating an indictment that featured false business records, Carey and I" -- and who's Carey, by the way?

A I think the book references Carey as Carey Dunn.

Q Okay. "--- spoke about reviving the hush money allegations, which would bring the 'Zombie' theory back from the dead once again. The thought was to charge as false business records not only the documents relating to the SOFCs" -- which stands for statements of financial condition, is that correct, SOFC?

A I think the book defines SOFC as you've indicated. It's an abbreviation for statement of financial condition.

Q Okay. " -- relating to the SOFCs but also the phony invoices for 'legal services' that had been used to reimburse Michael Cohen for the money he had paid to Stephanie Clifford."

Do you remember that incident or that part of the case during your time at the New York County District Attorney's Office?

Ms. Dubeck. Objection.

The Witness. I refuse to answer your question for the reasons indicated.

Mr. [REDACTED] Okay. During your time at the District Attorney's Office, you also examined a number of other potential avenues to prosecute President Trump. Is that correct?

Ms. Dubeck. Objection.

The Witness. Same answer, if that's acceptable to you.

Mr. [REDACTED] You looked at several of President Trump's golf properties, the Briarcliff Golf Club, the Trump National Golf Club, the Jupiter golf course. Is that correct?

Ms. Dubeck. Objection.

The Witness. Again, I will rely on the rights articulated in paragraphs 4, 5, and 6 of my statement.

Mr. [REDACTED] You examined whether President Trump could be indicted for defrauding Deutsche Bank. Is that correct?

Ms. Dubeck. Objection.

The Witness. Same answer.

Mr. [REDACTED] Did Deutsche Bank ever indicate to you that they felt like they were a victim of fraud?

Ms. Dubeck. Objection.

The Witness. Same response. Again, I'm relying on the rights referenced in, I believe, paragraphs 4, 5, and 6 of my statement.

Mr. [REDACTED] You examined whether President Trump could be indicted in New York for papers he submitted to GSA as part of the Old Post Office Hotel that he was attempting to acquire and redevelop. Is that correct?

The Witness. Same answer. I guess same response.

Mr. [REDACTED] You examined during your time in the New York District Attorney's Office whether President Trump could be prosecuted in New York over the Trump International Hotel and Tower in Chicago?

Ms. Dubeck. Objection.

The Witness. Same response. Again, I'm trying to just save time and energy. If you want me to elaborate, I will do so.

Mr. Gaetz. Mr. Pomerantz, did you violate any person's constitutional rights while you worked at the Manhattan D.A.'s Office?

Ms. Dubeck. Objection.

The Witness. Same answer.

Mr. Gaetz. Mr. Pomerantz, did you violate any person's constitutional rights when you worked on the Trump investigation?

Ms. Dubeck. Objection.

The Witness. I have the same response to your question.

Mr. Gaetz. Did you ever violate any canons of legal ethics while you worked at the Manhattan District Attorney's Office?

Ms. Dubeck. Objection.

The Witness. The same response.

Mr. Gaetz. And did you violate any canons of legal ethics when you were

investigating President Trump?

Ms. Dubeck. Objection.

The Witness. Same response.

Mr. Gaetz. Did you violate any New York State Bar rules while you were working in the Manhattan District Attorney's Office?

Ms. Dubeck. Objection.

The Witness. Same response.

Mr. Gaetz. And did you violate any New York State Bar rules while you were investigating President Trump?

Ms. Dubeck. Objection.

The Witness. Same response.

Mr. Gaetz. Did you misuse any Federal funds while you were working in the Manhattan District Attorney's Office?

The Witness. Same response.

Mr. Gaetz. Did you misuse any Federal funds while investigating President Trump?

The Witness. Same response.

Mr. Gaetz. Did you break any laws when you worked at the Manhattan District Attorney's Office?

Ms. Dubeck. Objection.

Mr. Witness. Same response.

Mr. Gaetz. And did you knowingly break any laws when investigating President Trump?

Ms. Dubeck. Objection.

The Witness. Same response.

Mr. Gaetz. Yield back.

Chairman Jordan. When did you sign the book deal?

The Witness. I'm not going to answer your question, Mr. Chairman, for the reasons indicated.

Chairman Jordan. I'm not asking about what's in it. We already know you're not going to talk about what you said you wrote. I just want to know when you signed the agreement on the book.

The Witness. Yes. And I'm not going to answer that question in reliance on paragraphs 5 and 6 of my statement.

Chairman Jordan. When did you tell the D.A.'s Office you were thinking about writing the book?

The Witness. Likewise, not going to answer that question.

Chairman Jordan. Who's the publisher of the book?

The Witness. Simon & Schuster.

Chairman Jordan. Did they come to you or did you go to them?

The Witness. I'm not going to answer that question sir.

Chairman Jordan. Did you get an advance for the book?

The Witness. I'm also not going to answer that question.

Chairman Jordan. When did you start writing the book?

The Witness. I'm not going to answer that question either, for the reasons indicated, although I'm not referencing paragraph 4 of my statement in that regard. That's paragraphs 5 and 6.

Chairman Jordan. How did you select the title?

The Witness. The same answers.

Mr. Armstrong. In your opening statement, you said the Manhattan D.A.'s Office

warned you, you could face criminal liability.

You're asserting your -- asserting Fifth Amendment privilege.

The Witness. Yes, sir.

Mr. Armstrong. Who in the D.A.'s Office told you that?

The Witness. The reference in my statement to -- the comment that was made in open court on April 19th, I believe, was a reference to statements made by Ms. Dubeck, if I'm not mistaken.

Mr. Armstrong. So when was that? I'm sorry.

The Witness. The statement in paragraph --

Mr. Armstrong. 5?

The Witness. 4. Oh, yes, you're right, paragraph 5, says: "When we were before the United States District Court on April 19th, a lawyer from the Manhattan District Attorney's Office said that my book, quote, 'exposed me to criminal liability.'" I think the "me" should be in brackets, by the way.

That was Ms. Dubeck.

Mr. Armstrong. Has there been any follow-up since then with you directly?

The Witness. I'm not going to answer that question, sir.

Mr. Armstrong. Are you aware of an active investigation?

The Witness. I'm not going to answer that question.

Mr. Armstrong. Are you aware of any similar investigation?

The Witness. Same answer.

Mr. Armstrong. Any convictions?

The Witness. Conviction?

Mr. Armstrong. It's public record. Are you aware of any other similar convictions?

The Witness. Not of me. I can answer that.

Mr. Armstrong. Okay.

The Witness. The reference -- never mind. I'll wait for the next question.

Mr. Armstrong. All right.

Mr. [REDACTED] You also, while you were at the New York County District Attorney's Office, pursued matters at Mar-a-Lago in Florida for investigation?

Ms. Dubeck. Objection.

Mr. [REDACTED] Is that correct?

The Witness. I won't answer based on the fourth and fifth paragraphs of my statement.

Mr. [REDACTED] The Seven Springs property and the easement, conservation easement, you pursued that as an avenue to investigate or indict President Trump? Is that correct?

Ms. Dubeck. Objection.

The Witness. Same answer.

Mr. [REDACTED] You pursued the Trump property at 40 Wall Street, which is in Manhattan, correct?

The Witness. 40 Wall Street is in Manhattan.

Ms. Dubeck. Objection to the balance of the question.

Mr. [REDACTED] So the objection is to whether you pursued the 40 Wall Street as an avenue to investigate or prosecute President Trump?

The Witness. Yes. And I'm not going to answer that question.

Mr. [REDACTED] You also looked at his -- something you referred to as the triplex apartment in Trump Tower as an avenue to potentially indict or prosecute him for overstating the square footage or value of the property. Is that correct?

Ms. Dubeck. Objection.

The Witness. Same response.

Ms. Stefanik. Do you know any of the Members of Congress on this committee?

The Witness. Sorry?

Ms. Stefanik. Do you know any of the Members of Congress on this committee?

The Witness. I do not.

Ms. Stefanik. So you've never had any conversations with Dan Goldman, Adam Schiff, Darrell Issa, Jim Jordan, myself, Kelly Armstrong ever?

The Witness. I believe that's correct.

Ms. Stefanik. How long have you known Cy Vance?

The Witness. Bear with me for one moment, if you would.

Mr. [REDACTED] Go off the record?

The Witness. Yes. Thank you.

[Discussion off the record.]

The Witness. On the advice of counsel, I'll invoke my right not to answer the question under the fifth paragraph.

Ms. Stefanik. Under the Fifth Amendment?

The Witness. Yes.

Mr. [REDACTED] Of how well you know Cy Vance? Is that right?

The Witness. Yes.

Ms. [REDACTED] [REDACTED] could you wait until the noise in the hallway is gone?

Mr. [REDACTED] Absolutely. We're off the record here as we're dealing with the sound.

[Discussion off the record.]

Ms. Stefanik. Do you respect Cy Vance?

The Witness. I'm not going to answer that question. Intending no disrespect to either you or Mr. Vance --

Ms. Stefanik. So you do respect Cy Vance?

The Witness. -- I'm refusing to answer.

Ms. Stefanik. You respect Cy Vance, your public comments, your extensive respect for his tenure at the District Attorney's Office.

The Witness. Yes, I won't answer that question.

Ms. Stefanik. Yes, you won't answer it or, yes, you respect Cy Vance?

The Witness. I won't answer the question.

Ms. Stefanik. Do you view Cy Vance as political?

The Witness. I refuse to answer your question.

Ms. Stefanik. Under what basis?

The Witness. On the basis of my privilege against self-incrimination.

Ms. Stefanik. So you're asserting the Fifth Amendment?

The Witness. Yes.

Ms. Stefanik. Do you -- how long have you known Alvin Bragg?

The Witness. Same answer.

Ms. Stefanik. Fifth Amendment?

The Witness. Yes, ma'am.

Ms. Stefanik. Do you respect Alvin Bragg?

The Witness. Same answer.

Ms. Stefanik. Fifth Amendment?

The Witness. Yes.

Ms. Stefanik. Are you keeping track of how many times he has asserted his Fifth?

Do you view Alvin Bragg as political?

The Witness. I have the same response to your question.

Ms. Stefanik. And you are aware in your book you wrote very specifically on page 204 that Alvin Bragg is a political actor? I'm sorry, 264.

The Witness. Yes. The book states: "Like all elected prosecutors, Alvin Bragg is a political actor."

Ms. Stefanik. And the book also states: "He cares deeply about his progressive agenda."

The Witness. I believe you're quoting accurately from the book.

Ms. Stefanik. Quoting accurately from the book that you yourself wrote, as you just said in this deposition.

The Witness. I've acknowledged writing the book.

Ms. Stefanik. Yes.

Do you recall Alvin Bragg's 2021 campaign for District Attorney.

The Witness. Yes, I won't answer that question in reliance upon my constitutional rights as reflected in my statement.

Ms. Stefanik. The fifth paragraph, Fifth Amendment?

The Witness. And the sixth.

Ms. Stefanik. Alvin Bragg --

The Witness. Paragraph, not amendment.

Ms. Stefanik. I understand.

Alvin Bragg's campaign communicated to voters of his involvement in lawsuits targeting President Trump. Is that your recollection as a native New Yorker?

The Witness. Oh. Yeah, I won't answer that question in reliance on my Fifth Amendment rights.

Ms. Stefanik. Did you tell anyone to vote for Alvin Bragg in either the primary or general election?

The Witness. I refuse to answer that question.

Ms. Stefanik. Your book says you did. And the book is true, correct?

The Witness. The book speaks for itself.

Ms. Stefanik. And it's true?

The Witness. I'm not going to go beyond the book.

Ms. Stefanik. So there are no lies in the book? You stand fully behind this publication under your name?

The Witness. That's correct.

Ms. Stefanik. Did you know Alvin Bragg before he became D.A.? Had you ever met him before or worked with him before?

[11:06 a.m.]

The Witness. No.

Ms. Stefanik. What was your assessment of Alvin Bragg as an attorney?

The Witness. I refuse to answer that question.

Ms. Stefanik. Have you always been compensated for your legal services prior to your work for the New York District Attorney's Office.

The Witness. No.

Ms. Stefanik. What example were you not compensated? Just give us a few examples.

The Witness. I did particular matters on a pro bono basis.

Ms. Stefanik. And why did you decide not to be compensated, or not to pursue compensation in the case for the New York District Attorney's Office.

The Witness. No, I won't answer that question on the basis of my Fifth Amendment rights, insofar as it relates to my work at the Manhattan District Attorney's Office.

Ms. Stefanik. How would you describe the culture in the District Attorney's Office under Alvin Bragg.

Ms. Dubeck. Objection.

The Witness. I refuse to answer on the basis of the District Attorney's Office objection and my rights under the Fifth Amendment.

Ms. Stefanik. How would you describe the culture in the District Attorney's Office under Cy Vance.

Ms. Dubeck. Objection.

The Witness. Same answer.

Ms. Stefanik. On page 58 in your book -- which you have said your book is

accurate and factual, "My creative theorizing smacked into District Attorney New York's cautious and conservative culture, as it would several times during my tenure."

So you had challenges working through the culture of the District Attorney's Office?

Ms. Dubeck. Objection.

The Witness. I won't go beyond what is written in the book in responding to your question. I believe you --

Ms. Stefanik. Accurately quoted it?

The Witness. Accurately quoted it, yes.

Chairman Jordan. What about the day one memo? What are your thoughts on that?

The Witness. I refuse to answer that question on the basis of my Fifth Amendment rights.

Mr. Goldman. Sorry. Which rights?

The Witness. My Fifth Amendment rights.

Mr. Goldman. Are you invoking the paragraph six with respect to legislative purpose as well?

The Witness. Yes.

Chairman Jordan. I think it's our hour.

██████████

BY MR. ██████████

Q On page 22 of your book, you referred to President Trump as an "unscrupulous wheeler-dealer. Is that correct?

A Bear with me one moment, if you would.

Did you say page 26?

Q 22.

A 22.

The book indicates, I'm quoting, "I had heard stories 35 years earlier from lawyers who had represented Trump in his business dealings, and I took from those stories that he was an unscrupulous wheeler-dealer."

Q On page 23, you state, "I was not a fan."

A That's a correct -- that line would appear in the book, and you've accurately quoted.

Q On page 98, you refer to the President's "narcissistic personality."

A Correct.

Q On page 99, you state, "Trump was incredibly cheap and completely dishonest."

A That's not correct. The language you are quoting omits the introduction to that --

Q Okay. Fair enough.

A -- verbiage. That is what -- the book indicates that Cohen -- the reference there is to Michael Cohen.

Q Okay.

A Cohen -- again, I'm quoting here, "Cohen also told us that Trump was incredibly cheap and completely dishonest in many of his business dealings."

So in this respect, the book is reciting what information had been relayed by Michael Cohen.

Q On page 103, your book states, "Trump, though, was not just a pathological liar, but a hapless, arrogant, and horrible liar." Is that correct?

A It's correct that that is -- yes, the book -- you've accurately quoted from the

book.

Q On page 109, there's a reference to President Trump being a "bully."

A The book contains that reference, yes, sir.

Q I believe you state -- the sentence says, "He was also a bully who cultivated a reputation as a tough guy."

A You've accurately quoted from the book.

Q On the same page, you go on to compare President Trump to John Gotti, the head of the Gambino organized crime family. Is that correct?

A There is a reference to Mr. Gotti, and the book speaks for itself in that regard.

Q Okay.

Mr. Issa. May I ask a quick question?

Mr. [REDACTED] Okay.

Mr. Issa. A few minutes ago, the congresswoman asked you, and you answered that you stand fully behind the book. The book is correct. Do you remember saying that?

The Witness. I do.

Mr. Issa. So you didn't take your -- you waived your Fifth Amendment, and answered the question that the book in its entirety is correct.

My only question to you is, will you answer individual questions since you answered that the entire book is correct? You didn't say it speaks for itself. You said it's correct.

So having answered once that the book is correct, could you please answer for the counsel specifics of if something is correct or not correct? I don't understand where the nuance is.

The Witness. Can we have a moment?

Mr. Issa. Yeah.

[Discussion off the record.]

Mr. [REDACTED] Back on the record?

Mr. Finzi. Is there a question pending?

Mr. [REDACTED] Mr. Issa asked whether he would -- you said -- you know, you testified today that the book is accurate in response to Ms. Stefanik.

And Mr. Issa just asked -- Mr. Issa can jump in if I --

Mr. Issa. If the book is accurate in its totality, then why are you not answering individual questions about accuracy? Or can we take that the answer in every case is yes, yes, and yes?

Mr. Finzi. With all respect, we indicated at the beginning that we were not going to debate assertions of privilege. We are asserting the privilege. We are not going to debate whether it's appropriate or not.

Mr. Issa. I'm sorry. The Fifth Amendment and it being waived or not waived is fairly clear. If you answer a question related to something, and you've answered it, then a follow-up is based on the waive as to that.

Now, if your client wants to reengage and simply say, I now am in peril having said that the book is correct, and you now want to take the Fifth every other time, we'll understand.

But I just wanted to clarify, because he had answered that every single nuance of this book effectively by saying the book is correct. He's been very careful with his words. I simply wanted to point that out and ask, would he answer questions that the counsel is asking that are a breakdown of Ms. Stefanik's question?

Mr. Wells. So the record is clear, I will direct him not to answer any questions.

There is no intent to waive the Fifth Amendment in any respect. The book speaks for himself. But I understand your -- I understand your argument.

And as we said at the beginning, the time and place to debate the merits of any of these arguments will be if and when we get in front of a court.

Ms. Dubeck. And I think you have restated the question differently than it was asked. But to the extent --

Mr. Issa. Could we have it read back? I think that's worth our time.

Mr. [REDACTED] Can we go off the record?

[Discussion off the record.]

Mr. [REDACTED] Okay. Back on the record.

Ms. Dubeck. To the extent that was the import of the question, I object.

Mr. Gaetz. Mr. Pomerantz, do you know --

Mr. Issa. He answered.

Ms. Dubeck. Yes. It's on record.

Mr. Issa. The cat is out of the bag.

Mr. Gaetz. Mr. Pomerantz, do you know what a subject matter waiver is relative to the Fifth Amendment?

The Witness. I'm not going to debate my understanding of the Fifth Amendment with you, sir.

Mr. Gaetz. But you've heard of a subject matter waiver before, right?

The Witness. I'm not going to indicate my knowledge of the Fifth Amendment and its application.

Mr. Gaetz. I yield back.

BY MR. [REDACTED]

Q Getting back to the John Gotti statement on page 109, you write in your

book -- which you've indicated to Ms. Stefanik as true -- "In my career as a lawyer, I had encountered only one other person who touched all of these bases: John Gotti, the head of the Gambino organized crime family and the so-called Teflon Don."

Is that a fair reading of your book?

A Yes, you read it accurately.

Q On page 112, you refer to the President as "a master of breaking the law."

Did I get that correct?

A The full sentence is, "Trump had become a master of breaking the law in ways that were difficult to reach."

Q On page 176 and 177, you write, "I saw him as a malignant narcissist, and perhaps even a megalomaniac who posed a real danger to the country and to the ideals that matter to me. His behavior made me angry, sad, and even disgusted."

Did I read that correctly? Is that what you wrote about President Trump?

A You read it correctly. You omitted the following sentence, which reads that "On a professional level, I could not allow my emotional reaction to Trump to affect my activities. It was completely irrelevant."

Q And is that true? Did your feelings about President Trump affect your work at the New York County District Attorney's Office where you were working for free?

Ms. Dubeck. Objection.

The Witness. I won't go beyond the statement in the book.

BY MR. [REDACTED]

Q On page 186, you posit the question of whether Former President Trump was suffering from some sort of mental condition that made it impossible for him to distinguish between fact and fiction.

Is there a mental condition that you're aware of that makes it difficult for

individuals that are afflicted with such a mental condition to distinguish between fact and fiction?

A I refuse to answer your question, Mr. [REDACTED] on the bases indicated in my statement.

Q On page 220 --

Mr. Issa. Are we back to paragraph five again?

The Witness. Paragraph five and paragraph six.

Mr. Issa. Okay.

Mr. Wells. So the record is clear -- and I respect the Congressman's concern -- every objection or refusal to answer today has included paragraph five, the Fifth Amendment. There are some objections where, in addition to the Fifth Amendment, paragraph four, which is the prosecutor's objection, or paragraph six, proper legislative purpose.

But every objection today -- so there's no confusion, so we're all on the same page -- involves paragraph five, an assertion of the Fifth.

Mr. Issa. The only reason I'm asking --

Mr. Wells. Oh, I understand. I actually agree with you.

I would urge my client --

Mr. Issa. If we could assert four, five, six, or five, six, so that we know what we're --

Mr. Wells. You and I are on the same page.

Mr. Issa. I love the shortcut, though.

Mr. Wells. Okay.

BY MR. [REDACTED]

Q On page 225, you, in your book, write, "I was worried I'd become a Johnny

One Note, always arguing the reasons for prosecuting Trump until I was blue in the face and nobody wanted to hear from me anymore."

Or I'm sorry. I read that incorrectly. "And nobody wanted to hear me anymore."

Did I read that correctly, at least the second time?

A Yes. Yes, sir.

Q And was that true?

Ms. Dubeck. Objection.

Ms. Stefanik. The book is true. He has already answered that the book is true.

The Witness. The book speaks for itself.

Mr. [REDACTED] Mr. Jordan?

Chairman Jordan. On page 170 of the book, you say, "I thought there might be an argument that Trump" -- and you're referring to President Trump there -- "having assumed an office that required him to take care that the laws be faithfully executed, and having urged the country to trust him to uphold the law, should be held to a higher standard." And the word "higher" is in a different font.

Do you really believe that? Because in the very next paragraph, you say -- you quote our second President, and you say, "We're a Nation of laws and not men," and then "No one is above the law, to the equal treatment of the law."

And I'm trying to figure out which statement do you believe.

The Witness. I am not understanding why you believe there is a tension between those statements.

Mr. [REDACTED] Let me refer you --

Ms. Stefanik. Why do you believe there's no tension between those statements?

Chairman Jordan. Is it equal treatment under the law, or it Donald Trump held

to a higher standard than everyone else in the county -- every other citizen in the country?

The Witness. I'm not going to go beyond my book. I think the intent of the language is plain.

Mr. Issa. What reason are you not going beyond the statement that you made?

The Witness. Because I'm not required to do so.

Mr. Issa. Under what?

The Witness. Under either the Fifth Amendment or, in my view, the First Amendment and the due process clause of the Fifth Amendment as well, which indicates, as I understand it, that I cannot be punished for refusing to answer questions that are -- that relate to activities and views that are protected by the First Amendment.

BY MR. [REDACTED]

Q Just to put a final point on what Mr. Jordan was getting at, on page 260, you write, "In my mind, the same evidentiary standard should apply to Presidents and paupers alike."

And I think Mr. Jordan was trying to make the point that, on 170, you wrote, "I thought there might be an argument that Trump, having assumed an office that required him to take care that the laws be faithfully executed, should be held to a higher standard of personal conduct."

Isn't that --

Chairman Jordan. Yep.

Ms. Dubeck. To the extent you're asking about his thinking while he was at the District Attorney's Office, I object.

Chairman Jordan. We're asking about the thinking he articulated in his book.

Mr. Issa. If you don't mind, if you're going to object, will you also instruct the

witness not to answer?

Ms. Dubeck. I was told I am not allowed to instruct the witness --

Mr. [REDACTED] Yeah, we have an agreement where she is not going to do that.

Mr. Issa. Oh, I apologize. Thank you.

Mr. Finzi. Is there a question pending?

Mr. [REDACTED] Yes.

Mr. Finzi. What is it?

Mr. [REDACTED] I was referring, on page 260, he states, "In my mind, the same evidentiary standard should apply to Presidents and paupers alike." But on page 170, he writes that there might be a higher standard of personal conduct for President Trump.

I'm asking the witness to reconcile those two statements.

The Witness. I refuse to answer your question on the basis of the fifth paragraph of my statement and the sixth paragraph.

Mr. [REDACTED] Okay. I believe our hour is up.

Mr. Finzi. Okay. Is this a good time for a break?

Mr. [REDACTED] Yes, sir. We'll go off the record.

[Recess.]

Ms. [REDACTED] Good morning. We can go back on the record. It's 11:46.

Mr. Pomerantz, thank you, again, for joining us.

BY MS. [REDACTED]

Q In the first hour, you talked through your length of service as a prosecutor prior to joining the Manhattan District Attorney's Office.

Can you remind me again how many years you served as a prosecutor?

A I served 6 years en toto as a Federal prosecutor, one stint for 4 years, and then for just shy of 2 years as criminal division chief.

Q And during that time period, did you ever face discipline for committing any type of prosecutorial misconduct?

A No.

Q Okay. And then after you left public service -- or, I guess, between your public service stints, you were in private practice, right?

A Yes.

Q Did you ever face discipline for violating any provision of the New York State Bar code of ethics?

A No.

Q What about any other bar rules?

A No.

Q For any other jurisdiction?

A I did not.

Q Okay. What day did you resign from the Manhattan District Attorney's Office?

A February 23rd, 2022.

May I have one moment?

Q Sure.

Ms. [REDACTED] We can go off the record.

[Discussion off the record.]

Ms. [REDACTED] We can go back on.

The Witness. I understood your question to relate to the period prior to my service at the Manhattan District Attorney's Office?

BY MS. [REDACTED]

Q Correct. Correct. Prior to your service at the Manhattan District

Attorney's Office.

A Yes. Thank you.

Q And also with respect to the violation of have you violated any provision of the bar code of ethics or any other legal ethics requirements prior to your service with the Manhattan District Attorney's Office.

A Yes, that's how I understood your question.

Q Okay. And I'm sorry. You resigned from the District Attorney's Office on what day?

A February 23rd, 2022.

Q Okay. And before you resigned on February 4th, 2022, you made a presentation to the District Attorney's Office, correct?

Ms. Dubeck. Objection.

The Witness. Yes. I'll refuse to answer on the same basis that I indicated previously.

BY MS. [REDACTED]

Q Okay. And during that presentation -- this is from page 221 of your book -- you said that you made this presentation to all of the prosecutors involved in this matter, and you, quote, "began by pointing out the fabrication of values in the SOFCs had been pervasive, substantial, and continuous over many years," right?

Ms. Dubeck. Objection.

The Witness. I have the same response --

BY MS. [REDACTED]

Q Understood.

A Although I acknowledge the statement you read from the book, which reads, "En toto, I began by pointing out that the fabrication of values in the SOFCs had been

pervasive, substantial, and continuous over many years."

Q And we talked through earlier in the first hour and it's clarified in your book that SOFC stands for statements of financial condition, correct?

A That is correct.

Q I want to talk through some examples briefly of the statements of financial condition and the references to -- I'm sorry -- the references of values assigned to Mr. Trump's golf courses.

On page 150 of your book, you say that "Trump had bought the Jupiter golf course" -- which is, I believe, a reference to the Jupiter Florida golf course -- "in December 2012 for 5 million, but it was reflected on the backup materials to the 2013 SOFC as being worth \$62 million as of June 30th, 2013," correct?

Ms. Dubeck. Objection.

The Witness. I refuse to answer your question on the basis of the rights referenced in my statement. In this instance, with respect to all of the rights referenced in the statement.

BY MS. [REDACTED]

Q Understood. You continue on on pages 150 to 151 to describe an accounting scheme, potentially, that Mr. Trump engaged in.

And then on page 151, you say that, through this scheme, Trump was able to claim, quote, "a low value when dealing with the tax assessor, but a vastly higher value in the financial statement that was given to his bankers," correct?

Ms. Dubeck. Objection.

The Witness. Same answer.

BY MS. [REDACTED]

Q Okay. On the following --

Mr. Goldman. Same answer, meaning it was accurately read from the book, but you're not going to expand on it?

The Witness. That's true, although I note the book makes a reference to, as Michael Cohen had testified, Trump was claiming a low value in dealing with the tax assessor, and then it goes on from there.

BY MS. [REDACTED]

Q And it says up above that, "The bottom line was that the numbers on Trump's 2013 financial statement included a purported value for the Jupiter golf course of 62 million. Trump had paid only 5 million to buy it just a few months earlier, and he later sued the Palm Beach County tax authorities, arguing that they should have respected the fact that he bought the property in an arm's-length transaction for only \$5 million," correct?

Ms. Dubeck. Objection.

The Witness. And I'm refusing to answer that question for the reasons indicated.

BY MS. [REDACTED]

Q Okay. On the following page, you discuss Trump's triplex apartment.

You say that "Trump's statements of financial condition" -- SOFCs -- "for 2015 and 2016 reported the value of the apartment at \$327 million, an amount much higher than the price anyone has ever paid for a private residence in the United States from the beginning of the country through 2021," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q Okay. And you continue on and say, "The accounting backup for the valuation of Trump's triplex reflected that its value over \$300 million was based largely on

its reported size of 30,000 square feet," correct?

Ms. Dubeck. Objection.

The Witness. Same answer.

BY MS. [REDACTED]

Q Okay. And then you go on and you say that there was an article published in Forbes that reported that the Trump triplex was actually just shy of 11,000 square feet," correct?

Ms. Dubeck. Objection.

A Same response.

BY MS. [REDACTED]

Q And you say that on the basis of expert valuations, your experts later pegged the actual reasonable value of the triplex at roughly \$16 million, correct?

Ms. Dubeck. Objection.

The Witness. Same answer.

BY MS. [REDACTED]

Q So in these paragraphs, you lay out a scheme where Mr. Trump initially valued his apartment at \$327 million and said it was 30,000 square feet, but in fact, you have evidence or you obtained evidence showing that the apartment was actually 10,996 square feet and was valued at roughly \$60 million, correct?

Ms. Dubeck. Objection.

The Witness. Same response.

[Discussion off the record.]

The Witness. I should make clear, in respect of these questions where the district attorney has objected, I am asserting rights referenced in both the fourth and the fifth paragraph of my opening statement?

BY MS. [REDACTED]

Q Understood. You --

A And the sixth paragraph as well.

Q On page 186 of your book, you describe Trump's valuations from Mar-a-Lago, and you say, "Trump's valuations from Mar-a-Lago in the 7 years reviewed in detail by our experts had exceeded the actual reasonable value of the property by an average of more than 1,000 percent per year," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q Okay. I want to turn back to the discussion about the February 4th meeting, which is on page 221.

You say that "Our experts" -- meaning the experts with the Manhattan District Attorney's Office -- "had put together some charts with yearly statistics on the purchase and sale of golf properties," correct?

Ms. Dubeck. Objection.

BY MS. [REDACTED]

Q It says, the charts apparently showed that, quote, Trump's valuations with his golf courses were literally off the chart, correct?

The Witness. Same response.

Ms. Dubeck. Objection.

The Witness. I'm sorry. I should have waited for Ms. Dubeck to object. But no harm done.

BY MS. [REDACTED]

Q You say, "I argued that he had to have known this because he was a real

estate entrepreneur in the business of building, owning, and running golf courses, just as he surely knew that the apartment he built and in which he lived had not contained 30,000 square feet," correct?

Ms. Dubeck. Objection.

The Witness. I refuse to answer for the reasons previous stated.

BY MS. [REDACTED]

Q And you continue on, "The brazen, pervasive, and outlandish nature of the overvaluations, I argued, was important proof of Trump's intent," correct?

Ms. Dubeck. Objection.

The Witness. Same answer.

BY MS. [REDACTED]

Q And you say that -- in the February 4th presentation, you continued on, "I then spoke about the evidence tying Trump to the preparation of the financial statements," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q Okay. You say that "I noted that the SOFCs on their face were directed to Trump, contained language saying that he was responsible for their preparation and presentation, and repeated over and over that the valuations had been, quote, "prepared by Mr. Trump," end quote, working in conjunction with others, correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q "The assets described in the SOFCs were the assets that Trump had spent his

business life to build and acquire. Trump, as a person obsessed with his wealth and net worth, surely had familiarized himself with the SOFCs and how they had been prepared," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q "And he had certified time and again that the SOFCs had accurately presented his financial condition."

Ms. Dubeck. Objection.

The Witness. I refuse to answer for the reasons stated.

BY MS. [REDACTED]

Q You continue on, "I next displayed some documents reflecting Trump's review of the financial statements and addressed some witness testimony that we had gathered from the Attorney General or civil case files."

You said, "The testimony established that Weisselberg and Trump had reviewed the SOFCs before they were finalized, and at least some of the valuations had come directly from Trump, though Weisselberg and Jeff McConney, the Trump organization comptroller, had been key players," correct?

Ms. Dubeck. Objection.

The Witness. I refuse to answer.

BY MS. [REDACTED]

Q You then describe some of the admissions that came out in a defamation case brought against Mr. Trump by an individual named Tim O'Brien. You say, During that defamation case, quote, "Trump did not distance himself from the asset values in the financial statements. On the contrary, he complained that they were too low," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q You say, "I emphasized Trump's extraordinary control over the Trump organization, financial workings, including his personal signing of checks, close review of expenses, and approval of the financial terms on which every new member joined one of his golf clubs," correct?

Ms. Dubeck. Objection.

The Witness. I refuse to answer your question.

BY MS. [REDACTED]

Q You continue on, "During the presentation, you next turned to Trump's history of making up facts regarding his wealth. I spoke about the evidence we had received from Jonathan Greenberg, including the John Barron tapes, and Trump's correspondence with the Forbes staff regarding his wealth," correct?

Ms. Dubeck. Objection.

BY MS. [REDACTED]

Q And the John Barron tapes is a reference to language earlier in your book reporting on an interaction that Trump had had with Jonathan Greenberg, a reporter who worked at Forbes Magazine, correct?

Ms. Dubeck. Objection.

The Witness. I won't answer that question.

BY MS. [REDACTED]

Q Okay. And the description given in your book is that "Mr. Greenberg had taped a conversation in which Trump had falsely passed himself off as John Barron, a vice president and finance officer working for the Trump family. In fact, there was no John

Barron. Only Trump posing as Mr. Barron," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q Back to page 223, you say in your presentation, "I also alluded to the information that Forbes had made public regarding Trump's net worth obsession, his admission that he had tried to mislead Forbes about his wealth, and his statement that a high net worth, was quote, "good for financing," end quote, correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q You continue on, "I argued that the back-and-forth that Trump had with Forbes over the years on which the magazine had reported had put Trump on notice that his asset values were unreasonable," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q And you say, "Yet the pattern continued, and Trump had not taken any of the steps he could have taken if he wanted to ensure their accuracy," correct?

Ms. Dubeck. Objection.

The Witness. I refuse to answer for the reasons indicated.

BY MS. [REDACTED]

Q You say, "I then turned to Trump's many public statements and tweets about his wealth, noting that those statements helped prove that the size of his net worth was of central importance to Trump's public persona," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q Okay. So getting back to your February 23rd, 2022 resignation, you wrote a letter before you resigned, correct?

Ms. Dubeck. Objection.

Mr. Goldman. It's a simple fact. It's public.

The Witness. May I have a moment?

Ms. [REDACTED] Sure.

Ms. Dubeck. Our position was that the letter should not be published.

Objection.

The Witness. May I have a moment with counsel?

Ms. [REDACTED] We can go off the record.

[Discussion off the record.]

Mr. Goldman. Can we go back on the record?

Your position is also that the book shouldn't have been published, but we've acknowledged the existence of the book, and we've discussed the contents of the book as being the same thing for his letter of resignation. The fact of his letter of resignation can't undo the fact of his letter of resignation.

Ms. Dubeck. Submit it to the fact and reask the question.

BY MS. [REDACTED]

Q Okay. Prior to your resignation, you wrote a resignation letter, correct?

A I wrote a resignation letter.

Q Okay. And that resignation letter is included in your book at pages 248 to 251, correct?

A The book speaks for itself.

Q I want to turn to page 248.

The resignation letter reads, "I write to tender my resignation as a special assistant district attorney and to explain my reasons for resigning. As you know from our recent conversations and presentations, I believe that Donald Trump is guilty of numerous felony violations of the penal law in connection with the preparation and use of his annual statements of financial condition," correct?

Ms. Dubeck. Objection.

The Witness. I'm not sure what the question is. If the question is whether that language was included in the resignation letter which appears in the book, the book speaks for itself, and that language does appear.

As you understand, I hope, I'm not going to go beyond the language reflected in the letter or ask -- answer questions about it. But the letter is set forth in the book, and I acknowledge having written the letter.

BY MS. [REDACTED]

Q So to clarify for the record, do you believe that Donald Trump is guilty of numerous felony violations of the penal law in connection with the preparation and use of his annual financial statements -- I'm sorry -- his annual statements of financial condition?

Ms. Dubeck. Objection.

The Witness. I'm not going to comment about the letter beyond acknowledging that it was written and it appears in the book.

Mr. Goldman. Can you review the letter and tell us if there's any reference in the letter to a case against Donald Trump related to a charge of falsifying books and records?

[Discussion off the record.]

Ms. Dubeck. I object to the question.

Mr. Goldman. Based on what?

Ms. Dubeck. Asking for words beyond what is in the letter -- the intent behind the letter.

Mr. Goldman. We're just asking whether those words are in the letter or not as he sits here and reads the letter.

The Witness. Are the words "falsifying business records" in the letter?

Mr. Goldman. Yes. Books and records, specifically.

The Witness. The letter referred to financial statements as false. It does not use the language "false books and records."

Mr. Goldman. Does it reference Stormy Daniels or Stephanie Clifford?

The Witness. The letter does not reference Stormy Daniels or Stephanie Clifford.

BY MS. [REDACTED]

Q And to clarify, your February 4th, 2023 presentation -- nowhere in your book does it say that that presentation referenced Stephanie Clifford or Stormy Daniels, correct?

A Again, I think the book speaks for itself in that regard, and I'm not going to provide editorial comment to it.

Mr. Goldman. It's just a factual question, not an editorial question.

The Witness. As a factual matter, you are correct, sir.

Ma'am. Sorry. Ma'am and sir.

BY MS. [REDACTED]

Q In your letter, you say that "In fact, Mr. Vance concluded that the facts warranted prosecution, and he directed the team to present evidence to a grand jury and

to seek an indictment of Mr. Trump and other defendants as soon as reasonably possible," correct?

A The letter contains that language, and you've read it accurately.

Q Okay. And the reference to presenting evidence to a grand jury and seeking an indictment of Mr. Trump, that's a reference to the evidence involving inflated property values, correct?

Ms. Dubeck. Objection.

A Well, I won't enlarge on the meaning of what is written in the letter.

BY MS. [REDACTED]

Q Okay.

A I'm not taking issue with your reading of it, but I'm not going to comment further.

Q Okay. You say that after Mr. Bragg took office, he decided not to pursue that financial -- that inflation of properties case. And you say, "I do not question your authority to make it" -- meaning this decision -- "and I accept that you have made it sincerely. However, a decision made in good faith may nevertheless be wrong," correct?

A That language appears in the letter, and the letter appears in the book.

Q And you continue on, "In my view, the public interest warrants the criminal prosecution of Mr. Trump, and such a prosecution should be brought without any further delay," correct?

Ms. Dubeck. Object to anything beyond what is in the letter, what is printed in the book.

The Witness. And I won't go beyond what is printed in the book and in the letter.

BY MS. [REDACTED]

Q And then in the second-to-last paragraph on page 250, you say, "To the extent you have raised issues as to the legal and factual sufficiency of our case and the likelihood that a prosecution would succeed, I and others have advised you that we have evidence sufficient to establish Mr. Trump's guilt beyond a reasonable doubt, and we believe that the prosecution would prevail if charges were brought and the matter were tried to an impartial jury," correct?

Ms. Dubeck. Objection.

The Witness. Same response.

BY MS. [REDACTED]

Q Okay. That, again, was a reference to a criminal -- potential criminal charges based on Mr. Trump's alleged inflation of property values, correct?

Ms. Dubeck. Objection.

The Witness. I won't go -- I won't elaborate beyond the language of the letter as it appears in the book.

BY MS. [REDACTED]

Q Okay. Mr. Pomerantz, is it accurate that you resigned because District Attorney Bragg would not pursue the case that you believe you had made out?

Ms. Dubeck. Objection.

The Witness. Same answer.

Mr. Goldman. What was the objection?

Ms. Dubeck. That his decision-making and thinking at the time he resigned was based on confidential and privileged information.

The Witness. I think I already responded to that question.

BY MS. [REDACTED]

Q Okay. We're going to move on from your book, sir.

Are you familiar with Bragg v. Jordan, which is Southern District of New York case number 123-CV-3032-MKV?

A May I have a moment?

Ms. [REDACTED]: We can go off the record.

[Discussion off the record.]

Ms. [REDACTED]: We can go back on the record.

The Witness. I am familiar with the lawsuit you referenced in your question.

BY MS. [REDACTED]

Q Okay. You submitted a declaration in that lawsuit, correct?

A That is correct.

Ms. [REDACTED] Okay. I want to introduce this as Exhibit No. 5.

Mr. Finzi. Number five?

Ms. [REDACTED] Number five.

[Pomerantz Exhibit No. 5

Was marked for identification.]

BY MS. [REDACTED]

Q In paragraph three of this declaration, you state that you were sworn in as a special district attorney in New York County on February 2nd, 2021, correct?

A Yes.

Q And I think you testified earlier that that is the date that you were sworn in, correct?

A That is correct.

Q Okay. And in that same paragraph, you state that you resigned from this position on February 23rd, 2022, correct?

A Yes.

Q Okay. And you testified earlier that that is accurate? You did, in fact, resign on February 23rd, 2022?

A I did, in fact, resign on February 23rd, 2022.

Q District Attorney Bragg took office on January 1st, 2022, correct?

A Yes.

Q So doing the math, this means that your tenure at the District Attorney's Office overlapped with his time there for only about maybe 8 weeks, correct?

A Yes. Our tenures overlapped from January 1st to February 23rd, 2022.

Q And the grand jury indicted Mr. Trump in the case brought by the Manhattan District Attorney's Office on March 30th, 2023, correct?

A I believe that's correct.

Q So that was more than 13 months after you had left the District Attorney's Office, correct?

A Yes, ma'am.

Q Okay. Paragraph four of your statement in your declaration, reads, "I have had no conversations about prosecuting Mr. Trump with the district attorney or any member of the prosecution team following my resignation," correct?

A You've accurately read from my declaration.

Q And is that an accurate statement?

A I'm not going to go beyond the words of the declaration. As you see from the declaration, it was submitted under penalty of perjury.

I'm not suggesting by my answer to you that there's anything in the declaration that was false, but I'm not going to enlarge upon the declaration in answering questions today for the reasons reflected in my statement.

Q Okay.

Mr. Goldman. Mr. Pomerantz, can I just clarify?

The Witness. Yeah.

Mr. Goldman. Because this is obviously long after your tenure in the District Attorney's Office.

The Witness. Right.

Mr. Goldman. So you don't -- you can't opine about whether you've had any conversations with any member of the District Attorney's Office, the prosecutors, after you left the District Attorney's Office?

The Witness. My counsel wants to say something, and I have learned not to disrespect his desire to speak.

Mr. Wells. We are not going to get into discussions about explanations about what he can do and can't do or should do and doesn't do.

You can respond to the question.

The Witness. I no longer have the question in mind. My apologies.

Mr. Goldman. What objection are you asserting?

The Witness. It's been suggested to me that I'm asserting my rights under the Fifth Amendment, and that's what I'll do.

BY MS. [REDACTED]

Q According to public press reports, the decision to pursue the hush-money case in particular was made in July, 2022, which is approximately 5 months after you left, correct?

A I'm not familiar with that.

Ms. [REDACTED] Okay. We want to introduce for the record a New York Times article. It's published March 31st, 2023, updated April 4th, 2023. It's entitled, "How

Alvin Bragg resurrected the case against Donald Trump."

[Pomerantz Exhibit No. 6

Was marked for identification.]

BY [REDACTED]

Q And I'll give you a minute to review. Let me know when you're --

A I got distracted by my photograph. Apologies. I'll keep going.

Yes. What's your question?

Q So the fifth paragraph on the first page, fifth paragraph of the article overall, says that, "But by July" -- referring to July 2022 -- "Mr. Bragg had decided to assign several additional prosecutors to pursue one particular strand that struck him as promising, a hush-money payment made on Mr. Trump's behalf to a porn star during the final days of the 2016 Presidential campaign."

That's what the article says, right?

A Where are you referencing?

Q That is the fifth paragraph on the first page. It begins, "for a time."

A I see it. Yes. Yeah, I see that.

Q So according to this public reporting, Mr. Bragg elected to pursue the hush-money case in July 2022, which was, again, several months after you left the District Attorney's Office, correct?

A I see that referenced in the article, certainly.

Q Okay. So assuming the dates here are correct, that was at least 4 months after you left the District Attorney's Office, right?

A I left in February. This references July of the same year.

Q Okay. You have no nonpublic information about Mr. Bragg's decision to pursue this case after you left the District Attorney's Office, correct?

A I refuse to answer that question.

Mr. Goldman. Based on?

The Witness. Based on my lawyer telling me not to answer the question, which I assume was based on the Fifth Amendment.

Mr. Wells. Correct.

Mr. Goldman. Based on the Fifth Amendment?

Mr. Wells. That's what he said.

Mr. Goldman. No, it's what you said. What is the rationale?

Mr. Finzi. We're not arguing.

Mr. Wells. Same rules for both sides. Today's not the day for explanations. If we ever get to court, we'll explain.

BY MS. [REDACTED]

Q Mr. Pomerantz, you said you have no public -- no nonpublic -- you declined to answer our question regarding whether you have any nonpublic information about Mr. Bragg's decision to pursue the case.

You have no nonpublic information about what evidence the district attorney may have developed in that investigation in the time since you left his office, correct?

A Same answer.

Q You're objecting to answer?

A Yes.

Q Okay. And you also would have no personal knowledge of the district attorney's use of Federal forfeiture funds, correct?

A Bear with me for one moment.

Ms. [REDACTED] We can go off the record for a minute.

[Discussion off the record.]

Ms. [REDACTED] We can go back on the record.

BY MS. [REDACTED]

Q The question is, you have no personal knowledge of the district attorney's use of any Federal forfeiture funds, correct?

A I have no knowledge one way or the other about the use of Federal forfeiture funds. I know nothing about that.

Q Okay.

Mr. Goldman. Do you have -- do you know the entire universe of evidence in possession of the district attorney that is related to the case that was charged on March 30th?

The Witness. Respectfully, I won't answer that question, Mr. Goldman, on the basis of my Fifth Amendment rights.

Mr. Goldman. Do you have any reason -- are you aware that Mr. Bragg has made public statements that his office developed additional evidence related to the case that he charged after you left the office? Are you aware of public reporting to that effect? Public statements that Mr. Bragg made?

The Witness. Respectfully, I refuse to answer your question.

Mr. Goldman. Do you have any reason to disagree with any public reports and public statements by Mr. Bragg that his office developed additional evidence related to the case that had been charged after you left the office?

The Witness. Same response.

Mr. Goldman. The charge that was brought on March 30th is not the charge that you recommended Mr. Bragg bring in February of 2022. Is that right?

Ms. Dubeck. Objection.

The Witness. Same response. Relying on paragraphs four and five of my

statement.

Mr. Goldman. You talk about your investigation in the book extensively. And as we discussed, that investigation, you stated in your book, relates to the misevaluation of properties in possession of Donald Trump. Is that correct? Is that an accurate statement of what you say in your book?

The Witness. I'm not taking issue with your statement. But respectfully, the book speaks for itself at some length, and I'm not going to characterize or comment on your reading of it.

Mr. Goldman. Sure.

I'll note for the record that the book solely talks about a misevaluation case, not the false books and records case that was charged.

Mr. Pomerantz, you aren't a big fan of Mr. Bragg, are you?

The Witness. I will decline to answer your question.

Mr. Goldman. Which one?

The Witness. Whether I'm a big fan of --

Mr. Goldman. No, which reason?

The Witness. Paragraph five of my response and six.

[12:25 p.m.]

Mr. Goldman. You thought that he should have charged the case that you investigated, correct?

Ms. Dubeck. Objection.

Mr. Goldman. He didn't charge the case you investigated, did he?

Ms. Dubeck. Objection.

The Witness. I think what he charged is a matter of public record, about which I'm not going to comment further.

Mr. Goldman. But that wasn't the case that you investigated, was it?

Ms. Dubeck. Objection.

Mr. Goldman. That wasn't the case you recommended he charge, was it?

Ms. Dubeck. Objection.

The Witness. I won't answer that question.

Ms. [REDACTED] Turning back to your April 17th declaration. Paragraph 5 of that declaration concludes with this sentence: "Also, answering questions from the Judiciary Committee about my tenure as a prosecutor poses the risk that my testimony could be used to jeopardize or interfere with either the charged criminal case against Trump or other ongoing investigations." Correct?

The Witness. Yes, the declaration contains that language.

Ms. [REDACTED] Mr. Pomerantz, you were a prosecutor and a defense attorney for many, many years. Can you explain why the risk of interfering in an ongoing investigation is of concern to you?

Ms. Dubeck. To the extent that calls for information based on his tenure at the D.A.'s Office, I object.

Ms. [REDACTED] Can you speak based on your experience prior to your tenure with the D.A.'s Office?

The Witness. What's the question again? I'm sorry?

Ms. [REDACTED] Why is the risk of interfering in an ongoing criminal prosecution something that concerns you as a longtime prosecutor and defense attorney?

Mr. Finzi. Do you want to discuss?

Ms. [REDACTED] We can go off the record for a minute.

[Discussion off the record.]

BY MS. [REDACTED]

Q We can go back on the record.

A Thank you. Respectfully, I will follow my attorneys' instructions and not go beyond the language that appears in the declaration.

Q I want to move on. I'm going to turn to the April 6th, 2023 letter that you received from Mr. Jordan. That's exhibit 1 in this matter.

A Yes. I have it.

Q We have another copy too, if you need it.

On page 4 of this letter -- and again, this is the letter that was accompanying the service of subpoena on you -- Mr. Jordan claims that you hold a, quote, "personal animosity" towards former President Trump. And then he quotes a paragraph from your book. We've also heard other quotes that you have purportedly made about Mr. Trump here today.

Would you describe the excerpt quoted here and the other statements that have been raised as expressions of your First Amendment right to free speech?

Mr. Finzi. Would you repeat that question?

Ms. [REDACTED] He was asked fairly extensively about prior statements he's made

about President Trump and about some others as well.

BY MS. [REDACTED]

Q Would you describe those statements as expressions of your right to free speech? In other words, when you said something, that was exercising your free speech rights, right?

A I intended to exercise my free speech rights at various points, including the statement referenced in Mr. Jordan's letter, which is an excerpt from the book?

Q There was also a letter from Chairman Jordan that you received on March 22nd, correct?

A Yes.

Q Okay. And that letter also accuses you of, quote, "unfairly disparaging" President Trump, correct?

We can introduce that for the record if you don't recall.

A I don't know that it's an accusation. But I recall the letter generally.

Q You don't remember -- you don't recall that particular language?

A I do recall --

Q Yeah, we'll go ahead and introduce it for the record.

A No, I --

Q It's exhibit No. 7.

[Pomerantz Exhibit No. 7

Was marked for identification.]

BY MS. [REDACTED]

Q And the reference to unfairly disparaging President Trump is on page 3.

A Yes, I see it.

Q Okay. So that was an accusation that was put against you in the March

22nd letter, correct?

A I read it as expressing Representative Jordan's view of my book. I don't know that it's an accusation.

Q Mr. Pomerantz, do you believe that you have a First Amendment right to criticize people?

A I do.

Q Would you agree that to the extent you've been brought here today because you've criticized people, that that's an attack on your exercise of that right?

A I believe what is referenced in my statement, which is that I have the right to refuse to answer questions that would compel me to express opinions that I believe are protected by the First Amendment.

To the extent I have been brought here because I wrote a book that expressed opinions with which people may disagree, I do believe that that implicates First Amendment rights.

Q Do you think if others view you being brought here because you wrote a book that expresses opinions with others -- that others might disagree with -- do you think that could chill other people's willingness to make statements that criticize people in the future?

A I really don't want to get into how people might view the proceedings here today, whether others would be chilled or should be chilled, whether I should have written the book. I am just of the view that being called here, to the extent it is because I wrote a book and the impact of being asked to testify is to discourage that activity, that's unfortunate.

But this is not the place for me to get into a long exegesis about First Amendment rights or whether they've been chilled. I have my views on the matter. But how they

relate to the committee's legislative purpose is a mystery to me.

Mr. Goldman. Let me follow up on that legislative purpose.

We've talked a little bit about the litigation in this case and that you were nominally a defendant in it.

When you make the reference to legitimate legislative purpose, what are you -- why are you making -- why are you referring to that term? What is the relevance of that term?

The Witness. I'm not going to debate the statement in -- I'm not going to debate that portion of my statement which indicates that a person subpoenaed before a congressional committee has the right to refuse to answer questions that are not pertinent to a legitimate legislative purpose, although I believe that to be the law. Nor am I going to debate with you here as a witness the legitimacy of the committee's legislative purpose.

I have my views about it, as expressed in the statement. Whether you agree or disagree is not a matter about which I'm going to have a conversation with you under oath. I just don't think that's the purpose of this proceeding.

Mr. Goldman. Are you familiar with the Mazars case in the Supreme Court?

The Witness. I know whereof you speak?

Mr. Goldman. Have you read it?

The Witness. Yes.

Mr. Goldman. And in the Mazars case I will just note that the Supreme Court lays out the most recent explanation of Congress' investigative jurisdiction, which must be related to a legitimate legislative purpose.

Mr. Pomerantz, are you aware of reports that Mr. Trump or his lawyers communicated a desire for Chairman Jordan and other House Republicans to initiate this

investigation shortly after Mr. Trump came to understand that he would be charged by District Attorney Bragg?

It's a question of whether you've read public reporting.

[Discussion off the record.]

The Witness. I am aware of the press reports that you referenced in your question, sir.

Mr. Goldman. And is the information included in those press reports relevant to your assertion that there is no legitimate legislative purpose for this investigation?

The Witness. I won't expand on the thinking that led me to make the statement I made in my opening statement to you.

Mr. Goldman. Why? You testified in your opening statement about your conclusion that you don't think there's a legitimate legislative purpose. I'm just trying to understand why you don't think that.

Ms. [REDACTED] We can go off the record.

[Discussion off the record.]

Ms. [REDACTED] We're back on the record.

The Witness. My belief that there is no legitimate legislative purpose that motivates this deposition is informed by the press reports that you mentioned, but a wide variety of facts and information and circumstances accumulated over an indeterminate period of time. And I'm not going to attempt to psychoanalyze my own belief and provide you with a catalogue of the reasons for reaching the conclusion that I referenced in the statement.

Mr. Goldman. Well, you've been a lawyer for a long time, a very experienced, very accomplished lawyer. Based on your reading of the Mazars case, if Congress initiated an investigation into a specific criminal prosecution against a private citizen,

would that be a legitimate -- in a local District Attorney's Office -- would that be a legitimate legislative purpose, based on your understanding of the Mazars case?

The Witness. I'm not sure I follow that. If you can -- my apologies.

Mr. Goldman. No, that's fine.

If these reports are accurate and this investigation was initiated based on the request of a private citizen to intervene in a prosecution of that private citizen in a local District Attorney's Office, is that a legitimate Federal legislative purpose, based on your reading of the Mazars case?

The Witness. I wish not to get into a lawyers discussion with you about what is or is not a legitimate legislative purpose. While I might agree with your views, I certainly don't wish to get into a debate about this topic when the committee majority has its turn to resume questions. My strong preference would be to simply answer your questions or not answer them based on my legal rights with regard to the facts that led you to ask me to be here today.

Mr. Goldman. Are you -- let's move on.

Are you aware of any other investigation into specific cases in a -- any other congressional investigations into specific cases in a local district attorney's office?

The Witness. That are still pending?

Mr. Goldman. Ever.

The Witness. I'm not.

Mr. Goldman. Do you believe that this investigation is designed to harass and intimidate Mr. Bragg?

The Witness. I do.

Mr. Goldman. Do you think that this investigation would exist if Donald Trump were not the defendant in the People v. Donald Trump in the Manhattan District

Attorney's Office?

The Witness. I don't think it's fair, given that I've come here to assert my rights, among other things, about my political views, I don't want to start holding forth about what is or isn't appropriate as a political matter.

Mr. Goldman. Fair enough.

The Witness. I'll keep my own counsel in that regard.

Mr. Goldman. I just -- I want to switch gears and I'm going to give it back to our counsel.

First, I just want to clarify for the record, because you were asked this in the majority's hour, you and I have never met, correct, until today?

The Witness. That's correct.

Mr. Goldman. We've never spoken?

The Witness. Not that I recall.

Mr. Goldman. We both worked at the Southern District of New York but at different times.

The Witness. That's correct.

Mr. Goldman. When you take an oath as a Federal prosecutor -- and we're not going to talk about your time as a -- well, I'll say, when you take an oath as a Federal prosecutor, do you take an oath to proceed without fear or favor?

The Witness. You know, I'm not sure that's in the oath, but that's certainly in the spirit of what the job requires?

Mr. Goldman. And what does that mean to you?

The Witness. What it meant to me when I was sworn in as a Federal prosecutor, both times I was sworn in as a Federal prosecutor, is that you make decisions in cases without regard to the concern you may have about taking action. You can't be afraid

about the consequences of your actions if you believe that they're well informed and that they are based on the law and the facts and the evidence.

You don't act with favor means that you don't take official action or decline to take official action based on your relationship with a potential subject or because of your personal interests one way or the other. You make decisions that are based on the facts and the law and in the best interests of your client.

In the case you're referencing, my client was the Government of the United States, and I attempted to make decisions that were in the best interest of the government without regard to how they impacted my own circumstances or politics or career or anything else. You make decisions consistent with your obligations to serve the public interest.

Mr. Goldman. And did you use that same approach when you joined the New York County District Attorney's Office?

The Witness. I'm not going to talk about my activities as a Special Assistant District Attorney, respectfully.

Mr. Goldman. Based on your experience as a prosecutor -- well, let me start over.

You're aware of the criminal prosecution against The Trump Organization in the summer of 2022, correct?

The Witness. Am I aware of the prosecution?

Mr. Goldman. Yes.

The Witness. Yes.

Mr. Goldman. Okay. And that was a trial. Is that right?

The Witness. Yes.

Mr. Goldman. And The Trump Organization was convicted --

The Witness. Yes.

Mr. Goldman. -- of 17 crimes?

The Witness. Yes.

Mr. Goldman. Now, in your experience as a prosecutor, do prosecutors and investigators redouble their investigative efforts in advance of trial and in preparation for trial?

The Witness. Can I limit my response to my experience as a Federal prosecutor?

Mr. Goldman. Please.

The Witness. Yes, preparing for trial is always a period when prosecutors and law enforcement agents feverishly go about making sure they have gathered all the facts and are in position to present them.

Mr. Goldman. And is it common during that trial preparation to discover new evidence?

The Witness. Yes.

Ms. [REDACTED] We're actually out of time.

Do you have any?

We can go off the record.

[Recess.]

Mr. Schiff. Thank you for allowing me to ask questions before you begin your time.

Mr. Pomerantz, I am Adam Schiff from California.

The Witness. Yes, sir.

Mr. Schiff. I appreciate your being here today.

In your opening statement you said that "I do not for a moment believe" -- "I do not believe for a moment that I am here to assist a genuine effort to enact legislation or

to conduct legislative oversight. We are gathered here because Donald Trump's supporters would like to use these proceedings to attempt to obstruct and undermine the criminal case pending against him and to harass, intimidate, and discredit anyone who investigates or charges him."

I quite agree with the sentiments you've expressed. I can discern no legitimate legislative purpose either.

You have a lot of experience, though, as a prosecutor. And I'd like to ask you, in your experience, have you ever seen another situation where a committee of Congress sought to interfere with a specific criminal case in a specific jurisdiction? And what would be the impact if this were to become precedent for the Congress to intervene in other criminal cases in other parts of the country?

The Witness. I have not seen similar proceedings. But, respectfully, I don't want to hold forth and give you personal views on the wisdom or the impact of proceedings like this one.

My hope is to get out of this room as quickly as I can without inviting more debate and colloquy about matters of public policy. I'm not a policy expert. I'm just a lawyer. And we can all have our respective views about the impact of these proceedings, whether that impact is positive or negative.

So, respectfully, I'm going to decline your invitation to express my personal views.

Mr. Schiff. I appreciate that. Let me try one more time.

In your opening statement you also said, "This is neither the time nor the place for me to answer questions about the investigation or the pending indictment over the objection of the prosecutors. The charges against Mr. Trump should be heard and decided by a judge and a jury before politicians second-guess their merits or the decision to bring them. That's how our system works. Those who claim that they respect the

rule of law should wait for the courts to do their work."

If Congress had the power or authority to subpoena witnesses or materials in cases where there's a pending indictment and approaching trial, how might that interfere with a prosecution?

The Witness. I think historically it has been the view of the Department of Justice certainly that pending cases ought to be litigated and that responding to congressional inquiries creates a potential to jeopardize prosecutions, witness security, and so on.

I think that there has not been a deep and rich history of congressional investigations that touch on pending State prosecutions. But I don't see why the circumstances would be different with respect to State prosecutors fearing for the integrity of their prosecutions and investigations.

But, again, I hope you'll understand I'm not here to provide expert testimony or expert views. I don't consider myself an expert on the impact of congressional investigations on pending prosecutions.

I just know, having been a prosecutor, that you want to go about your business and prosecute your cases and have them litigated before the court that has jurisdiction and that responding to outside requests and demands is never something one looks forward to doing.

Mr. Schiff. Last question before I hand it back. Again, Mr. Chairman, I appreciate your indulgence.

It's been publicly reported that Mr. Trump's attorneys reached out to this committee to ask for the committee's help in impacting or through discovery in the Manhattan prosecution against Mr. Trump.

Is there a process in which a defendant in a criminal trial in New York City or

anywhere else can obtain discovery from prosecutors without having to seek Congress to do it for them? Isn't there a process in which defendants are entitled to Brady material where they get it directly from the prosecutor's office and don't require the intercession of Congress to do that?

The Witness. Well, New York has a very liberal criminal discovery regime. And in New York or outside of New York obviously defendants have the ability by way of motion practice to litigate the integrity of the decision to prosecute and to test whether a prosecution was brought for inappropriate reasons.

That opportunity certainly exists under Federal law. It exists under New York law. I'm not going to speak to other jurisdictions.

Mr. Schiff. Thank you, Mr. Chairman. I yield back.

Chairman Jordan. Mr. Pomerantz, do you know who disagrees with Mr. Schiff and your characterization of legislative purpose?

The Witness. Pardon me?

Chairman Jordan. Do you know who disagrees with Mr. Schiff and your characterization of legislative purpose?

The Witness. I don't know, but I can indulge in some guesses.

Chairman Jordan. Who would you guess?

Well, we'll save time. We'll go -- the people who disagree is the court and that's why you're here. Let me just read for the record what the court said.

"The committee is considering legislation to prohibit the use of Federal forfeiture funds to investigate a current or former President. This purpose standing alone is clearly sufficient to justify the subpoena and thereby to end this court's inquiry."

Do you know who else agrees with the court? The lady who's been objecting all morning, Ms. Dubeck. Bragg's counsel conceded that the investigation of the District

Attorney of New York's use of Federal funds is a valid legislative purpose.

But they go on.

"Defendants identify the possibility of legislative reforms to insulate current and former Presidents from State prosecutions such as by removing criminal actions filed against them from State to Federal court. In fact, there's been legislation introduced to do that."

This idea that it's not a legitimate legislative purpose is ridiculous. In fact, I understand it's unusual, but the court spoke to that as well.

Page 14, footnote 7. "Bragg notes that there is 'no prior case in which Congress has attempted to subpoena a State prosecutor for purpose of extracting information about an ongoing State prosecution.'"

Mr. Pomerantz, do you know of any situation where there's a case of a former President of the United States being criminally charged in a State trial court? Do you know of any situation like that?

The Witness. Other than the present one? I do not.

Chairman Jordan. And that's what the court said. "However, there is no prior case in which a former President of the United States has been criminally charged in State trial court, suggesting both parties swim in untested waters."

[Pomerantz Exhibit No. 8

Was marked for identification.]

BY MR. [REDACTED]

Q Mr. Pomerantz, are you aware of any Federal funds used by the District Attorney's Office in the prosecution of President Trump?

A I have no knowledge whatsoever on that topic.

Q Are you aware of any positions, some Assistant District Attorney positions,

that are funded by the Federal Government in the D.A.'s Office?

A I'm not aware one way or the other.

Q In a March 31st, 2023, letter we received from the District Attorney's Office, the general counsel wrote: "Our review of the office's records reflect that of the Federal forfeiture money that the office helped collect approximately \$5,000 was spent on expenses incurred relating to the investigation of President Trump."

Are you aware of that?

A I only was -- I became aware of it when I read the letter to which you refer. I have no other knowledge beyond what is contained --

[Pomerantz Exhibit No. 9

Was marked for identification.]

Mr. [REDACTED] We're marking this as exhibit 9.

The Witness. Yes, sir.

Mr. [REDACTED] Exhibit 8 was Judge Vyskocil's opinion Mr. Jordan referenced.

Were you aware before Ms. Dubeck's letter that the D.A.'s Office had used Federal funds in the prosecution of President Trump?

The Witness. I was not.

Mr. [REDACTED] Did you ever have any discussions while you were at the D.A.'s Office with anyone about the use of Federal funds?

Ms. Dubeck. Objection.

The Witness. I will refuse to answer on the basis of the objection from the District Attorney's Office.

Having said that, I will reaffirm my previous answer to you that I knew absolutely nothing about the use of Federal funds in connection with the Trump investigation.

Mr. [REDACTED] Did you ever discuss with anyone in the D.A.'s Office the issue of

President Trump's security were he to be indicted or convicted?

Ms. Dubeck. Objection.

The Witness. I decline to answer that question on the basis of the rights referenced in paragraphs 4 and 5 of my opening statement.

Mr. [REDACTED] Refresh my recollection about what paragraphs 4 and 5 --

Mr. Wells. In the spirit of efficiency, 4 relates to the objections of the D.A., 5 relates to the Self-Incrimination Clause of the Fifth Amendment, and 6 relates to the legislative purpose and First Amendment due process.

Mr. [REDACTED] Thank you.

So as I understand it, the question was whether you ever had any discussions with anyone in the D.A.'s Office about the issue of President Trump's security were he to be indicted or convicted. And you're invoking the Fifth Amendment on that particular question?

The Witness. Yes. If you'd give me one moment.

Mr. [REDACTED] Of course.

[Discussion off the record.]

The Witness. I do refuse to answer your question on the basis of my rights as reflected in the statement.

Mr. Wells. He said paragraphs 4 and 6 -- 4 and 5.

The Witness. 4 and 5, yes.

Mr. [REDACTED] Did you ever discuss with anyone in the D.A.'s Office how the former President's entitlement to lifetime Secret Service protection under Federal law would be accommodated were he to be convicted of a crime or sentenced to prison?

Ms. Dubeck. Objection.

The Witness. Same response, sir.

Mr. [REDACTED] And that response is?

The Witness. Is not to answer your question on the basis of the District Attorney's position that the information is privileged or confidential and my personal privilege not to be compelled to be a witness against myself.

Mr. [REDACTED] Mr. Gaetz, did you want to go or did you want me to continue?

Mr. Gaetz. I do have some questions.

Mr. [REDACTED] Okay.

Mr. Gaetz. Mr. Pomerantz, did the Manhattan D.A. ever issue you a cell phone?

Mr. [REDACTED] Do you want to go off the record?

Off the record.

[Discussion off the record.]

The Witness. On the advice of counsel, I'm not going to answer that question, sir.

Mr. Gaetz. Asserting what privilege?

The Witness. Privilege against self-incrimination.

Mr. Gaetz. And did the Manhattan's D.A.'s Office ever issue you a laptop?

The Witness. Same answer to that question, sir.

Mr. Gaetz. That you're asserting your Fifth Amendment right not to answer?

The Witness. Yes, sir.

Mr. Gaetz. And did they issue you any other hardware?

The Witness. Same response.

Mr. Gaetz. And were you given a Manhattan D.A. email address during your time there?

Mr. [REDACTED] Go off the record?

[Discussion off the record.]

Mr. Gaetz. We're back on the record.

The Witness. Yes, I refuse to answer your question on the same basis as I've previously indicated.

Mr. Gaetz. Do you use email now?

The Witness. Pardon me?

Mr. Gaetz. Since you've left the employ of the Manhattan D.A., do you use email as a method of communication?

The Witness. I decline to answer your question.

Mr. Gaetz. And who's your current email provider?

The Witness. I decline to answer that question.

Mr. Gaetz. On Fifth Amendment grounds?

The Witness. Yes, sir.

Mr. Gaetz. And I'm not trying to be pedantic, I'm just trying to make the record clear.

The Witness. No, I understand that. And I appreciate that.

Mr. Gaetz. And who's your current cell phone provider?

The Witness. Likewise, I refuse to answer that question on the basis of my rights under the Fifth Amendment.

Mr. Gaetz. How much money did you make on the book?

The Witness. I refuse to answer that question as well.

Mr. Gaetz. On what basis?

The Witness. That one is on the basis of both my Fifth Amendment rights and the rights articulated and referenced in paragraph 6 in my opening statement.

Mr. Gaetz. I yield back.

BY MR. [REDACTED]

Q This morning I asked you about the speech that Attorney General Jackson had provided.

A Yes, sir.

Q I also asked you about the ABA standards.

A Yes.

Q And I asked you about the U.S. Attorneys' Manual.

A Yes, sir.

Q And you had declined to answer those questions.

Now, if I rephrase my questions and say, are you familiar from your time as a Federal prosecutor with any of those three authorities about the principles of prosecution, does your answer -- are you able to answer the question?

A I'm able to answer the question, but I refuse to answer the question.

Q Okay.

A Not to parse the language too fine. I don't mean to be cute.

Q And I understand, sir.

During the last hour Mr. Goldman was asking you about there is fear and favor, and you walked through with Mr. Goldman the meaning behind fear and favor and how I believe you represented you were familiar with it from your time as a Federal prosecutor.

How does that differ from my questions?

A I don't want to get into a debate with you about my position with respect to particular questions. I respect your right to challenge my invocation of rights. I hope you don't, but if you do, we will have that discussion, I suppose.

But I believe that I have a fair basis on which to invoke my rights with respect to familiarity with the "Principles of Federal Prosecution," the U.S. Attorneys' Manual, and Justice Jackson's speech.

Mr. Bishop. Mr. Pomerantz, my name is Dan Bishop.

The Witness. Yes, sir.

Mr. Bishop. Just quickly for the sake of the record, I want to make available to you and your counsel that in Mitchell v. United States, a 1999 case in the United States Supreme Court, 526 U.S. 314, Justice Kennedy, writing for the Court, said: "It is well established that a witness, in a single proceeding, may not testify voluntarily about a subject and then invoke the privilege against self-incrimination when questioned about the details. The privilege is waived for the matters to which the witness testifies, and the scope of the 'waiver is determined by the scope of relevant cross-examination.'"

[Pomerantz Exhibit No. 10

Was marked for identification.]

Mr. Bishop. Also, on the same point, in the case of Morgan Art Foundation Limited v. McKenzie from the Southern District of New York, on December 15th, 2021, the Court said: "However, the Fifth Amendment privilege against self-incrimination is not self-executing and may be waived if not invoked. As relevant here, where a witness testifies voluntarily and therefore controls the extent of the disclosure, the privilege is waived for the matters to which the witness testified and the scope of the waiver is determined by the scope of relevant cross-examination."

Now, of course. Your counsel has appropriately said -- and I will be glad to hand a copy to you, if you would like.

The Witness. Yes, please.

Mr. Bishop. And I have got copies for other counsel as well.

[Pomerantz Exhibit No. 11

Was marked for identification.]

Mr. [REDACTED] I'm sorry, Mr. Bishop. Morgan is the second case you mentioned?

Mr. Bishop. It is.

Mr. [REDACTED] Okay. So that would be 11.

Mr. Finzi. So there's Mitchell and Morgan?

Mr. [REDACTED] So Mitchell's No. 10 and Morgan's No. 11. And I apologize, sir.

Mr. Bishop. Good. Thank you, Mr. [REDACTED] to keep the record clear. That's very helpful.

Mr. Finzi. Mitchell 10, Morgan 11?

Mr. [REDACTED] Correct.

Mr. Bishop. And of course counsel made the point they didn't want to debate privilege. I'm not. I'm just seeking to lay a record because the assertion of a privilege, of course, needs to have a reasonable basis. You just spoke to that, Mr. Pomerantz.

Earlier in your examination today, Ms. Stefanik of New York said, "So there are no lies in the book? You stand fully behind this publication under your name?" And your answer was, "That's correct."

Mr. Pomerantz, on page 170 of your book you say that -- let me make sure I get the context so that it's complete -- "No one could know exactly what the security dangers might be if we indicted Trump. I assumed that the MAGA crowd would make its presence felt. But we had to trust that our institutions and personnel could be secured no matter how events might unfold."

Sir, what you do mean by the MAGA crowd? What is that?

The Witness. I refuse to answer your question, sir, on the basis of the rights I asserted in the fifth and sixth paragraphs of my statement.

Mr. Bishop. And you continue to assert the right -- those rights, the right of the Fifth Amendment in particular, but notwithstanding of the information I've furnished. Is that correct?

The Witness. That's correct.

Mr. Bishop. On page 192 of the book you wrote: "I explained that I had made a deliberate effort not to think about the damage Trump had done to politics, the rule of law, respect for the truth, or the fabric of our democracy."

What is meant by the damage Trump had done to politics?

The Witness. I don't believe I am required to go beyond the language reflected in my book. And, accordingly, I refuse to answer your question.

Mr. Bishop. On the grounds that you've previously asserted. Is that correct?

The Witness. That's correct.

Mr. Bishop. What did you mean by the damage Trump had done to the rule of law?

The Witness. I take the same position with respect to that question, sir.

Mr. Bishop. What do you mean by the damage Trump had done to respect for the truth?

The Witness. I take the same position with respect to that language and likewise with respect to the fabric of democracy.

Mr. Bishop. What do you mean about the damage Trump had done to the fabric of our democracy?

The Witness. I take the same position and refuse to answer your question for the reason stated.

Mr. Bishop. On page 192 also you wrote: "Indeed I thought there might be an argument that Trump had assumed an office that required him to take care that the laws be faithfully executed and having urged the country to trust him to uphold the law should be held to a higher standard of personal conduct than the average citizen."

What do you mean by that?

Ms. Dubeck. Objection.

The Witness. I refuse to go beyond the language that appears in the book and provide you with a further explanation of what I meant.

Mr. Bishop. [Inaudible] did you not, sir, that for purposes of the prosecutorial action you sought from the office, that Trump should be treated differently than average citizens? Isn't that right?

Ms. Dubeck. Objection.

The Witness. I have nothing to add beyond my prior response.

Mr. Bishop. On page 198 of your book you say: "While it could be argued that the American people generally have been hurt by Trump's deceptions." What do you mean by that?

The Witness. I'm sorry, I missed your question.

Mr. Bishop. I'll repeat it. On page 198 of the book you write: "While it could be argued that the American people generally have been hurt by Trump's deceptions." What do you mean by that?

Ms. Dubeck. If you can pause. I'm not finding the language.

Mr. Bishop. All right. Let me help and I'll read the full sentence. At the bottom of -- the next to last paragraph on 198 it says: "While it could be argued that the American people generally have been hurt by Trump's deceptions, we were speaking about a victim in the legal sense, a person or entity that had received the SOFCs, relied on them to give money to Trump, and then suffered a financial loss." That's the whole sentence.

My question, though, is about the first clause of the sentence. What do you mean that the American people generally have been hurt by Trump's deceptions?

Ms. Dubeck. Objection.

The Witness. Yes, for the reasons stated in the fourth and fifth paragraph of my letter, I will decline to answer that question.

Mr. Bishop. To what deceptions to you refer?

The Witness. I refuse to answer that question for the reasons stated.

Mr. Bishop. In what way do you mean the American people generally have been hurt?

The Witness. Same answer, sir.

Mr. Bishop. At another point in the book, and I didn't note the page reference, perhaps you'll recall it, but you say: "I was haunted by the thought that there were many people everywhere who had been counting on us to hold Trump accountable for crimes that we would never get a chance to prove in court."

My question to you there is, what people?

Ms. Dubeck. Object.

The Witness. I decline to answer your question and believe I am not required to do so for the reasons reflected in my statement.

Mr. Bishop. Would the people include political enemies of Mr. Trump?

The Witness. I won't --

Ms. Dubeck. Objection.

The Witness. Excuse me, sorry.

I won't elaborate on the language that appears in the book and accordingly assert my rights under the fourth and fifth paragraphs of my statement.

Chairman Jordan. Were they the same people who said "go get him" on page 1 of the book?

The Witness. The same answer.

Mr. Bishop. On page -- withdrawn.

At another point you wrote: "Has the target generally been involved in antisocial behavior such that the community needs to be protected from further misbehavior or the target held to account for misdeeds that extend well beyond the particular crime at issue?"

How did that apply to Mr. Trump?

The Witness. I refuse to answer your questions for the reasons reflected in the fifth paragraph of my letter. I'm not certain, I may have answered too quickly before Ms. Dubeck had a chance to object, for which I apologize.

Ms. Dubeck. I lost track of whether he was asking something based on your time at the D.A.'s Office. To the extent he was, I object.

Mr. Bishop. I yield back.

Mr. [REDACTED]. To your knowledge, when was the first time the District Attorney's Office interviewed Michael Cohen?

Ms. Dubeck. Objection.

The Witness. I refuse to answer for reasons previously stated --

Mr. [REDACTED]. Given your experience --

The Witness. -- in paragraphs 4 and 5 of my statement for the record.

Mr. [REDACTED]: Okay.

Given your experience, how can you possibly believe Michael Cohen is a reliable witness?

Ms. Dubeck. Objection.

The Witness. I decline to answer for the reasons reflected in paragraphs 4, 5 and 6 of my statement.

Mr. [REDACTED]. So you're taking the Fifth Amendment on given your experience how can you possibly believe Michael Cohen is a reliable witness?

The Witness. Yes.

Mr. [REDACTED] Okay. Are you aware of the shifting information Mr. Cohen has put forward about the Stormy Daniels payments?

Ms. Dubeck. Objection.

The Witness. I decline to answer for the reasons indicated in the answer to your previous question.

BY MR. [REDACTED]

Q I believe in your book you say that you were following the Michael Cohen testimony when he appeared before Congress. It was the first big hearing of Chairman Cummings' tenure. Mr. Cohen testified back in 2019. I believe in your book that you said you watched that and you were following along. Is that correct?

A I believe that appears in the book, yes.

Q And as you sit here today, do you remember that testimony?

A I decline to answer that question based on my right not to be a witness against myself in a possible criminal proceeding.

Q I'd like to mark as exhibit 12 a letter from Steve Ryan to the Federal Election Commission.

[Pomerantz Exhibit No. 12

Was marked for identification.]

Mr. [REDACTED] Mr. Ryan is a -- Mr. Ryan was one of Michael Cohen's lawyers at the time.

Mr. Ryan writes: "In a private" -- he's writing on behalf of Michael Cohen to the Federal Election Commission here. "In a private transaction" -- this is the second paragraph" -- "in 2016, before the U.S. presidential election, Mr. Cohen used his own personal funds to facilitate a payment of \$130,000 to Ms. Stephanie Clifford. Neither

the Trump Organization nor the Trump campaign was a party to the transaction with Ms. Clifford, and neither was reimbursed by Mr. Cohen" -- or "neither reimbursed Mr. Cohen for the payment directly or indirectly."

Are you familiar with this letter? Have you ever seen this before?

Ms. Dubeck. Objection.

The Witness. I decline to answer.

Mr. [REDACTED] And as you know, in 2018 Michael Cohen says, through his lawyer, that nobody ever reimbursed him. And then when he showed up before Congress, it was Chairman Cummings' first big hearing in January 2019, he changed his tune and he said he was reimbursed.

Were you aware of that sort of a changing story of Mr. Cohen on that front?

Ms. Dubeck. Objection.

The Witness. I decline to answer your question.

[Pomerantz Exhibit No. 13

Was marked for identification.]

Mr. [REDACTED] I'd like to mark as exhibit 13 a letter from Mr. Jordan and Mr. Meadows to the Attorney General referring Michael Cohen for perjury for his appearance in February -- I'm sorry, it was February 2019. I think in my last question to you I said it was January 2019, but it was February 27th, 2019, that he appeared, first big hearing of the Democrats' new majority at the time.

And this letter sets forth numerous undeniable facts about Mr. Cohen perjuring himself during his appearance before the committee.

Have you ever seen this letter before?

Ms. Dubeck. Objection.

The Witness. I decline to answer your question, one way or the other, on the

basis of my Fifth Amendment rights.

Mr. [REDACTED] Okay. The bottom of page 1 it says:

"Several times during his testimony, Mr. Cohen denied committing various fraudulent acts that he pleaded guilty to in federal court. Specifically, Mr. Cohen said, 'I never defrauded any bank.'

"These denials are intentionally false. Mr. Cohen pleaded guilty to five counts of income tax evasion, one count of making false statements to a banking institution, one count of causing an unlawful corporate contribution, one count of excessive campaign contribution, and one count of making false statements to Congress."

In your experience, is there any way that Mr. Cohen could not have committed perjury when he testified one way and he pleaded guilty in an exact opposite fashion to the same set of facts?

Ms. Dubeck. Objection.

The Witness. I decline to answer the question for the reasons previously stated.

Mr. [REDACTED] When you were at the D.A.'s Office, did you consider this type of unreliability when considering Mr. Cohen as the narrator for the case against President Trump?

[1:43 p.m.]

Ms. Dubeck. Objection.

The Witness. Same response, sir.

BY MR. [REDACTED]

Q And in your book you did describe Mr. Cohen as a potential narrator for the prosecution against President Trump. Is that correct?

Well, I think this is in the book.

A The book says what it says. I'm not disputing your characterization.

Q Okay. So it's fair to say that in your book you talk about in a prosecution of this type you need a good narrator?

A I think there is a reference to the need for a narrator that appears in the book.

Q And Michael Cohen was considered as that possible narrator?

Ms. Dubeck. Objection.

The Witness. I rest on what's set forth in the book. I'm not taking issue with your characterization.

BY MR. [REDACTED]

Q Going back to the letter, Mr. Cohen repeatedly testified that he did not seek employment in the White House following President Trump's election. And this is demonstrably material and intentionally false, too.

The testimony is -- that testimony is in indirect conflict with court filings made by the U.S. Attorney's Office in the Southern District of New York which stated: During and after the campaign, Cohen privately told friends and colleagues, including in text messages, that he expected to be given a prominent role and title in the new administration. When that did not materialize, Cohen found a way to monetize his

relationship with and access to the President.

Was that a fact that you were aware of?

Ms. Dubeck. Objection.

The Witness. The same response, sir.

BY MR. [REDACTED]:

Q At the hearing Mr. Jordan asked Mr. Cohen: You wanted to work in the White House?

And Mr. Cohen said: No, sir.

And that answer, when Mr. Cohen said "no, sir," is expressly contradicted by the text messages that the Southern District of New York used in the case against Mr. Cohen.

With that said, I mean, how is that not perjury before Congress?

Ms. Dubeck. Objection.

The Witness. I refuse to answer the question for the reasons reflected in paragraphs 4 and 5 of my statement.

Mr. Bishop. Mr. Pomerantz, on page 178 your book you have this paragraph. It says: "Carey drafted a lengthy outline of defense arguments. The defense outline claimed that a prosecution would be politically motivated and would violate Trump's constitutional rights. It noted that the district attorney and the Attorney General were Democrat politicians who supposedly were trying to prevent Trump from becoming president again. It detailed some of New York State Attorney General Letitia James's public statements about Trump in reference to Alvin Bragg's campaign statements about having repeatedly sued the Trump administration. It suggested that Trump would move to disqualify the prosecution and seek a transfer of venue out of New York City. It characterized the case as a political vendetta that had wasted vast resources in the hunt for a viable theory of criminal liability after Trump, all at a time when murders and violent

crime were increasing."

I'll stop there. Did I read it accurately?

The Witness. Pardon me? Yes, you read it accurately, of course.

Mr. Bishop. Do you know what the defense of selective or vindictive prosecution is?

The Witness. I decline to answer your questions.

Mr. Bishop. Are you aware that prosecuting someone criminally in retaliation for First Amendment expressive activity or associational activity is unconstitutional?

Ms. Dubeck. Objection.

The Witness. I decline to answer your question. I'll resist the temptation to elaborate on it.

Mr. Bishop. Were any of the factual bases that Carey laid out in his lengthy outline of defense arguments inaccurate?

Ms. Dubeck. Objection.

The Witness. I decline to answer your questions for the reasons reflected in paragraphs 4, 5, and 6 of my statement.

Mr. Bishop. Did you undertake to or did anyone else working with you on the investigation of Mr. Trump undertake to rebut any of the factual bases underlying the outline of this defense argument furnished by Carey?

Ms. Dubeck. Objection.

The Witness. I would like to make the same response to that question as to your previous one, sir.

Mr. Bishop. Which is declining to answer --

The Witness. Yes.

Mr. Bishop. -- on the basis of your asserted privileges?

The Witness. Yes, sir.

Mr. Bishop. Thank you.

BY MR. [REDACTED]

Q Are you familiar with Bob Costello?

A Yes.

Q And how do you know him?

A We served together in the Office of the United States Attorney for the Southern District of New York during the time I was line assistant between 1978 and 1982. I don't recall for exactly what portion of that period of time Mr. Costello was a prosecutor, but that is one of the ways in which I was familiar with Mr. Costello.

Q Are you aware that Mr. Costello was called to the grand jury -- this most recent grand jury that indicted President Trump?

Ms. Dubeck. Objection.

BY MR. [REDACTED]

Q Mr. Costello has made a number of TV appearances talking about these types of things. I'm just asking if you're aware of the public reporting on this.

A I saw public reporting.

Chairman Jordan. You said you worked with him in the Southern District of New York, and you said that's one of the ways you were aware of Mr. Costello.

What were the other ways. Was he a friend?

The Witness. I need a moment with counsel.

Mr. [REDACTED] Of course.

[Discussion off the record.]

Chairman Jordan. I can withdraw the question. I was -- I just was curious. I can withdraw it.

The Witness. Thank you. That's very helpful.

Chairman Jordan. No, I get it. I get it.

You said that the one way -- well, that's fine. I get it.

The Witness. I appreciate that.

BY MR. [REDACTED]

Q Are you aware that Mr. Costello was representing Mr. Cohen at any point in time?

Ms. Dubeck. Objection.

The Witness. I'm aware of public reports of that type.

BY MR. [REDACTED]

Q Now, are you aware of reports of what Cohen told Costello was different from what Cohen evidently told Ryan right around the same time period about the Stormy Daniels payments? Are you aware of that public reporting?

A I believe I did see that in public reporting as well.

Q Are you aware that Cohen alleged that somebody dangled a pardon over him, you know, if he cooperates and doesn't say negative things about President Trump?

Ms. Dubeck. Objection.

The Witness. I'm limiting my response to publicly reported materials in the last several months, I guess, and so limited, I don't recall.

BY MR. [REDACTED]

Q Okay. So Cohen alleged that Costello referenced that, you know, some pardon might be available to him.

Are you aware of that?

Ms. Dubeck. Objection.

The Witness. Again, limiting my response to recent press reports, that sounds

familiar, but I don't recall it with any acuity.

BY MR. [REDACTED]

Q Okay.

A Yes, but I'm not basing my response on anything having to do with my employment in the D.A.'s Office.

Q And are you aware that the Southern District of New York U.S. Attorney's Office looked at potentially prosecuting President Trump based on the pardon allegation?

Ms. Dubeck. Objection.

Mr. [REDACTED] Go off the record.

[Discussion off the record.]

The Witness. All right. Respectfully, I decline to answer the question.

BY MR. [REDACTED]

Q Okay. And did you know the Southern District of New York decided not to prosecute because they decided Cohen was completely unreliable and could not be considered as a legitimate witness at any prosecution?

Ms. Dubeck. Objection.

The Witness. I decline to answer that question as well for the reasons previously given.

BY MR. [REDACTED]

Q Okay. And do you expect that Michael Cohen will be called as a witness before the New York District Attorney's case that's just been filed?

Ms. Dubeck. Objection.

The Witness. I decline to answer.

BY MR. [REDACTED]:

Q Returning back to your opening statement --

A Yes, sir.

Q -- what's the basis for your conclusion that you are certain you broke no laws?

A I would be very surprised if a court ruled that I had no privilege to answer that question, and I'm asserting my Fifth Amendment rights with respect to that.

Q Has anyone from the District Attorney's Office explicitly or implicitly threatened to prosecute you if you answer the committee's questions?

A I decline respectfully to answer your question.

Q When did you first hear that the District Attorney's Office was pursuing some potential criminal investigation of you?

A I will take my counsel's advice and refuse to answer that question, sir.

Q When we were with Judge Vyskocil on the 19th --

A Yes, sir.

Q -- the District Attorney's Office, you know, represented that they sent you this letter raising the prospect of a criminal prosecution.

Do you remember that?

A I do.

Q Was that the first time you heard of that?

A The first time I heard of a letter?

Q Right. Like had you -- was that the first time you heard that you were under criminal investigation?

Did it surprise you?

A I'm not going to answer your question with regard to whether I was surprised.

Q On the basis of the Fifth Amendment?

A Fifth Amendment, and also the rights summarized in the sixth paragraph of my statement.

Q What's the sixth paragraph again?

A My position being there the question whether I was surprised by what I heard in open court in January is not, I believe, a matter that's pertinent to your legislative purpose.

Q Don't you think this investigation of you, this purported investigation of you is simply a pretext, simply a pretext to block your testimony here today?

It's not a real investigation, is it?

A I respectfully decline to answer your question.

Q Have you been interviewed by the D.A.'s Office on this topic?

A I respectfully decline to answer your question.

Q Have they asked for any documents from you?

A I respectfully decline to answer your question.

Q Okay.

Chairman Jordan. Mr. Pomerantz --

The Witness. Yes, sir.

Chairman Jordan. -- you resigned in February of 2022.

The Witness. 2022, that's correct.

Chairman Jordan. And did the District Attorney's Office know you were working on a book anytime between February 2022 and February of 2023?

The Witness. I decline to answer your question.

Chairman Jordan. But they didn't put you under notice that you were potentially under criminal investigation until, according to your statement, shortly before the publication of your book?

The Witness. I'm not sure what you're referencing.

Chairman Jordan. I'm referencing your statement, page 2 of your statement.

"Shortly before the publication of my book, the District Attorney's office warned me that I could face criminal liability if, among other things, I disclosed grand jury material or violated a provision of the New York City Charter dealing with the misuse of confidential information."

The Witness. Yes, sir, that's accurate.

Chairman Jordan. So the first time you were put on notice?

Mr. [REDACTED]. Off the record.

[Discussion off the record.]

Mr. [REDACTED]. Back on the record.

The Witness. The question again was whether I was on notice of a possible criminal investigation?

Mr. [REDACTED]. Mr. Jordan asked you the first time you were on notice, and he referenced your statement.

The Witness. The statement references a letter that I received in January of 2023, which I believe you have.

Chairman Jordan. Okay.

Mr. [REDACTED]. Did you need to lodge an objection?

Ms. Dubeck. It didn't sound like quite exactly the same question, so --

Mr. [REDACTED]. Okay.

BY MR. [REDACTED]:

Q But the letter that you received in January 2023, it's just a pretext, isn't it? I mean, is there a real investigation going on?

A You're asking me?

Q Yes. They're not really going to prosecute you? They're not really investigating you, are they?

A I hope you're right. But I'm not speaking for the District Attorney's Office --

Q That's fair.

A -- in respect of how tangible is the fear of criminal prosecution.

Q Okay. You got the letter in January. Was that the first time the D.A.'s Office communicated with you that they were disappointed you were writing a book or trying to stop the publication of the book?

Mr. Finzi. Could we have a second?

Mr. [REDACTED]. Sure. Go off the record.

[Discussion off the record.]

Mr. [REDACTED]. We'll go back on the record.

BY MR. [REDACTED]:

Q Your answer, sir?

A I decline to answer your question with respect -- for the reasons indicated.

Q Okay. Can you tell us about all of the communications you've had with the D.A.'s Office since January of this year, other than the ones we've discussed, which was this receiving of the letter?

Ms. Dubeck. Objection.

Mr. [REDACTED]. Well, I mean, he's no longer with the Office.

Ms. Dubeck. January of this year?

Mr. [REDACTED]. January of this year.

Ms. Dubeck. Withdrawn.

BY MR. [REDACTED]:

Q What I'm getting at, okay, if I may?

A Yes, sir.

Q What I'm getting at is they didn't try very hard. They didn't try very hard to get you to not publish the book. I mean, they may have written this letter, paper in the file. And if I'm mistaken, if I'm mistaken, please help me understand that I'm wrong.

You got the letter from them. What other -- did they call you on the phone and urge you? Did you have any meetings with them in person?

A Mr. [REDACTED], I don't believe that I'm required in this context to articulate for you all of the reasons which lead me to invoke my privilege.

Q Fair enough.

And let me just, if I may, articulate why we're asking, okay, just as a courtesy.

We believe that it's possible and worth investigating that this whole, you know, New York District Attorney's Office, you know, so-called investigation is a sham, and it's simply a pretext to prevent you from coming here and talking about your book. And so, because of that, I mean, that could invoke some serious implications. I mean, that could be obstruction of Congress. And so it's worthwhile for us. And so we don't, you know, mean to be pedantic or, you know, any -- don't mean any disrespect by it. But we are trying to understand the volume of communications, the type of effort that the District Attorney's Office, you know, put forth to try to get you to stop the book. And if they did put forth an effort that we don't know about, I mean, that would be great, a great fact to have on the record.

A I would be delighted to hear, Mr. [REDACTED], that my fear of criminal prosecution is completely baseless and unfounded. I don't believe that to be the case and, therefore, I am invoking my rights as reflected.

Q Okay. And let me just say, I'm not disputing that you believe -- I'm not disputing your belief that you think that they might be actually conducting a criminal

investigation. Because when somebody is faced with a letter saying that there's an investigation, a human being, a normal conclusion is to be concerned about that. Okay. So fair enough. I'm not trying to be disrespectful of that.

A I appreciate that.

Q But from our point of view, okay, from the point of view of the Congress, the record looks pretty thin. And it looks like a pretext to us -- not to you, but to us, and so, consequently, just trying to ask you if you can catalog the efforts that the D.A.'s Office made to get you to stop writing the book.

A I don't think I am or can be required to respond to a question that seeks to probe my good faith invocation of the Fifth. I believe -- I know that I have a good faith basis to invoke my privilege. If your investigation should result in a declaration by the District Attorney's Office that they have no such intent, that criminal prosecution of me is never going to happen, then we will have a different exchange.

Q So if they write you a letter and they say they're declining to take any further action, you might be willing to come back and answer some of our questions?

A I would have a very different conversation with my attorneys.

Q When Mr. Jordan initially --

A It was hard enough for them on the record that we do have.

Q When we initially wrote to you in the earlier part of this year, the first letter --

A Yes.

Q Mr. Jordan sent you two letters, right?

A Yes.

Q He sent you the first letter asking for voluntary cooperation, and then it was followed up with the subpoena.

A Yes, sir.

Q You replied to our first letter -- thank you for that -- and basically said that the D.A.'s Office is telling you not to cooperate.

Can you tell us about the conversation you had with the D.A.'s Office before you wrote us back?

A I referenced and attached, I believe, a letter I received from Ms. Dubeck at the District Attorney's Office.

Q And did you have a telephone conversation with her?

Mr. [REDACTED] We can go off the record. Sorry.

[Discussion off the record.]

Mr. [REDACTED] We can go back on the record.

The Witness. Respectfully, I decline to answer your question about communications with the District Attorney's Office.

BY MR. [REDACTED]:

Q Okay. And then when we sent the subpoena to you --

A And I understand your -- withdrawn. Never mind. I already talked --

Q You can finish. I'm sorry.

A No, it's okay.

Q On our -- the second time we wrote you the letter --

A Yes.

Q -- and we included the subpoena, I emailed you, and you replied back very graciously and very professionally, you indicated that you didn't have a lawyer at that time. Is that correct?

A I think I said that I would be in touch with you after finalizing the arrangements for counsel.

Q And so, is it fair to say that in your conversations that you had with the D.A.'s Office, you weren't represented by counsel?

A I don't think that is fair to say. I don't know what time period you're referring to.

Q So we wrote -- our first letter was dated March 20th, and then the subpoena was April 6th, so -- and when I emailed the subpoena to you, at that time you hadn't engaged Mr. Wells?

Did you have different counsel, or was Mr. --

A I'm not going to get into who represented me when throughout the months preceding this appearance.

Q Okay.

Chairman Jordan. I don't think the question was who. I think the question was, was there anyone representing you in that time frame.

The Witness. I respectfully assert my Fifth Amendment rights in that regard.

BY MR. [REDACTED]

Q I mean, is it a fair investigative data point that if you didn't have counsel until Mr. Wells, which, you know, Mr. Wells was engaged after the subpoena was sent, and isn't that a fair piece -- good data point or piece of evidence that maybe shows that the interactions that you had had with the D.A.'s Office up until the time that you engaged Mr. Wells -- did you have an attorney is what we're getting to. And if you didn't, isn't it fair for us to conclude that that's a good piece of evidence showing that this might not be a real investigation that they're pursuing?

A I decline to answer your question.

Mr. [REDACTED] I would like to mark the indictment as exhibit 14, and then the statement of facts as exhibit 15.

[Pomerantz Exhibit Nos. 14 and 15

Were marked for identification.]

BY MR. [REDACTED]

Q You've read the indictment. Correct?

A The indictment of Donald Trump?

Q Yes.

A Yes.

Q Have you read the statement of facts?

A Yes.

Q Now, the indictment was returned by the grand jury, correct?

A I assume so.

Q But the statement of facts was not?

A I don't know.

Mr. [REDACTED] Okay. Well, let's -- this is number 14, the indictment.

Do we have the statement of facts one too?

Ms. [REDACTED] They are both marked.

Mr. [REDACTED] What's that?

Ms. [REDACTED] Yes.

Mr. [REDACTED] So you've got both the statement of facts and the indictment?

Mr. Witness. Yes, sir.

Mr. [REDACTED] Okay.

Ms. [REDACTED] Are these separate exhibits?

Mr. [REDACTED] They are 14 and 15.

Ms. [REDACTED] And 14 is the indictment?

Mr. [REDACTED] 14 is the indictment. 15 is the statement of facts.

BY MR. [REDACTED]:

Q Let me just ask you, what's the difference between utilizing -- based on your experience, utilizing a statement of facts to supplement an indictment versus a speaking indictment?

A I couldn't answer your question. I don't know the answer.

Q Okay. I mean, you were a prosecutor in the Office. Did you -- during your time with the D.A.'s Office, did you -- were you responsible for indicting anyone? Any cases that you worked on land in an indictment?

Ms. Dubeck. Objection to the extent it calls for nonpublic information.

The Witness. You referring to my tenure in the Manhattan District Attorney's Office?

BY MR. [REDACTED]

Q Correct.

A I respectfully decline to answer.

Q Okay. Could you just help us understand, how does a statement of facts ordinarily get released? What's the process?

A I can't help you understand that. I don't know the answer to that question.

Q Okay. In reading the indictment --

A Yes, sir.

Q -- can you tell us whether the D.A.'s Office found new evidence that you weren't aware of, you know, from your time in the Office?

Ms. Dubeck. Objection.

The Witness. I respectfully decline to answer.

BY MR. [REDACTED]

Q Okay. Is that based on the Fifth Amendment?

A I think tilting toward the fourth paragraph of my statement, without excluding the fifth.

Q The fourth paragraph, is that --

Mr. Finzi. It's the District Attorney's objections.

Mr. [REDACTED] Okay.

The Witness. My discipline slips as the day wears on, but I hope you'll make sure that I adequately state on the record the basis for my nonresponse.

BY MR. [REDACTED]

Q Okay. So there are 34 counts in the indictment that are bootstrapped to an unstated crime to prosecute.

Do you know what that unstated crime is?

Ms. Dubeck. Objection.

Mr. [REDACTED] Well, I'm just asking if he knows, and he's read the indictment. I think he can answer that question.

The Witness. I decline to answer that question on the basis of the fourth and fifth paragraphs of my statement.

BY MR. [REDACTED]

Q Okay. And can you help us understand why, in your experience, a prosecutor in this instance might -- like, what's the strategy behind not naming the crime in the indictment?

Ms. Dubeck. Objection.

Mr. [REDACTED] Well, I'm just asking, you know, his experience, and I'm just trying to better understand why the crime is not in the indictment, just his experience as a lawyer. I mean, you're a decorated, long-serving lawyer.

The Witness. I don't know how many decorations I got, but I have a long career

as a defense attorney and a prosecutor.

BY MR. [REDACTED]:

Q So you're in a good position, I think, to help us understand what's the strategy behind not naming the underlying crime.

Ms. Dubeck. Objection.

The Witness. I can't answer, and I decline to answer. Even if I could answer, I wouldn't know the answer.

BY MR. [REDACTED]

Q Okay.

A And I can't answer, so the state of my knowledge is basically irrelevant.

Q Okay.

Chairman Jordan. Mr. Pomerantz, you gave the District Attorney's Office a year of your life. You worked for free. And before Congress ever got in this picture, they told you they might -- that you might face criminal liability for a book that you wrote.

Does that tick you off?

The Witness. I decline to answer.

BY MR. [REDACTED]

Q And you didn't just work for free. You gave up your weekends. You gave up your -- you had -- according to your book, you had a month's long -- correct me if I'm wrong. But you had a month's long visit planned in Sonoma so you could be with one of your new grandchildren.

A 2 months.

Q 2 months. I mean, you gave quite a lot to this Office, the District Attorney's Office. Is that not, obviously, correct?

A I decline to answer.

Q I think we're --

A Regretfully.

Mr. [REDACTED] I think we're at our time.

Ms. [REDACTED] [REDACTED], do you have a lot left?

Mr. [REDACTED] Go off the record, please.

[Discussion off the record.]

[Recess.]

Ms. [REDACTED] It is 2:44. We can go back on the record.

BY MS. [REDACTED]

Q Mr. Pomerantz, in the prior hour you were asked about the Southern District of New York's determination about the reliability of Mr. Cohen as a witness.

Do you recall being asked about that?

A Yes.

Q And I believe that you said you couldn't answer -- you declined to answer the question?

A That's correct.

Q In your experience as a prosecutor and defense attorney, though, there are circumstances in which a witness may not be sufficient in one proceeding, but in an unrelated proceeding or a different proceeding there could be, for example, corroborating evidence or other material that might change the circumstances for that, on the witness's reliability, right?

A You're asking me in general terms?

Q In general, in general terms.

Mr. Finzi. Could we go off the record for 1 second?

Ms. [REDACTED] Sure. Yes, we can go off the record.

[Discussion off the record.]

Ms. [REDACTED] We can go back on the record.

The Witness. I think the only thing I can say is that, as my own testimony probably indicates, there's no such thing as a perfect witness. Witnesses have flaws and strengths that run the gamut of human behavior.

BY MS. [REDACTED]

Q You were asked earlier about the -- you know, when you had an attorney --

A Yes.

Q -- in relation to this year. And you recall that?

A Yes.

Q Without getting into who represented you and when, you know, you've now been brought before this committee for a deposition that's run, I don't know, 5 hours and change. Before that, there was a fair amount of letters and motions practice in court even.

Would you agree that anybody who was facing a congressional investigation may want to hire counsel?

A Yes.

Q I want to turn to the January 18th letter, and it was not introduced in the last round, so I am going to introduce it as exhibit 16 now.

Mr. [REDACTED]. Sorry, what number are we up to?

Ms. [REDACTED] I think it's 16.

Mr. [REDACTED]. Yes.

[Pomerantz Exhibit No. 16

Was marked for identification.]

BY MS. [REDACTED]

Q Do you recall receiving this letter?

A I received this letter.

Q And this was the letter I think that was referenced earlier when reference was made to the January 18, 2023, letter, correct?

A Yes.

Q This letter was sent from Ms. Dubeck, who is sitting at the table today, correct?

A Yes.

Q And it was addressed to you, but also to the general counsel of Simon & Schuster and the executive vice president and general counsel and secretary of Paramount Global, correct?

A Yes.

Q So this was sent to you, but also to attorneys. Correct?

A Yes.

Q And in the first line, the very first sentence of this letter, it says: "This letter is in response to Simon & Schuster's public announcement, on January 11, 2023, of the forthcoming publication of your book," correct?

A Yes.

Q So the announcement of your book -- according to just on the terms of this letter, the announcement of your book happened on January 11, 2023. It was publicized on that date, right?

A That's what the letter says.

Q And within a week of learning of that publication, the District Attorney's Office had written to you, correct?

A The letter reflects on its face having been sent a week after the public

announcement of the publication of the book that I wrote.

Q On the second page of the letter, the second full paragraph says that "Prior to commencing his work with the D.A.'s Office, Mr. Pomerantz acknowledged in writing his understanding that most or all of the information he would have access to regarding the investigation is protected by" -- and it goes on and refers to the grand jury secrecy provisions, correct?

A That's what the letter says.

Q Did you -- is it accurate that you signed a nondisclosure form or some other document prohibiting you from disclosing information that you learned?

A I'm not going to answer that question and assert my constitutional rights as reflected in the fifth paragraph of my statement.

Q In the following paragraph, it says: "In addition, because Mr. Pomerantz has been separated from the D.A.'s Office for nearly a year, he is not capable of making any assessment of whether the disclosures he intends to disseminate in this publication have a substantial likelihood of materially prejudicing an adjudicative proceeding," correct?

A That's what the letter says.

Q So the District Attorney's Office actually put you on notice that with publication of your book, you know, you unilaterally were not capable of determining whether that might prejudice an adjudicative proceeding, correct?

A Well, I'm not going to expand beyond what the letter says on its face. I'm not taking issue with your characterization.

Q Okay. It goes on: "Based on the pre-publication descriptions of the book and the benefit of current knowledge of the matter, but without access to the manuscript, this Office believes there is a meaningful risk that the publication will

materially prejudice ongoing criminal investigations and related adjudicative proceedings," right?

A Yes, that's what's stated in the letter.

Q So it says without access to the manuscript. So the District Attorney's Office, based on the face of this letter, did not have access to your manuscript prior to its publication, correct?

A I'm not going to respond to that question.

Q And then in the following paragraph, it cites to New York City Charter chapter 68, section 2604(d)(5)?

A Yes.

Q And are you familiar with that statute?

A As we sit here today?

Q Yes. We can withdraw it. That's fine.

A Thank you.

Q So the paragraph says that, in relevant part, chapter 68, section 2604(d)(5) provides that no public servant shall, after leaving city service, disclose or use for private advantage any confidential information gained from public service which is not otherwise made available to the public, correct?

A You've accurately stated what the letter contains.

Q And you don't have any reason to believe that this is not an accurate recitation of that code section, correct?

A I have no reason to believe that the letter misstates the language of that chapter of the city charter.

Q And then in the final --

A It doesn't state all of the language of that section of the city charter, but

what is here is contained in the city charter.

Q Thank you.

And then the final sentence of that paragraph reads: "To the extent this book discloses information, Mr. Pomerantz obtained as a public service without this office's approval, Mr. Pomerantz is unlawfully converting confidential government information for his personal advantage," right?

A That's what the letter says.

Q And so, as early as January 18, 2023, which was a week after the announcement that your book would be published, the District Attorney's Office had written to you to say that you were potentially acting unlawfully, correct?

A The letter says -- contains the language that you have referenced and speaks of the unlawful conversion of confidential government information.

Q And then the final sentence, the final paragraph of this letter, which is on page 3, it says: "The Office," referring to the District Attorney's Office, "urges Mr. Pomerantz not to take any further steps that would damage an ongoing criminal investigation," right?

A Yes. That's contained in the letter.

Q So, again, as early as January 18th, the District Attorney's Office had written to you and said, you know, Do not take any further steps that would damage an ongoing criminal investigation, correct?

A The letter says what it says.

Ms. [REDACTED] All right. Thank you. We don't have any further questions.

The Witness. Thank you.

We can go off the record.

[Discussion off the record.]

Mr. [REDACTED] Back on the record.

BY MR. [REDACTED]

Q This morning we were going through some of the investigative matters you were pursuing against former President Trump. I think we left off at the Trump Tower triplex apartment.

The angle there was that he overstated the value of the apartment, or was it that he overstated the square footage? I know Mr. Cohen said that the square footage was exaggerated. But were both subject to the -- were you pursuing both angles as a potential investigative avenue?

Ms. Dubeck. Objection.

The Witness. Once again, I decline to answer your questions for the reasons stated in the fourth and fifth paragraphs of my statement.

BY MR. [REDACTED]

Q The vignette, the John Baron vignette where he was having communications with the Forbes reporter, was that an avenue of independent investigation, or was that fact pattern going to be used to support a different charge?

Ms. Dubeck. Objection.

The Witness. I decline to answer for the reasons stated. I'm not sure I understand your question, but I'm sure however you meant it, I won't be answering it.

BY MR. [REDACTED]

Q Okay.

A With apologies. I don't mean to make light, and I intend no disrespect whatsoever.

Q I'm sorry. I'll restate it.

Do you remember the name of the Forbes reporter? I believe his first name was

Jonathan.

A I believe you're referring to Jonathan Greenberg.

Q Yes, sir, yes, sir.

So my question was the allegations that Mr. Greenberg brought forth from his reporting with Forbes was that, if I'm not mistaken, that Mr. Trump was overstating his overall net worth. And my question was whether that was an independent avenue of investigation, or whether that was you considered using the Forbes reporter to support the financial statement -- the statements of financial condition investigation that you were pursuing?

Ms. Dubeck. Objection.

A I decline to answer both because it calls for confidential or privileged information in view of the District Attorney's Office, and for the other reasons referenced in paragraphs 5 and 6 of my statement.

BY MR. [REDACTED]

Q In your book you talk about investigating the Trump Foundation, aspects of Trump University. And my question is, was there an independent investigation into Trump University that potentially could have been the source of an indictment, or were those facts -- that fact pattern simply going to be used in the enterprise corruption theory case that you were working on?

Ms. Dubeck. Objection.

The Witness. The same response as to the previous question. Same nonresponse, I guess.

BY MR. [REDACTED]

Q There were various insurance fraud matters that you write about in your book, such as there was tornado damage at one of the Florida golf courses, I believe.

There was some insurance fraud allegations relating to an elevator fire at the --

A I actually think you are incorrect to the extent you're referring to what's written in the book. The book references tornado damage to a golf course in Westchester.

Q Oh, I'm sorry. It was in New York. Okay.

Was there not also a potential insurance matter at one of the golf properties in Florida, or was that just simply the Westchester property?

Ms. Dubeck. Objection.

The Witness. I decline to answer to the extent that it calls for information that goes beyond what's referenced in the book.

BY MR. [REDACTED]

Q Okay. Do you remember if that was included in the book? Was there an insurance matter relating to a Florida golf course?

Ms. Dubeck. It's only calling for the book, so --

The Witness. I don't believe that appears in the book.

BY MR. [REDACTED]

Q Okay. On page --

A Perhaps I should have written a shorter book.

Q On page 205, you write regarding the District Attorney, that he was missing the urgency of the situation and underestimating the special needs of the Trump investigation and potential prosecution.

Was that something you ever confronted Mr. Bragg about personally?

Ms. Dubeck. Objection.

BY MR. [REDACTED]:

Q It's right in the middle of page 205.

A Yes, I see it. I decline to answer for the reasons previously stated. I do see the reference in the book.

Q Okay. On page 213, you had an in-person meeting with the District Attorney. Was that your first in-person meeting with him?

I understand because of the pandemic a lot of the work that you did was remote and meetings happened over Zoom. But at some point, you did have some meetings in person with Mr. Bragg. Is that correct?

Ms. Dubeck. Objection.

BY MR. [REDACTED]

Q You're reporting in your book you did.

A The book references meetings and conversations, a variety of them.

Q Okay. And do you know how many in-person meetings?

Ms. Dubeck. Objection.

The Witness. Decline to answer beyond what's contained in the book.

BY MR. [REDACTED]

Q Okay. Which number objection would that one be?

A Oh, the fourth paragraph and the fifth paragraph and the sixth paragraph of my statement.

Q The sixth paragraph, legislative purpose?

A No. The sixth paragraph references the First Amendment.

Q Oh, okay.

A And to the extent you're asking me to elaborate on the facts --

Q Oh, no, I'm sorry, sir. I'm not asking you to elaborate. I'm just wondering how many in-person meetings you had with the District Attorney, because you wrote about them all in the book and I --

Ms. Dubeck. Objection.

The Witness. I have nothing to add beyond the book. In fact. Well, I'll leave it there.

BY MR. [REDACTED]

Q Anyway, on page 213 towards the bottom, you write: "The discussion degenerated into chaos and confusion. On top of it, Alvin came into the meeting late, spent much of his time looking at his phone, and then left early, saying he just wanted to see the important documents, as though the whole sprawling case could be reduced to a collection of just a few" -- or sorry -- "collection of a few crucial documents, which made no sense."

Did you ever have a chance to communicate that to Mr. Bragg, your frustration?

Ms. Dubeck. Objection.

The Witness. I decline to answer that question for the reasons previously articulated.

BY MR. [REDACTED]:

Q Later on in the book I think you wrote an email to Mr. Bragg. And did you mention your frustration with him coming in late, looking at the phone, and so forth?

Ms. Dubeck. Objection.

A What is the question, whether I wrote an email to --

BY MR. [REDACTED]

Q Whether you expressed your frustrations to Mr. Bragg. I mean, if you just remember whether you did or didn't.

Ms. Dubeck. Objection.

The Witness. Well, the issue was not the state of my recollection. It's the application of the privilege that I asserted, which I will rely on?

BY MR. [REDACTED]

Q Did you spend -- do you think Mr. Bragg was as willing as Mr. Vance to dig into the facts of this case?

Ms. Dubeck. Objection.

The Witness. I refuse to answer that question, Mr. [REDACTED] respectfully.

BY MR. [REDACTED]

Q Okay. For the most part in your book, and I think without exception, you refer to Mr. Vance in a very favorable light. Is that a fair assessment?

A I'm not taking issue with your perception, but I have nothing to add to what appears in the book.

Q Okay. On page 264 --

A Yes.

Q -- there's a part of the book that says: "Most plane crashes" -- I'm sorry. "All I know for sure is that the investigation turned into the legal equivalent of a plane crash. Most plane crashes have more than a single cause, and this one also may have had multiple causes. The biggest one, in my opinion, was 'pilot error.' Alvin made the wrong decision about whether to charge the case."

When you wrote the biggest cause of the metaphorical plane crash was pilot error, were you referring to Mr. Bragg as the pilot in that instance?

A I won't go beyond the language that appears in the book. Again, I'm not taking issue with the inference that you draw, but the book speaks for itself. And I object to being compelled to make statements that go beyond what appears in the book.

[3:08 p.m.]

Mr. [REDACTED] Okay. On page 265, the penultimate paragraph, last sentence.

The Witness. Yes.

Mr. [REDACTED] "He jumped into very deep water and immediately was in over his head."

Is that a reference to Mr. Bragg?

Ms. Dubeck. Objection.

The Witness. Again, the book speaks for itself.

BY MR. [REDACTED]

Q Page 218.

A Yes.

Q You write: "As I tossed and turned, I asked myself whether we had done everything we could do to convince Alvin to let us bring our case against Trump. I kept thinking that maybe we were being rash.

"I also thought about Alvin's relative youth and wondered if he was in over his head. From what I knew, he had never run an organization anywhere close to the size of the District Attorney's Office, and he had scant experience in leading or defending high-profile prosecutions."

That view that you expressed about Mr. Bragg, have you since come to a decision to revise that conclusion?

A I decline to answer on the basis of my privilege against self-incrimination.

Q Okay. You know, in several -- you know, you mentioned on page 208 that when you were getting out of law school, Mr. Bragg was a toddler.

A Yes, I recall that sentence.

Q And you, by all accounts, are experienced, but you're not that old.

A At times --

Q And Mr. Bragg is not that young. I mean, he's almost 50.

A At times, I feel very old, Mr. [REDACTED] and this is one of those times.

Q Fair enough. But at the time, Mr. Bragg -- I mean, he's almost 50 years of age, as far as I understand. I mean, he's not that young.

A He seems younger and younger to me as I get older and older. I notice that with a lot of people.

Q Okay.

A I'm 72 as we speak.

Q Right. So do you think his relative youth played a part in -- like, do you think he's not capable of running the office?

Ms. Dubeck. Objection.

The Witness. I did not say that in the book, and I'm not going to comment on that. And I'm asserting my rights, as my lawyer reminds me.

Mr. [REDACTED] Were you surprised -- in light of the first day memo and in light of the progressive agenda the District Attorney has advanced -- were you surprised at the resources devoted to the Trump matter as compared to some of the basic crime that most district attorney's offices make a priority?

Ms. Dubeck. Objection.

The Witness. I decline to answer for the reasons indicated.

Mr. [REDACTED] In 2022, Mr. Bragg's first year as the D.A., crime in New York City rose significantly when compared to the previous year. According to NYPD data, New York City saw a 23 percent surge in major crimes.

Do you think there's different things the office can do to address that crime surge, given your experience with the office?

Ms. Dubeck. Objection, to the extent it calls for information about his experience with the office.

The Witness. What was your question again? Do I think there are different things the office can be doing?

Mr. [REDACTED]. Yeah. What can the office do differently to deal with this crime epidemic? I mean, they're devoting a lot of resources -- a tremendous amount of resources to the Trump prosecution. And they're doing this, and at the same time, there's just a raging crime epidemic.

The Witness. I'm not necessarily acquiescing in your characterization. Having said that, I have no ability to hold forth on what a district attorney's office can or should do with regard to the problem of street crime and violent crime and thefts and so on.

If I had a view, my lawyer would probably tell me not to share it. And in fact, I don't have the expertise to express a view on that.

Mr. [REDACTED]. Okay.

Chairman Jordan. You related in your book, Mr. Pomerantz, that -- I believe your son is an officer in the NYPD?

The Witness. My son is a lieutenant in the NYPD.

Chairman Jordan. I appreciate his service.

You related in there an exchange of, I think, text messages and conversations you had with him regarding the day one memo, which seemed to indicate that he did not have a very high regard for what was contained in that memorandum.

The Witness. I respectfully decline to answer your question and do so, in particular, with regard to paragraph 6 of my statement. I really have to object to the notion that my son's views as a New York City police officer, whatever they may be, are germane to your legislative purpose.

Chairman Jordan. With all due respect, Mr. Pomerantz -- and, again, we appreciate your son's service. We appreciate your service.

We have a crime subcommittee on the Judiciary Committee. We are concerned about crime. We are concerned about Federal funds being used in the District Attorney's Office and they're not prosecuting bad guys who do bad things to people. And we know that it's happening in the city of New York. That's why we did a hearing there just a few weeks ago.

So that was the motivation for the question.

The Witness. I understand.

Chairman Jordan. Thank you.

Mr. [REDACTED] You referenced various outside law firms. Two firms assisted with the so-called Zombie theory?

Ms. Dubeck. Objection.

Mr. [REDACTED] Was that the same firm or a different firm? Not asking you -- I mean, I'd like to know the name of the firm. Will you tell me the names of the firms?

Ms. Dubeck. Objection.

The Witness. No.

Mr. Wells. It's getting late, guys.

The Witness. I respectfully decline -- well, I did answer your question, I guess, literally speaking. The question was whether I would tell you, and I answered no.

BY MR. [REDACTED]

Q Okay. Was it the same firm?

The Zombie case, there's a legal theory that -- various legal theories -- that needed to be run to ground. In your book, you talk about how there is an outside law firm helping the D.A.'s Office. And I asked you for the name of that law firm. It's

mentioned at two different points.

In the fall of 2019, before you joined the District Attorney's Office, they commissioned -- and this is on page 40 -- they commissioned an outside firm. And then, when you joined the District Attorney's Office and you were looking at whether the money laundering -- the money laundering idea could be used, you went back, as I understand it, and had the help of an outside law firm.

So my question is, what was the name of those firms, and were they different?

A First, I think your question misstates the facts --

Q Okay.

A -- in the sense that the book does not reference getting an outside counsel's opinion with respect to potential money laundering charges.

Q Okay.

A The book does reference outside opinions with regard to false statement and the predicate acts necessary to elevate a false filing charge from a misdemeanor to a felony.

And you correctly point out that the book references a law firm at one point and also references a law firm at a separate point. And now your question is whether those were the same law firms.

Q Correct.

A And having clarified your question, I refuse to answer it for the reasons indicated in my statement.

Q When you were working on your -- on the SOFC matter in late March, you wrote in your book that, "The District Attorney's Office began ramping up work that our outside consultant, FTI, was doing to parse Trump's tax returns and financial statements."

What was FTI doing for the District Attorney's Office?

Ms. Dubeck. Objection.

The Witness. The question was what was FTI doing for the District Attorney's Office?

BY MR. [REDACTED]:

Q Right.

A Yeah, I decline to answer that question for the reasons indicated in my statement.

Q And why is it that on one hand you're willing to name FTI in the book but not the law firms?

A I decline to answer your question on the advice of my counsel. Well, I should say, generally, I'm trying to follow the advice of my counsel each and every time I assert my rights.

Q You mention in the book the assistance of lawyers from the Paul, Weiss firm as well as the Davis Polk firm?

A You're referring, I believe, to lawyers described in the book as having been seconded to the District Attorney's Office?

Q Correct. The work that those lawyers were performing, was that the same work as the outside law firms were consulted on, or were they two different subject matters?

Ms. Dubeck. Objection.

The Witness. I decline to answer for the reasons previously stated.

Mr. [REDACTED] Is there any prohibition from the District Attorney's Office to get free help from outside law firms that you're aware of?

Ms. Dubeck. Objection.

The Witness. I decline to answer the question. I'll leave it there.

Mr. [REDACTED]. In the congressional context, for example, if a government agency was using the services of a law firm for free, there would be issues because that money is not authorized or appropriated and so forth.

And I'm wondering if there's any companion idea in the District Attorney's Office or is there just no restrictions on how much free help they can get.

Ms. Dubeck. Objection.

The Witness. I decline to answer the question for the reasons stated.

Mr. [REDACTED]. Okay.

Chairman Jordan. Can I?

Mr. Pomerantz, in the letter that Ms. Dubeck sent you as general counsel for the D.A.'s Office -- Ms. Dubeck, who's been here with us this entire time representing the D.A.'s Office -- that she sent to the lawyer for Paramount, I think the parent company for Simon & Schuster, she sent the letter to the general counsel for Simon & Schuster and to you on the 18th. And they make clear in the letter they discovered that you were going to publish a book based on an announcement from your publisher, Simon & Schuster, and then they send you the letter on the 18th.

Did you talk with them, did you try to work it out, when they tell you on the 18th? Because my understanding is the book -- you get this letter on the 18th, and the book is published the next month. Did you have communications with them trying to work this out?

The Witness. The book was published on February 7th, 2023. And I decline to answer whether there were any conversations between the date of the letter and February 7th.

Mr. Wells. Just so the record is clear, that's January? It that the January letter?

Chairman Jordan. January 18th, 2023. It's exhibit 16, the letter from

Ms. Dubeck to Mr. Pomerantz and Simon & Schuster and the parent company.

Did you think about, when you got the letter, did you think about, "Wait a minute, let's put the brakes on this"?

The Witness. I respectfully decline to answer on the grounds of -- on the basis of my Fifth Amendment rights.

Chairman Jordan. Is it fair to say if you would have -- if you'd have held back on publishing the book, that there would have been no need for this letter?

If you told them, "You know what?" -- let's say it this way. If you held back on publishing the book, didn't publish the book, that you wouldn't be facing possible criminal liability?

The Witness. I respectfully decline to answer.

Chairman Jordan. Okay.

Mr. [REDACTED] But I guess what Mr. Jordan is getting to is, were there any conversations before the letter came that could have resolved the situation?

The Witness. Prior to the letter?

Mr. [REDACTED] Right.

Chairman Jordan. Between the 11th -- when Simon & Schuster announces "People v. Donald Trump, An Inside Account" by Mark Pomerantz is going to be available at some date -- between the 11th and the 18th, when they send you the letter, did you talk to them?

The Witness. Yes, I decline to answer that question.

Chairman Jordan. Okay.

Mr. [REDACTED] And am I also correct that you're declining to answer whether you had any communications with them outside of the letter?

The Witness. Yes.

Mr. [REDACTED] Okay. I think we're done. We'll go off the record.

[Whereupon, at 3:24 p.m., the deposition was concluded.]

Certificate of Deponent/Interviewee

I have read the foregoing ____ pages, which contain the correct transcript of the answers made by me to the questions therein recorded.

Witness Name

Date



**LAWFARE: HOW THE MANHATTAN DISTRICT ATTORNEY’S OFFICE AND A NEW
YORK STATE JUDGE VIOLATED THE CONSTITUTIONAL AND LEGAL RIGHTS
OF PRESIDENT DONALD J. TRUMP**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government
U.S. House of Representatives



July 9, 2024

EXECUTIVE SUMMARY

On April 4, 2023, Manhattan District Attorney Alvin Bragg announced that he secured a 34-count criminal indictment against President Trump that bootstrapped misdemeanor state charges for allegedly falsifying New York business records to an ambiguous, unknown federal crime to aggravate the charges to felonies.¹ The indictment focused on payments that former Trump employee Michael Cohen made to Stephanie Clifford (also referred to as Stormy Daniels) in 2017. Legal experts have detailed serious legal and constitutional deficiencies with Bragg’s politicized prosecution. First, as one legal scholar explained, even if the alleged bookkeeping irregularities “amount[ed] to fraud crimes . . . the transactions in question could not possibly have had the slightest impact on the 2016 election. They didn’t occur until months later—specifically, from February 14 through December 5, 2017.”² Second, “even if Bragg had jurisdiction to enforce federal campaign finance law” and “even if Bragg were correct that the . . . payments were in-kind campaign contributions that had to be disclosed,” any disclosure would have been due “several months into 2017. Again, there could not conceivably have been any impact on the 2016 election.”³

In March 2023, the Judiciary Committee opened an investigation into Bragg’s unprecedented indictment of President Trump, including by requesting that former Manhattan Special Assistant District Attorney Mark Pomerantz provide relevant documents and testimony pertaining to his role leading the investigation into President Trump.⁴ On instructions from Bragg, Pomerantz refused to cooperate with our oversight.⁵ The Committee issued a subpoena for Pomerantz’s testimony, litigated it in the U.S. District Court for the Southern District of New York upon Bragg’s objection, and prevailed, resulting in Pomerantz appearing for a deposition before the Committee on May 12, 2023.⁶ Despite Pomerantz’s conduct at the deposition—he refused to answer the most basic of questions—the Committee’s investigation proved fruitful.⁷ On April 25, 2024, the Committee released its interim findings—in short, Bragg’s prosecution of President Trump was politically motivated, unethically and likely unlawfully focused solely on one person, and “opened the door for future prosecutions of a former president—or current candidate—that would be widely perceived as politically motivated.”⁸

On May 15, 2024, the Judiciary Committee’s Select Subcommittee on the Weaponization of the Federal Government held a hearing highlighting the weaponization of the rule of law

¹ Press Release, N.Y. Cnty. Dist. Atty’s Office, District Attorney Bragg Announces 34-County Felony Indictment of Former President Donald J. Trump (Apr. 4, 2023) [hereinafter “Bragg Press Release”].

² Andrew C. McCarthy, *Bragg’s case against Trump is utterly incoherent*, N.Y. POST (Apr. 5, 2023).

³ *Id.*

⁴ Letter from Rep. Jim Jordan, H. Comm. on the Judiciary, to Mr. Mark F. Pomerantz, Former N.Y. Cnty. Special Assistant District Att’y (Mar. 22, 2023) [hereinafter “Mar. 22, 2023 Letter to Pomerantz”].

⁵ Letter from Mr. Mark F. Pomerantz, Former N.Y. Cnty. Special Assistant District Att’y, to Rep. Jim Jordan, H. Comm. on the Judiciary (Mar. 27, 2023).

⁶ *See* Opinion and Order Denying Temporary Restraining Order, *Bragg v. Jordan*, 1:23-cv-3032 (MKV) (S.D.N.Y. Apr. 19, 2023); STAFF OF THE H. JUDICIARY COMM., 118TH. CONG., AN ANATOMY OF A POLITICAL PROSECUTION: THE MANHATTAN DISTRICT ATTORNEY’S OFFICE’S VENDETTA AGAINST PRESIDENT DONALD J. TRUMP, at 3 (Apr. 25, 2024) [hereinafter “ANATOMY OF A POLITICAL PROSECUTION”].

⁷ ANATOMY OF A POLITICAL PROSECUTION at 3.

⁸ *Id.* at 34.

through the use of lawfare tactics and exposing the two-tiered justice system that extends from the highest offices in the Department of Justice to the offices of politically ambitious state and local prosecutors. The Committee heard testimony from former federal prosecutor James Trusty, who testified about the dangers of lawfare, or, as Trusty put it, “an end-justify-the-means mentality” that is the “antithesis of justice.”⁹ The Committee also heard from Gene Hamilton, a former Department of Justice official, who highlighted the unprecedented use of lawfare against President Biden’s political opponents. Finally, the Committee also heard from Robert Costello, Michael Cohen’s former attorney, who testified about Cohen’s credibility and highlighted the deficiencies in Cohen’s testimony.

On June 13, 2024, the full Committee on the Judiciary convened a hearing to further examine the left’s use of lawfare to target political adversaries.¹⁰ The Committee heard testimony from experts that President Trump’s prosecution in Manhattan was riddled with defects. The Committee heard testimony from Federal Election Commission (FEC) Commissioner James “Trey” E. Trainor, III who explained how Bragg’s prosecution was “a significant deviation” from a well-established legal framework as Bragg “usurped the jurisdiction that Congress [] explicitly reserved for federal authorities.”¹¹ The Committee also heard from a constitutional law scholar and attorney Elizabeth Price Foley who explained in detail how the trial violated President Trump’s constitutionally protected due process rights. Finally, the Committee heard from Missouri Attorney General Andrew Bailey who drew on his expertise as Missouri’s chief law enforcement officer to discuss how Bragg’s prosecution was clearly “politically motivated and replete with legal error.”¹²

A fundamental principle of the American system of justice is that no individual is above the law. But just as important is the precept that prosecutors prosecute conduct, not individuals. Manhattan District Attorney Alvin Bragg, however, ran for office on a platform of investigating and prosecuting President Trump, bragging about his extensive experience suing President Trump. Although Bragg was initially hesitant to bring charges once he became district attorney, he faced intense political pressure to do so, including a leaked resignation letter from a special assistant district attorney who attacked Bragg for being too timid. That same prosecutor, Mark Pomerantz, later authored a tell-all book in which he took Bragg to task for failing to prosecute President Trump. Unsurprisingly, just months after Pomerantz’s book premiered—and *after* President Trump declared his candidacy for the 2024 Republican presidential nomination¹³—Bragg succumbed to this political pressure and filed charges relying on Pomerantz’s theory of the case.

⁹ *Hearing on the Weaponization of the Federal Government, Before the H. Comm. on the Judiciary*, 118th Cong. (May 15, 2024) [hereinafter “May 15, 2024 Weaponization Hearing”] (written testimony of James Trusty).

¹⁰ *Hearing on the Manhattan District Attorney’s Office Before the H. Comm. on the Judiciary*, 118th Cong. (2024) [hereinafter “Manhattan District Attorney Hearing”].

¹¹ Manhattan District Attorney Hearing (Written testimony of Comm’r James E. “Trey” Trainor, III, Fed. Election Comm’n [hereinafter “Trainor Written Testimony”]).

¹² Manhattan District Attorney Hearing (written testimony of Attorney General Andrew Bailey).

¹³ Gabby Orr, *et al.*, *Former President Donald Trump announces a White House bid for 2024*, CNN (Nov. 16, 2022).

This interim staff report explains the several ways in which Bragg’s prosecution of President Trump suffers from severe legal and procedural defects. These infirmities include, but are not limited to:

- Bragg’s unconstitutional and unprecedented Russian-nesting-doll theory of criminal liability, in which the jury never had to reach unanimity beyond a reasonable doubt as to each element of the criminal offenses;
- Bragg’s usurpation of the federal government’s exclusive authority to prosecute alleged violations of federal campaign finance laws and the Biden-Harris Administration’s refusal to intercede to protect federal interests; and
- Judge Merchan’s egregious legal rulings before and during the trial that all cut against President Trump’s rights, including:
 - Judge Merchan’s failure to recuse himself for manifest political bias against President Trump;
 - The unconstitutional gag order he imposed on President Trump during the trial;
 - Judge Merchan’s admission of plainly inadmissible, irrelevant, and unfairly prejudicial testimony against President Trump; and
 - Judge Merchan’s refusal to permit former Federal Election Commission Chairman Bradley Smith to testify as to the meaning and complexities of the Federal Election Campaign Act.

President Trump never had a real shot at a fair trial in Manhattan. In a more neutral jurisdiction, where a politically ambitious prosecutor was not motivated by partisanship and a trial judge with perceived biases did not refuse to enforce a fair proceeding, President Trump would have never been found guilty.¹⁴ But Manhattan is anything but a neutral jurisdiction. President Trump promised to appeal, stating, “We will fight for our constitution. This is far from over.”¹⁵ But the Democrats’ use of lawfare accomplished its short-term goal—it removed President Trump from the campaign trail and diverted attention away from President Biden’s missteps and failing policies.

Since Alvin Bragg announced last year his political prosecution of President Trump, the Committee and Select Subcommittee have conducted oversight of politically motivated prosecutions and the partisan use of lawfare to achieve political ends. The state or local prosecution of a current or former president by a popularly elected district attorney raises substantial federal interests and raises serious concerns about conflict between state and federal entities. While Bragg and Congressional Democrats dismiss these concerns, the Committee has taken steps to ensure that certain federal officials may have a fair trial in a more neutral venue. The Committee’s and Select Subcommittee’s oversight work is not done, but this interim report presents the facts about how the Manhattan District Attorney’s Office and a Manhattan judge worked together to deprive President Donald J. Trump of his constitutional and legal rights.

¹⁴ James Lynch, *Trump Found Guilty on All Counts in Hush-Money Trial*, NAT’L REV. (May 30, 2022).

¹⁵ *Id.* (internal quotation marks omitted).

TABLE OF CONTENTS

Executive Summary	1
Table of Contents	4
I. Introduction.....	5
A. Alvin Bragg’s Political Prosecutorial Pursuit of President Trump	7
B. Bragg Relied on Convicted Perjurer Michael Cohen to Convict President Trump.....	11
II. Bragg’s “Russian-nesting-doll” Theory of Criminality and Judge Merchan’s Equally Bizarre Jury Instructions Violated President Trump’s Due Process Rights	14
III. Bragg Usurped the Authority of the Justice Department and Federal Election Commission by Pursuing Charges Against President Trump Related to Alleged Violations of Federal Campaign Finance Laws	21
IV. Judge Merchan’s Rulings During the Trial Violated President Trump’s Constitutional Rights Inside and Outside of the Courtroom.....	25
A. Judge Juan Merchan’s Political Bias Prejudiced President Trump	25
B. Judge Merchan Unconstitutionally Silenced President Trump.....	27
C. Judge Merchan Permitted DA Bragg to Prejudice President Trump at Trial by Permitting Inadmissible Testimony	28
D. Judge Merchan Deprived President Trump of a Constitutionally Fair Trial by Refusing to Allow Former FEC Commissioner Bradley Smith to Testify as an Expert Witness on President Trump’s Behalf	30
Conclusion	33

I. INTRODUCTION

The New York County District Attorney’s Office’s (DANY) multi-year investigation into former President Donald J. Trump—and subsequent indictment and prosecution—is unprecedented. Since at least 2018, the DANY has weaponized the New York criminal justice system, combing through every aspect of President Trump’s personal life and business affairs in an effort to indict and convict him of a crime, no matter how ill-conceived, contrived, or unlawful the theory of criminal liability.¹⁶

Around the time the DANY began its pretextual investigation into President Trump, Michael Cohen, President Trump’s former disgraced lawyer—and Bragg’s star trial witness—pleaded guilty to five counts of willful tax evasion; one count of making false statements to a bank; one count of causing an unlawful campaign contribution; and one count of making an excessive campaign contribution in federal court.¹⁷ Federal prosecutors in Manhattan described Cohen’s criminal conduct in that case as “knowing and calculated acts—acts Cohen executed in order to profit personally, build his own power, and enhance his level of influence.”¹⁸ Three months later, Cohen pleaded guilty to lying to Congress.¹⁹ By July 2019, the U.S. Attorney’s Office for the Southern District of New York (SDNY) ended its investigation into payments made by Cohen to Stephanie Clifford. Federal prosecutors determined that no additional people would be charged alongside Cohen and that no one else—including President Trump—was responsible for the conduct.²⁰

Although the SDNY ended its investigation, the DANY under the leadership of Cyrus (“Cy”) Vance continued its investigation. In mid-2019, the DANY interviewed Cohen in prison²¹ and, by October 2019, the DANY gathered some of the facts related to the payments that Cohen made to Clifford.²² In late 2019, however, Vance decided not to bring charges “against anyone in connection with the . . . money paid to Clifford or the [allegedly] phony invoicing scheme by which Michael Cohen had been reimbursed for the money he had laid out.”²³

Nonetheless, Vance continued with the investigation. In December of 2020, Carey Dunne, who at the time served as counsel to Vance, asked Mark Pomerantz to join a group of outside advisors to Vance’s team investigating President Trump, which Pomerantz accepted

¹⁶ MARK POMERANTZ, *PEOPLE VS. DONALD TRUMP: AN INSIDE ACCOUNT* (2023) [hereinafter “POMERANTZ”]; Andrew Feinberg, *New York prosecutors warn Trump of possible indictment, report says*, THE INDEPENDENT (Mar. 10, 2023).

¹⁷ Press Release, U.S. Attorney’s Office, Southern District of New York, Michael Cohen Pleads Guilty In Manhattan Federal Court To Eight Counts, Including Criminal Tax Evasion And Campaign Finance Violations (Aug. 21, 2018); Information, *United States v. Cohen*, No. 18-cr-602 (S.D.N.Y. Aug. 21, 2018).

¹⁸ The Government’s Sentencing Memorandum at 27-28, *United States v. Cohen*, No. 18-cr-602 (S.D.N.Y. Dec. 7, 2018).

¹⁹ Information, *United States v. Cohen*, No. 18-cr-850 (S.D.N.Y. Nov. 29, 2018).

²⁰ See POMERANTZ at 1; Mark Berman, *et al.*, *The prosecutor, the ex-president and the ‘zombie’ case that came back to life*, WASH. POST (Mar. 17, 2023); Shawna Chen, *Timeline: The probe into Trump’s alleged hush money payments to Stormy Daniels*, AXIOS (Mar. 18, 2023); Mar. 22, 2023 Letter to Pomerantz, *supra* note 4.

²¹ Kara Scannell, *et al.*, *Trump defense cross-examines Michael Cohen in hush money trial*, CNN (May 14, 2024) (“Cohen confirms first time he met DA office officials was 3 months into his prison sentence[.]”).

²² See Berman, *supra* note 20; Chen, *supra* note 20.

²³ POMERANTZ at 41-42.

immediately.²⁴ Throughout 2020 and 2021, the DANY’s investigation of President Trump continued.²⁵ In his self-serving book, *People v. Trump: An Insider’s Account*, Pomerantz explained the many legal theories that the DANY considered to prosecute President Trump and he made clear that his goal was to prosecute President Trump—it was just a matter of finding the crime to pin on the President.²⁶

After President Trump left office, Pomerantz revisited “whether there were other felony charges that could be brought in connection with the payment that Cohen had made to Clifford and the ensuing [alleged] coverup.”²⁷ Pomerantz concocted a “novel legal theory” under New York’s money laundering statute, which he admitted was “neither intuitive nor obvious.”²⁸ According to Pomerantz, money laundering is a series of financial transactions that are designed to “conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of criminal conduct.”²⁹ This theory was “novel” because the “proceeds” were based on Clifford’s criminal conduct—namely, her “extortion of Donald Trump.”³⁰ That theory, however, went nowhere because New York’s money laundering statute required the payments that Cohen allegedly agreed to be made on President Trump’s behalf—or the “dirty money”—to have been actually received by Clifford.³¹

Pomerantz then began focusing on President Trump’s Statements of Financial Condition (SOFC), which he believed, based on Cohen’s claims, must be criminal.³² Pomerantz examined multiple years’ worth of the financial statements made for multiple golf properties, Deutsche Bank, the Old Post Office Hotel, Doral Resort, Trump International Hotel & Tower in Chicago, Mar-A-Lago, Seven Springs, 40 Wall Street, the Triplex Apartment, and Trump Tower.³³

Despite repeated failure, Pomerantz considered another novel theory of criminal liability—charging President Trump under New York’s Enterprise Corruption statute for “pattern crimes.”³⁴ Under this theory, Pomerantz attempted to amalgamate several unrelated and baseless allegations against President Trump into a crime. Pomerantz was not subtle. He prejudged the results of this case and had decided that President Trump would be prosecuted for some crime—any crime. It was only a matter of pinning a crime on him.

Pomerantz faced one major hurdle in his pursuit of President Trump: his colleagues did not entirely agree with him. For daring to question his novel theories, Pomerantz accused his fellow DANY lawyers and investigators of being “relentlessly negative, dwelling on all the difficulties and issues with the case, and refusing to acknowledge the positives” during an internal meeting on December 10, 2021, where he referred to his former colleagues as

²⁴ POMERANTZ at 4.

²⁵ See generally POMERANTZ.

²⁶ *Id.*

²⁷ POMERANTZ at 43-44.

²⁸ *Id.* at 58.

²⁹ *Id.* at 44; N.Y. PENAL LAW § 470.10.

³⁰ POMERANTZ at 57.

³¹ *Id.* at 60.

³² *Id.* at 97-100.

³³ *Id.* at 64, 74, 99, 152, 165, 167, 185, 208.

³⁴ *Id.* at 105-106.

“conscientious objectors”³⁵ for stating that the obvious: the case was “weak” and had “many fatal flaws.”³⁶ Rather than engage in meaningful reflection and attempt to meet the concerns of his colleagues, Pomerantz dismissed them as either too lazy to do the work, ignorant of the evidence, or afraid of bringing charges against President Trump.³⁷

A. Alvin Bragg’s Political Prosecutorial Pursuit of President Trump

Throughout his run for district attorney, Alvin Bragg made President Trump a focal point of his campaign.³⁸ On December 13, 2020, for instance, Bragg stated:

Let’s talk about what’s waiting for the new DA. The docket. We know there’s a Trump investigation. I have investigated Trump and his children and held them accountable for their misconduct with the Trump Foundation. I also sued the Trump administration more than 100 times for DACA, the travel ban, separation of children from their families at the border. So I know that work. I know how to follow the facts and hold people in power accountable.³⁹

On March 17, 2021, Bragg stated that, as district attorney, he “will hold [Trump] accountable”⁴⁰ Similarly, on March 23, 2021, he boasted that he had “sued the Trump administration over 100 times”⁴¹ In June 2021, Bragg stated, “It is a fact that I have sued Trump more than a hundred times. I can’t change that fact, nor would I. That was important work. That’s separate from anything that the D.A.’s office may be looking at now.”⁴² In Bragg’s view, he had one purpose: to prosecute President Trump.

On January 1, 2022, Bragg was sworn in as the New York County District Attorney.⁴³ Immediately upon taking office, Bragg issued a ten-page manifesto that promised radically soft-on-crime, anti-victim policies in New York County.⁴⁴ This so-called “Day One” memorandum, dated January 3, 2022, instructed his assistant district attorneys not to prosecute several crimes,

³⁵ Of his DANY colleagues, Pomerantz stated: “[I]t was frustrating to feel like we were about to march into battle, and were strapping on our guns and equipment, but when we looked around at the rest of the platoon we saw a lot of conscientious objectors.” *Id.* at 194.

³⁶ *Id.* at 191–92, 194.

³⁷ *Id.* at 160, 171–72.

³⁸ See, e.g., Maria Ramirez Uribe & Loreben Tuquero, *Here’s what Manhattan District Attorney Alvin Bragg said about Donald Trump during his DA campaign*, POLITIFACT (Apr. 12, 2023); Katelyn Caralle, *Meet the Dems competing to prosecute Trump: Manhattan DA candidate BRAGGED about suing Donald ‘more than 100 times’ – while his opponent interviewed to be federal judge but didn’t get it*, DAILY MAIL (June 2, 2021).

³⁹ Uribe & Tuquero, *supra* note 38.

⁴⁰ *Id.*

⁴¹ Emily Ngo, *Why the Manhattan DA Candidates Say They’re Ready to Take on the Trump Investigation*, SPECTRUM NEWS NY 1 (Mar. 23, 2023).

⁴² Jonah E. Bromwich, *et al.*, *2 Leading Manhattan D.A. Candidates Face the Trump Question*, N.Y. TIMES (June 2, 2021).

⁴³ Michael Gold & Jonah E. Bromwich, *Who Is Alvin Bragg, the D.A. Leading the Prosecution of Trump*, N.Y. TIMES (Apr. 13, 2023).

⁴⁴ Letter from Alvin L. Bragg, Manhattan Dist. Att’y, to Manhattan Dist. Att’y Staff (Jan. 3, 2022) [hereinafter “Day One Memo”].

including trespassing, resisting arrest, and engaging in prostitution.⁴⁵ Bragg would no longer prosecute armed robberies as felonies.⁴⁶ Rather, he directed that armed robberies be considered as misdemeanor larcenies unless someone was shot during the course of the robbery.⁴⁷ Moreover, Bragg announced that his office would not seek prison sentences for criminal defendants unless they were charged with homicides, domestic violence felonies, sex crimes, and public corruption.⁴⁸ Bragg directed his prosecutors not to request prison sentences in excess of 20 years, absent “exceptional circumstances.”⁴⁹ The public backlash that followed—including from local law enforcement—forced Bragg to walk back some of the policies in his Day One memo.⁵⁰

Meanwhile, despite campaigning heavily on his goal of prosecuting President Trump, Bragg realized that the case against President Trump was thin. On January 8, 2022, Pomerantz told Bragg that his case against President Trump “was ready to be charged.”⁵¹ On January 11, 2022, Pomerantz and Dunne presented former President Trump’s financial statements to Bragg and his team in support of their theory of prosecution.⁵² Bragg’s team, however, expressed “considerable angst” about using Cohen as a witness and sought to pivot away from Pomerantz’s proposed fraud charges.⁵³ On January 24, 2022, an investigative team meeting “quickly degenerated into a whirlwind of negativity” because other DANY officials rightly questioned the credibility of Pomerantz’s main witness, Michael Cohen.⁵⁴

Shortly thereafter, within the first few weeks of February 2022, Pomerantz and Dunne held several conversations with Bragg and his team to explain their multi-faceted investigation into President Trump.⁵⁵ Pomerantz argued that the case against President Trump based upon the Clifford payment facts—famously known as the “zombie” case—had multiple pitfalls, and notwithstanding possible “work-arounds,” none were appealing.⁵⁶ Further, his DANY colleagues were “dubious about whether Trump had been ‘extorted’ in the first place.”⁵⁷ Bragg therefore halted the investigation into President Trump despite “fac[ing] incredible political pressure from

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ Nicole Gelinas, *Let’s Break Down Exactly What Manhattan DA Alvin Bragg’s Memo Says*, N.Y. POST (Jan. 11, 2022).

⁴⁸ Day One Memo.

⁴⁹ *Id.*

⁵⁰ Jonah E. Bromwich, *Manhattan D.A. Sharpens Crime Policies That Led to Weeks of Backlash*, N.Y. TIMES (Feb. 4, 2022).

⁵¹ POMERANTZ at 205-07.

⁵² *Id.* at 207-08.

⁵³ *Id.* at 208-209 (internal quotation marks omitted).

⁵⁴ *Id.* at 212 (“As I started to detain Cohen’s potential testimony against Trump, Susan Hoffinger brought her phone out to play a recording of one of Cohen’s recent media appearances, in which he had taken credit as the person who had first spoken about the false financial statements and had crowed about his importance as a witness in the case. This was exactly opposite to the point I was making at the meeting”); *Id.* at 213 (“Although the new team knew nothing about the underlying facts, and nothing about how the Weisselberg case had been put together, they had read the defense motion papers attributing critical importance to Cohen, dumping all over him, and claiming that he had tainted the prosecution.”).

⁵⁵ *Id.* at 221-26, 228.

⁵⁶ *Id.* at 61.

⁵⁷ *Id.*

his Democratic base to indict [President] Trump.”⁵⁸ As a result, Pomerantz and Dunne dramatically resigned in protest, with Pomerantz leaking his scathing resignation letter to the *New York Times*.⁵⁹ Amid the fierce backlash to the First Day Memo and the fallout from the investigation into President Trump, Bragg issued an “unusual” public statement about the DANY’s investigation into President Trump, “emphasizing that the investigation into Trump and his business was far from over.”⁶⁰

In December 2022, Bragg “beefed up [his] office” by hiring senior U.S. Department of Justice official Michael B. Colangelo to fill the void left by the abrupt departure of Pomerantz and Dunne.⁶¹ Bragg hired Colangelo to “jump-start” his office’s investigation of President Trump, reportedly due to Colangelo’s “history of taking on Donald J. Trump and his family business.”⁶²

Colangelo’s employment history demonstrated the obsession that he shared with Bragg and Pomerantz to investigate a person—Donald Trump—rather than prosecute a crime.⁶³ At the New York Attorney General’s Office, Colangelo—who, for some time, held the title of Chief Counsel for Federal Initiatives⁶⁴—ran investigations into President Trump,⁶⁵ leading “a wave of state litigation against Trump administration policies.”⁶⁶ On January 20, 2021, the first day of the Biden Administration, Colangelo began serving as the Acting Associate Attorney General—the number three official at the Justice Department.⁶⁷ Upon the confirmation of Associate Attorney General Vanita Gupta, Colangelo began serving as the Principal Deputy Associate Attorney General.⁶⁸ However, in December 2022, Colangelo seemingly stepped down from his senior Justice Department position to become a line prosecutor at a local prosecutor’s office and to lead its investigation of President Trump.

⁵⁸ Jeff Coltin, *Alvin Bragg’s about to become the most famous prosecutor in America (but no questions, please)*, POLITICO (Apr. 13, 2024); see also Jeff Coltin, *This reluctant prosecutor just made Donald Trump a felon*, POLITICO (June 1, 2024) (“Bragg was also criticized by many Democrats for not quickly bringing a criminal conspiracy case against Trump that assistants in the office had been building.”).

⁵⁹ Coltin, *supra* note 58. *Read the Full Text of Mark Pomerantz’s Resignation Letter*, N.Y. TIMES (Mar. 23, 2022).

⁶⁰ Berman, *supra* note 20.

⁶¹ Jacob Shamsian, *Manhattan DA’s office hires attorney with extensive experience investigating Trump, suing his administration*, BUSINESS INSIDER (Dec. 5, 2022); see Erica Orden, *Liberal Manhattan DA takes on Trump in perilous legal fight*, POLITICO (Dec. 5, 2022); Ben Protess *et al.*, *How the Manhattan DA’s investigation into President Donald Trump unraveled*, N.Y. TIMES (March 5, 2022).

⁶² Jonah E. Bromwich, *Manhattan D.A. hires ex-Justice official to help lead Trump inquiry*, N.Y. TIMES (Dec. 5, 2022); see also Emma Colton, *Trump prosecutor quit top DOJ post for lowly NY job in likely bid to ‘get’ former president, expert says*, FOX NEWS (Apr. 25, 2024) (noting that Mr. Colangelo also held high-level positions in the Obama-Biden Administration, including “deputy director of the . . . National Economic Council and as chief of staff at the Labor Department.”).

⁶³ Shamsian, *supra* note 61; Patricia Hurtado, *Ex-DOJ Lawyer With Trump Experience Joins Manhattan DA’s Team*, BLOOMBERG (Dec. 5, 2022).

⁶⁴ Staff Profile, U.S. Dep’t of Justice, Former Acting Associate Attorney General Matthew Colangelo (last updated Apr. 22, 2021) [hereinafter “Colangelo Staff Profile”].

⁶⁵ Shamsian, *supra* note 61; Hurtado, *supra* note 63.

⁶⁶ *Who’s who in the Manhattan DA’s Donald Trump indictment*, ASSOCIATED PRESS (Mar. 31, 2023).

⁶⁷ Colangelo Staff Profile, *supra* note 64.

⁶⁸ Bromwich, *supra* note 62.

Shortly after Colangelo joined the DANY, Bragg empaneled a grand jury to hear evidence in a “years-old probe” regarding the alleged 2016 payment to Clifford.⁶⁹ Then, on April 4, 2023, Bragg announced his indictment of President Trump on 34 counts of first-degree falsifying business records⁷⁰—violating the American Bar Association’s guidance that a “prosecutor should not file or maintain charges greater in number or degree than . . . are necessary to fairly reflect the gravity of the offense or deter similar conduct.”⁷¹ Even without the egregious overcharging, the indictment was an “unprecedented abuse of prosecutorial authority.”⁷² Falsifying business records is ordinarily a misdemeanor subject to a two-year statute of limitations,⁷³ which would have expired long ago. Bragg used a novel and untested legal theory to bootstrap the misdemeanor allegations as a felony by alleging that President Trump was involved in falsifying records to conceal a second crime.⁷⁴ The facts surrounding Bragg’s indictment of President Trump have “been known for years,”⁷⁵ and federal officials had previously declined to bring charges.⁷⁶

Although both the SDNY and the DANY previously declined to further investigate the alleged payments to Clifford,⁷⁷ Bragg opted to revive the DANY’s investigation at a politically opportune moment—shortly after President Trump announced his White House run.⁷⁸ The timing and basis for the DANY’s prosecution of President Trump was clearly motivated by political calculations.

On April 15, 2024, President Trump’s trial began in Manhattan, where Colangelo led the opening statements for the prosecution.⁷⁹ The prosecution ultimately called 20 witnesses.⁸⁰ On May 30, 2024, the Manhattan jury found President Trump guilty on all 34 charges of falsifying business records.⁸¹ President Trump’s sentencing is scheduled for September 18, 2024.⁸²

⁶⁹ *Reports: New grand jury in NY examining Trump hush money*, ASSOCIATED PRESS (Jan. 30, 2023).

⁷⁰ Bragg Press Release, *supra* note 1.

⁷¹ AM. BAR ASS’N, CRIMINAL JUSTICE STANDARDS FOR THE PROSECUTION FUNCTION § 3-4.4(d) (4th ed. 2017). *Cf. Lafler v. Cooper*, 566 U.S. 156, 185 (2012) (Scalia, J., dissenting) (conceding the “grave risk[] of prosecutorial overcharging that effectively compels an innocent defendant to avoid massive risk by pleading guilty to a lesser offense”).

⁷² See Letter from Jim Jordan, Chairman, H. Comm. on the Judiciary *et al.* to Alvin L. Bragg, Dist. Att’y, N.Y. Cnty. (Mar. 20, 2023).

⁷³ *Id.*

⁷⁴ See *id.*; Ben Protess, *et al.*, *In Trump Case, Bragg Pursues a Common Charge With a Rarely Used Strategy*, N.Y. TIMES (May 7, 2023).

⁷⁵ Berman, *supra* note 20.

⁷⁶ Jed Handelsman Shugerman, *The Trump Indictment Is a Legal Embarrassment*, N.Y. TIMES (Apr. 5, 2023) (“Mr. Bragg’s predecessor, Cyrus Vance Jr., had almost a year to bring this case after Mr. Trump left office, but did not do so, and Attorney General Merrick Garland’s Justice Department also declined.”).

⁷⁷ POMERANTZ at 39, 61; see also Berman, *supra* note 20.

⁷⁸ POMERANTZ at 46; see also William K. Rashbaum, *et al.*, *Manhattan prosecutors begin presenting Trump case to grand jury*, N.Y. TIMES (Jan. 30, 2023).

⁷⁹ Graham Kates & Katrina Kaufman, *Trump trial gets underway in New York with jury selection in historic case*, CBS NEWS (Apr. 15, 2024); Ben Feuerherd, *Colangelo ends opening statement by preempting defense’s expected attack on Cohen’s credibility*, POLITICO (Apr. 22, 2024).

⁸⁰ Zach Schonfeld, *Here are the 22 witnesses who testified at Trump’s trial*, THE HILL (May 21, 2024).

⁸¹ *Read the Verdict Sheet in the Trump Manhattan Criminal Trial*, N.Y. TIMES (May 30, 2024).

⁸² Jake Offenhartz & Jennifer Peltz, *Judge delays Trump’s hush money sentencing until at least September after high court immunity ruling*, ASSOCIATED PRESS (July 2, 2024).

B. Bragg Relied on Convicted Perjurer Michael Cohen to Convict President Trump

Although Bragg stated in February 2022 “that he ‘could not see a world’ in which he would indict Trump and call Michael Cohen as a prosecution witness,”⁸³ Bragg’s “star witness” in his prosecution of President Trump was none other than Michael Cohen. Cohen, however, had a serious credibility problem, which is why prosecutors were reluctant to rely on him in the first place.

On February 28, 2019, Republicans on the House Committee on Oversight and Reform referred Cohen to the Justice Department for perjury and knowingly making false statements during his testimony before the Committee on February 27, 2019.⁸⁴ Urging the Justice Department to take appropriate action, Members cited six specific lies told by Cohen, including:

1. Cohen denied committing various fraudulent acts to which he had pleaded guilty in federal court.⁸⁵
2. Cohen repeatedly testified that he did not seek employment in President Trump’s White House, despite evidence from the U.S. Attorney’s Office for the Southern District of New York demonstrating that “Cohen privately told friends . . . that he expected to be given a prominent role and title in the new administration.”⁸⁶
3. Cohen stated that he did not direct the creation of a Twitter account known as @WomenForCohen, which is contradicted by statements from the owner of the IT firm that created the account for Cohen.⁸⁷
4. Cohen attested in his Truth in Testimony form that he did not have any reportable foreign government contracts, despite entering into two contracts in 2017 with entities owned in part by foreign governments.⁸⁸
5. Cohen’s testimony at the hearing contradicted various aspects of his written statement submitted in advance of the hearing.⁸⁹
6. Cohen asserted that he committed crimes out of “blind loyalty” to President Trump, which was contradicted by findings made by federal prosecutors and a federal court.⁹⁰

⁸³ POMERANTZ at 208-09.

⁸⁴ Letter from Rep. Jim Jordan & Rep. Mark Meadows to Hon. William Barr, Att’y Gen., U.S. Dep’t of Justice (Feb. 28, 2019); *Hearing with Michael Cohen, Former attorney for President Donald Trump: Hearing before the H. Comm. on Oversight & Reform*, 116th Cong. (2019).

⁸⁵ Letter from Rep. Jim Jordan & Rep. Mark Meadows to Hon. William Barr, Att’y Gen., U.S. Dep’t of Justice (Feb. 28, 2019).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.*

⁹⁰ *Id.*

Cohen’s willful and intentional false statements of material fact were contradicted by the record established by the Justice Department in *United States v. Cohen*.⁹¹ On May 8, 2024, Chairman Jim Jordan and Oversight Committee Chairman James Comer renewed the referral to the Biden-Garland Justice Department.⁹² The Biden-Garland Justice Department has taken no action to indict Cohen for making false statements to Congress.

In 2023, Cohen admitted to lying to Congress during a separate proceeding before Congress in 2019. At a hearing in the politicized lawsuit brought by the New York Attorney General against President Trump, Cohen admitted to lying under oath during a 2019 deposition before the House Permanent Select Committee on Intelligence (HPSCI).⁹³ President Trump’s attorney asked Cohen if he lied during the deposition when testifying about whether he was directed to inflate certain financial numbers, to which Cohen responded, “Yes.”⁹⁴ This revelation in court prompted HPSCI to refer Cohen again to the Justice Department for perjury and knowingly making false statements to Congress.⁹⁵

During a May 15, 2024, hearing before the Select Subcommittee, Robert Costello, Cohen’s former attorney, testified about Cohen’s credibility. Costello testified that the SDNY previously “turned down” the exact case Bragg brought against President Trump because “they assessed that Michael Cohen . . . was totally unworthy of belief.”⁹⁶ Throughout Costello’s representation of Cohen, Costello would ask Cohen for “information that would implicate [President] Trump” to help “get [Cohen] out of his legal troubles”⁹⁷ Cohen told Costello many times that he did not have any incriminating evidence on President Trump.⁹⁸ Despite not having any evidence on President Trump, Cohen told Costello that he would “do whatever the F . . . [he] has to do” to not spend a day in jail.⁹⁹ Cohen had the ability “to implicate [President] Trump in exchange for eliminating his own enormous legal problems [but] he repeatedly said he had nothing truthful on [President] Trump.”¹⁰⁰ Costello further testified that, throughout his representation of Cohen, Cohen would “lie[] repeatedly both about consequential and inconsequential details. Whenever it suited his purposes, Michael Cohen showed no hesitation to lie.”¹⁰¹ Costello also testified at the Manhattan trial and provided similar information—including

⁹¹ 18-cr-602 (S.D.N.Y. Aug. 21, 2018); Letter from Rep. Jim Jordan & Rep. Mark Meadows to Hon. William Barr, Att’y Gen., U.S. Dep’t of Justice (Feb. 28, 2019).

⁹² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, and Rep. James Comer, Chairman, H. Comm. on Oversight and Accountability, to Hon. Merrick B. Garland, Att’y Gen., U.S. Dep’t of Justice (May, 8, 2024).

⁹³ Letter from Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence, and Elise Stefanik, Member of Congress, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Justice (Nov. 14, 2023) (citing Transcript of Record at 2407:24-2410:22, *People of the State of New York v. Donald J. Trump et al.*, No. 452564/2022, Part 37 (N.Y. Sup. Ct. Oct. 25, 2023)).

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ May 15, 2024 Weaponization Hearing (written testimony of Robert Costello).

⁹⁷ *Id.* at 6.

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Id.* at 8.

¹⁰¹ *Id.* 8-9.

that Cohen previously told him that “President Trump knew nothing about [the] payments” at the heart of Bragg’s case.¹⁰²

Despite Cohen’s lack of credibility, during President Trump’s trial, Bragg heavily relied on Cohen’s testimony and credibility.¹⁰³ Cohen was the prosecution’s last witness and he spent four days testifying with the purpose of shedding light on President Trump’s alleged crime.¹⁰⁴ Yet, the only discernible crime that Cohen shed light on was his own. In particular, Cohen admitted on the stand that he stole from the Trump Organization.¹⁰⁵ Cohen testified that he sought reimbursement from the Trump Organization for \$50,000 to pay a vendor but only gave the firm about \$20,000—pocketing about \$30,000 for himself.¹⁰⁶ When asked on cross-examination if he “stole [the money] from the Trump Organization,” Cohen responded, “Yes, sir.”¹⁰⁷ When asked why he stole \$30,000, Cohen testified that he was “angry” because his annual bonus had been reduced.¹⁰⁸ *Politico* reported that “[t]he total theft actually amounted to \$60,000, because all sums were doubled to cover taxes Cohen might owe.”¹⁰⁹ One legal analyst explained, “The fact that [Cohen] was never charged with larceny is important because . . . larceny in New York State[] is more serious of a crime than falsifying business records.”¹¹⁰ In other words, Bragg’s star witness committed a more serious offense than President Trump, yet Bragg not only let him off the hook but also relied on him to go after President Trump.

Even more troubling, Cohen’s advisor, Lanny Davis, boasted to *Politico* that Bragg’s prosecution of President Trump all stemmed from Cohen’s testimony to Congress in 2019—the same testimony for which he was referred for perjury.¹¹¹ Davis confessed to calling the DANY after “Michael was sent to prison” because “the evidence of financial fraud was on the record in the [congressional] hearings and that Vance’s office should interview Michael And that’s how it began.”¹¹² In short, to prosecute President Trump, Bragg revived this “zombie” case relying on a known—and convicted—liar and his testimony at a congressional hearing in which he lied at least six times.¹¹³

¹⁰² Erica Orden, *Costello testifies that Cohen told him ‘Trump knew nothing about’ the Daniels payment*, POLITICO (May 20, 2024).

¹⁰³ Erica Orden, *Michael Cohen is an admitted liar. He’s still going to be the star witness against Trump*, POLITICO (Apr. 14, 2024).

¹⁰⁴ Matthew Haag, *Michael Cohen’s Trump Testimony Was Intense. Here Are the Highlights*, N.Y. TIMES (May 21, 2024) (“Mr. Cohen, Donald J. Trump’s former personal lawyer and fixer, spent four days on the stand in Mr. Trump’s criminal trial.”).

¹⁰⁵ Josh Gerstein, *Cohen admits he stole from the Trump Organization*, POLITICO (May 20, 2024).

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ Madeline Halpert & Kayla Epstein, *Trump trial: Cohen says he stole thousands from company*, BBC (May 20, 2024).

¹⁰⁹ Gerstein, *supra* note 105.

¹¹⁰ Hanna Panreck, *Michael Cohen stealing from Trump org ‘more serious’ than alleged Trump crime: CNN legal analyst*, FOX NEWS (May 20, 2024).

¹¹¹ Politico Staff, *Porn Stars, felons, and spin doctors: Who will jurors believe in Trump’s case?*, POLITICO (Mar. 24, 2023).

¹¹² *Id.*

¹¹³ Jonathan Turley, *Get ready for Manhattan DA’s made-for-TV Trump prosecution: high on ratings, but short on the law*, THE HILL (Mar. 18, 2023); Letter from Rep. Jim Jordan & Rep. Mark Meadows to Hon. William Barr, Att’y Gen., U.S. Dep’t of Justice (Feb. 28, 2019); Letter from Rep. Michael Turner, Chairman, H. Permanent Select

II. BRAGG’S “RUSSIAN-NESTING-DOLL” THEORY OF CRIMINALITY AND JUDGE MERCHAN’S JURY INSTRUCTIONS VIOLATED PRESIDENT TRUMP’S DUE PROCESS RIGHTS

The Fourteenth Amendment’s Due Process Clause prohibits the deprivation of any individual’s life, liberty, or property without due process of law.¹¹⁴ Due process embodies the idea that “criminal prosecutions must comport with prevailing notions of fundamental fairness.”¹¹⁵ The U.S. Supreme Court has made clear that due process requires “notice of the specific charge” levied against the accused and a meaningful opportunity to be heard “on the issue raised by that charge.”¹¹⁶ Several legal scholars, including former federal prosecutor Andrew McCarthy, have explained how Bragg’s prosecution of President Trump violated his due process rights. As McCarthy wrote, this is because the indictment against President Trump took:

[A] single transaction—Trump’s reimbursement to Michael Cohen of the \$130,000 Cohen paid to [Stephanie Clifford] to stay mum about an alleged 2006 fling [pursuant to an agreed-upon non-disclosure agreement (NDA)]—and ludicrously slic[ed] it into 34 transactions, each of which [it] brands as felony falsification of business records.¹¹⁷

In the words of law professor Elizabeth Price Foley, the procedural and substantive defects of this theory of liability amount to an unlawful “Russian-nesting doll theory of criminality” that offends notions of due process.¹¹⁸

On June 13, 2024, Professor Foley testified before the Committee and explained that Bragg’s case against President Trump presented a textbook example of a “Russian-nesting-doll theory of criminality: The charged crime hinged on the intent to commit another, unspecified crime, which in turn hinged on the actual commission of *yet another* unspecified offense.”¹¹⁹ She explained:

[President Trump] was charged with first-degree falsification of business records, which hinged on the intent to commit another, unspecified crime. As elaborated below, it became clear what this other, predicate crime was (New York election law) only when, after all evidence had closed, the judge instructed the jury. That predicate crime, moreover, required *further proof* that Mr. Trump *actually committed* yet another offense—i.e., the “unlawful means” by which New York’s election law was violated. At trial, there was no proof

Comm. on Intelligence, and Elise Stefanik, Member of Congress, to Hon. Merrick Garland, Att’y Gen., U.S. Dep’t of Justice (Nov. 14, 2023).

¹¹⁴ U.S. CONST. art. XIV, § 1.

¹¹⁵ *California v. Trombetta*, 467 U.S. 479, 485 (1984).

¹¹⁶ *Cole v. Arkansas*, 333 U.S. 196, 201 (1948)

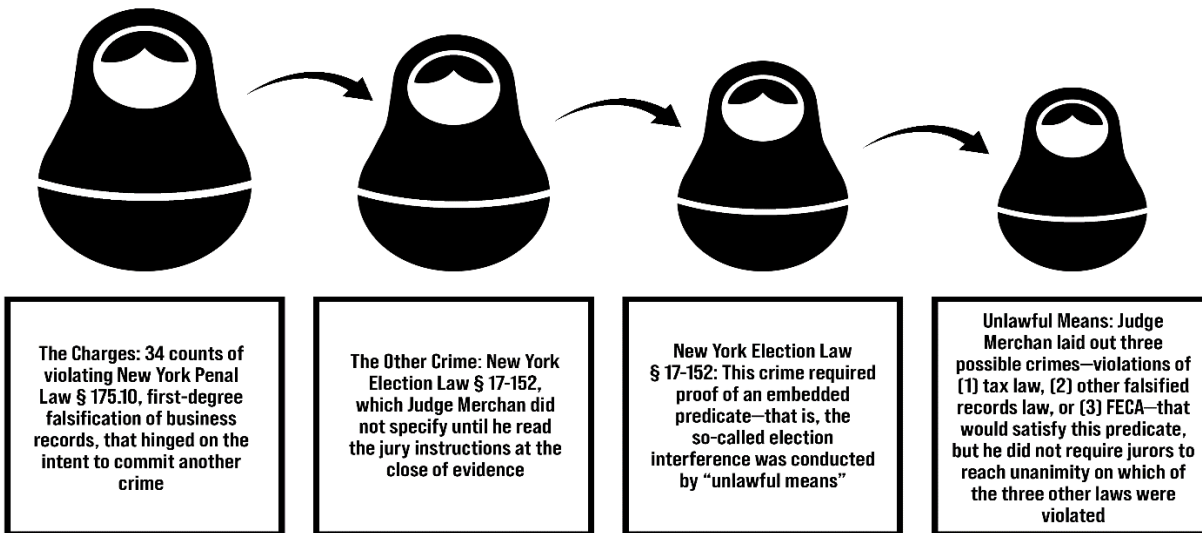
¹¹⁷ McCarthy, *supra* note 2.

¹¹⁸ Manhattan District Attorney Hearing (written testimony of Prof. Elizabeth P. Foley, FIU College of Law [hereinafter “Foley Written Testimony”]).

¹¹⁹ David B. Rivkin Jr. & Elizabeth Price Foley, *Trump’s Trial Violated Due Process*, WALL ST. J. OPINION (last updated June 4, 2024).

that this *second* predicate offense was actually committed, and indeed, it wasn't even clear what the second predicate was—like the first predicate—until the judge instructed the jury.¹²⁰

Professor Foley testified that “unpacking the nesting dolls reveals layers upon layers of due process defects inhering in these bizarre, unprecedented charges.”¹²¹



As a result, in the words of Professor Foley, “Mr. Trump’s New York trial violated [the] twin pillars of due process”: notice of the specific charges and the elements therein and a meaningful opportunity to be heard on those charges.¹²² Utilizing an actual nesting doll at the hearing to help demonstrate the due process problems, Professor Foley observed:

But I thought I would also bring another visual of the Russian nesting dolls to give you some sense of the complexity of the theory of criminality with which Mr. Trump was faced [with] in New York.

The first doll represents the actual charges in the indictment against Mr. Trump. There were 34 charges of felony falsification of business records under New York law. And to make it a felony falsification, you have to meet all of the elements of misdemeanor falsification which means you have to have a falsified business record with an intent to defraud and then to make it a felony, you have an additional that must be proven. That additional element is the intent to commit another crime. All right?

¹²⁰ Foley Written Testimony at 2.

¹²¹ *Id.* at 3.

¹²² Manhattan District Attorney Hearing at 23.

So the next nesting doll is what is that other crime that Mr. Trump intended to commit? Well, Mr. Trump wasn't sure and neither were his attorneys, so he asked the New York prosecutor for what is called a bill of particulars, saying hey, please tell me what that other crime you think it was that I intended to commit. The prosecutor interestingly responded and said you don't have a right to know. We don't have to tell you what that specific crime was and . . . in other words, without limiting our ability to change our minds during the trial, the other crimes that Mr. Trump may have intended to commit, may include one of four things: first, New York election law; second, New York tax law; third falsification of other business records, presumably other than the 34 with which he was actually charged; and finally, the Federal Election Campaign Act, FECA, right?

* * *

FECA, as you probably know, is the Federal Election Campaign Act, is a federal law that is over 100 pages long. And if you read it, you see that there is lots of different crimes embedded in that one mega statute. So Mr. Trump didn't know for sure what was that other crime that the prosecutor thought he intended to commit and in fact, the first time he learned what it was during the jury instruction when Judge Juan Merchan told the jury that that other crime was New York election law. Okay? That is far too late for due process purposes, for purposes of notice, right? That is after all of the evidence has closed.¹²³



¹²³ *Id.* at 23-26.

Professor Foley concluded that the layers, complexities, novelty, and lack of notice that President Trump had of the charges against him resulted in “a travesty of justice,” which was “clearly a violation of due process.”¹²⁴

The violation of President Trump’s due process rights did not end with the nesting-doll theory of criminality. It was compounded by the defective jury instructions that Judge Juan Merchan read to the jurors after the close of evidence. The instructions were comprised of 55-pages of confusing and seemingly unlawful charges.¹²⁵ Specifically, Judge Merchan told the jury that they had to agree unanimously on whether to convict President Trump on each of the 34 counts of falsifying business records with the intent to conceal damaging information before the 2016 election.¹²⁶ This required them, unanimously, to determine that President Trump used “unlawful means” to conceal this information.¹²⁷ However, Judge Merchan instructed the jurors that they “did not have to agree on a singular unlawful act” to convict.¹²⁸ He instructed the jurors “that they would have to find only that Mr. Trump committed bookkeeping infractions to conceal [1] a campaign finance violation, [2] tax law infraction or [3] falsification of business records,” but they “didn’t have to agree on the underlying crime to find the former president guilty.”¹²⁹

One New York criminal law expert reasoned that, by offering “three different theories as to how the false records could have violated state election law, limit[ing] instruction on what some of those theories required, and the fact that jurors were not required to agree on which had been proven,” Judge Merchan created “a real issue for the appeal.”¹³⁰ As a matter of law, legal scholar Andrew McCarthy explained, Judge Merchan should have instructed the jurors “that they had to find at least one of these objective crimes and they had to be unanimous on that finding in order to convict Trump.”¹³¹

Professor Foley underscored the constitutional defect that emanated from Judge Merchan’s jury charge, calling it “a cafeteria style of approach where non-unanimity was allowed on the underlying means by which the New York election [law] was violated. I think those are clear due process violations.”¹³² Professor Foley elaborated:

It was not until all evidence was closed that the New York trial judge, Judge Juan Merchan, finally revealed, in his jury instructions, that the other crime Trump intended to commit was Section 17-152 of New York election law. Moreover, he instructed the jury: “Although you must conclude unanimously that the defendant conspired to

¹²⁴ *Id.* at 27.

¹²⁵ See Aysha Bagchi, *Read the jury instructions in Donald Trump’s New York criminal hush money trial*, USA TODAY (May 20, 2024).

¹²⁶ Erica Orden & Ben Feuerhead, *Looming over Trump’s conviction: Reversal by the ‘13th juror,’* POLITICO (June 2, 2024).

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ Alex Swoyer, *Here are Trump’s top three arguments for appeal after guilty verdict in hush money trial*, WASH. EXAM. (May 30, 2024).

¹³⁰ Orden & Feuerhead, *supra* note 126 (internal quotation marks omitted).

¹³¹ Andrew C. McCarthy, *The ‘Other Crime’ in the Trump Trial: Conflating Ends and Means*, NAT’L REV. (June 3, 2024).

¹³² Manhattan District Attorney Hearing at 71.

promote or prevent the election of any person to a public office by unlawful means, you need not be unanimous as to what those unlawful means were.” Judge Merchan then hand-selected three laws that he told the jury “you may consider” as the “unlawful means” by which state election law was violated. . . . These instructions violated due process in several critical ways.

* * *

However one slices it, therefore, unanimity was required to determine the basis upon which the predicate crime Mr. Trump allegedly intended to commit—New York’s election law—was based. New York election law was the “other crime” that elevated Mr. Trump’s falsification of business records to a felony offense. . . . Judge Merchan’s instruction that the jury “need not be unanimous as to what those unlawful means were” was therefore unconstitutional¹³³

Simply put, Professor Foley explained, “due process demands that felony verdicts be unanimous.”¹³⁴

Indeed, Representative Kelly Armstrong, who spent many years as a criminal defense attorney, homed in on this exact point with Professor Foley during the hearing. In an exchange with Representative Armstrong, Professor Foley articulated the fundamental flaw in the trial: the prosecutor, the defendant, and the judge ultimately “don’t know how the jury got to where they got at the end.”¹³⁵ She testified:

Q. I’ve actually read all the jury[] [instructions]. The unlawful means is where we get this grab bag, right, Ms. Foley?

A. Yes, that’s where we get three possibilities instructed by the
—

Q. And basically pick. But I went through the jury instructions and here’s my question. What elements of any of those predicate claims are unlawful? I mean, conspiracy in and of itself is – so if you charge a second offense driving under the influence usually the sentence for a second offense is different than a first offense. In order to get to the second offense you have to prove the first offense beyond a reasonable doubt.

A. Right.

¹³³ Foley Written Testimony at 3-5.

¹³⁴ *Id.* at 4 (internal citation omitted).

¹³⁵ Manhattan District Attorney Hearing at 154.

- Q. Now, in those types of cases it's a certified record of a court judgment. You just put it in the record. . . . So when we're talking about these unlawful offenses and these three pictured things and dealing with the New York misdemeanor statute that when you combine with the other misdemeanor statute you end up getting to this felony and passed it to your statute of limitations. But was the jury required to prove any of those underlying elements beyond a reasonable doubt to any of those crimes? Because I'm talking about the Fifth Amendment and the due process part of that.
- A. No, and in fact, you know, based on the instructions we don't even know which of those possible three areas of law the jury decided –
- Q. Yeah, I've read it.
- A. — because they didn't have to be unanimous. But it's really more than three laws too, by the way, because the tax laws that he instructed the jury on could include local, state, and federal tax laws. And by the way, the mention of local or federal tax laws had never been made at all before at most, right. The prosecution had mentioned the possibility of state tax laws as being the first predicate, not second.
- Q. Yeah. And I'm actually into the third layer of this because unlawful means – I mean, I'm just thinking of – I've never defended a case in New York. I just never practiced in New York. But I have defended cases in state court and I've defended cases in federal court and I'm thinking about arguing against a case when you – I mean, I made my living on if there were seven elements of a crime. Winning one of them – like, I don't need to win all seven. I got to get proof beyond a reasonable doubt on one of the seven elements and they're not laid out anywhere in this whole process, are they?
- A. No. I mean, that's the problem. You don't know how the jury got to where they got at the end. In fact, you didn't even know how they could get there until they were instructed, and then once they were instructed because they could, you know, kind of pick and choose which of the unlawful means they wanted to base the New York election law violation on you have absolutely no idea why President Trump was guilty of a felony based upon theories of two different

misdemeanors.¹³⁶

Judge Merchan’s jury instructions unconstitutionally permitted the jury to find President Trump guilty even if they disagreed on what the “unlawful means” were.

The record could not be clearer: Bragg’s trial of President Trump violated basic principles of due process. Given these fundamental constitutional violations, experts have concluded that ample grounds support President Trump’s success on appeal.

¹³⁶ *Id.* at 152-54.

III. BRAGG USURPED THE AUTHORITY OF THE FEDERAL GOVERNMENT BY PURSUING CHARGES RELATED TO ALLEGED VIOLATIONS OF FEDERAL CAMPAIGN FINANCE LAWS

When Congress established the Federal Election Campaign Act (FECA) of 1971, it granted the Federal Election Commission (FEC) and the Justice Department the “exclusive jurisdiction over the enforcement of federal campaign finance laws.”¹³⁷ FEC Commissioner Trey Trainor explained that this exclusivity “ensures a uniform and consistent application of campaign finance laws across the United States, preventing a patchwork of enforcement that could vary from state to state and district to district.”¹³⁸ By prosecuting President Trump on a theory that he violated federal campaign finance laws, Commissioner Trainor concluded that Bragg “usurped the jurisdiction that Congress has explicitly reserved for the federal authorities” and “undermine[d] the statutory framework established by FECA.”¹³⁹

During his testimony on June 13, 2024, Commissioner Trainor explained that Bragg’s usurpation of federal prerogative should have compelled “Attorney General Garland and the DOJ” to “intervene in the prosecution of Donald Trump.”¹⁴⁰ Indeed, the Justice Department had previously intervened in the FEC’s investigation into the \$130,000 payment to Clifford and requested the agency stand down—which it did.¹⁴¹ Despite the Justice Department’s failure to intervene to halt Bragg’s usurpation of federal authority, Commissioner Trainor noted how the Biden-Garland Justice Department “had no issues with intervening in eight pending investigations being conducted by the FEC into the supposed \$130,000 payment that was alleged to be misreported on a campaign finance report.”¹⁴² Commissioner Trainor testified:

Those eight matters involved Michael Cohen, Donald J. Trump, Donald J. Trump for President and its treasurer, Trump Organization, LLC, Timothy Jost, and Essential Consultants, LLC. The public now knows that on July 31, 2018, the FEC, at the request of DOJ, voted to provide certain documents from the matters to DOJ and hold those matters in abeyance. Then, on June 5, 2019, the Commission voted, again at the behest of DOJ, to continue holding those matters in abeyance. Finally, on July 15, 2019, the United States Attorney’s Office for the Southern District of New York informed the United States District Court for the Southern District of New York that it had “effectively concluded its investigations” of the campaign finance violations to which Michael Cohen pled guilty, and, concurrently, that it no longer sought to maintain under seal the grand jury materials related to that investigation.

¹³⁷ Trainor Written Testimony at 1.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.* at 2.

¹⁴¹ Manhattan District Attorney Hearing at 60-61.

¹⁴² Trainor Written Testimony at 2.

DOJ inserted itself so fully into an ongoing FEC investigations that, once the abeyance request was lifted, the Commission faced a statute of limitations bar on prosecuting the matters. Clearly, the DOJ knows a great deal about the federal campaign finance issues that Alvin Bragg has prosecuted. DOJ counsel knew the extent to which they themselves had exercised federal jurisdiction, investigated, and found no illegal activity by anyone other than Michael Cohen. However, they have sat idly by and allowed a state officer to assert federal jurisdiction where they themselves had taken jurisdiction and couldn't prosecute.¹⁴³

During the hearing, Chairman Jordan asked Commissioner Trainor to elaborate on the Justice Department's decision to allow a rogue state prosecutor to claim jurisdiction over the matter despite the fact that the federal government had primary jurisdiction over it. Commissioner Trainor testified:

- Q. Commissioner Trainor, I want to read from your testimony. "They have sat idly by and allowed the state officers to assert federal jurisdiction where they themselves had taken jurisdiction and couldn't prosecute." I want you to unpack that sentence for us again real quick.
- A. . . . [A]ll of these claims with regard to the \$130,000 for Ms. [Clifford] stem from a complaint that was filed at the Federal Election Commission following the 2016 election.
- Q. Which you guys were investigating?
- A. We were in the process of investigating that.
- Q. And the DOJ came to you and said stand down; we are taking over, and give us your information?
- A. They asked us to abate that and several other matters.
- Q. They, meaning the Southern District of New York?
- A. That is correct.
- Q. And they took your information and you guys . . . voted to stand down and give it to the federal authority, right?
- A. That is correct, Mr. Chairman.
- Q. And they determined that there was nothing there to

¹⁴³ *Id.*

prosecute other than Michael Cohen—

- A. That is correct. They took a . . . very long time in doing it and when they sent it back to us, we had no more authority to investigate because they sent it back to us and we were barred by the statute of limitations from even investigating the normal civil things that we would look at with regard to those type of expenditures.
- Q. But your point here is they have sat idly by and allowed a state officer to assert federal jurisdiction where they themselves had intervened, to use the word, and taken jurisdiction from you and concluded there was nothing there regarding a federal statute, right? . . .
- A. That is correct, Mr. Chairman. And I don't know what role Mr. Colangelo played in that investigation that took place when they took it away from the Federal Election Commission. [He] [d]id that investigation and then he later left the office to go prosecute this at the state level.¹⁴⁴

Commissioner Trainor further explained that, because “the Department of Justice did not zealously represent the United States in this particular case to go in and defend the jurisdiction that this Congress has given through FECA to the Federal Election Commission and to the Justice Department,” it “abrogated [its exclusive jurisdiction] to a local official to prosecute.”¹⁴⁵ In essence, the Justice Department’s inaction in this case, Commissioner Trainor explained, could create “50 different standards of what violat[es] federal election law.”¹⁴⁶ Such a disparity in the law would upend the uniform application of federal law and the principle of equal protection.¹⁴⁷ Commissioner Trainor testified:

The implications of such jurisdictional overreach and disregard for the principles of federalism at issue are profound. If local district attorneys are permitted to initiate prosecutions based on their interpretations of federal campaign finance laws, we risk eroding the uniformity and predictability that FECA aims to provide. This could lead to a fragmented enforcement landscape where political motivations and local biases influence the application of laws meant to govern national elections and provide public transparency into the financing of campaigns.

* * *

¹⁴⁴ Manhattan District Attorney Hearing at 60-62.

¹⁴⁵ *Id.* at 115.

¹⁴⁶ *Id.* at 115-16.

¹⁴⁷ *Id.*

This encroachment on federal jurisdiction should raise serious concern that qualified candidates will be deterred from seeking public office, fearing that their political activities, past and present, might be subjected to disparate legal standards depending on the locality. It is essential to preserve the centralized enforcement mechanism that FECA envisions to ensure fair and impartial oversight of federal campaign finance regulations.¹⁴⁸

Ultimately, Bragg’s prosecution of President Trump “under the guise of federal campaign finance violations represent[ed] a clear usurpation of federal jurisdiction,” an attack on equal protection of the law and the integrity of our electoral system, and set a “dangerous precedent of local prosecutorial overreach in matters of federal concern.”¹⁴⁹ The Biden-Garland Justice Department’s silence—in failing to stand up for federal interests in Bragg’s politically motivated prosecution of President Trump—speaks volumes.

¹⁴⁸ Trainor Written Testimony at 3.

¹⁴⁹ *Id.*

IV. JUDGE MERCHAN’S RULINGS DURING THE TRIAL VIOLATED PRESIDENT TRUMP’S CONSTITUTIONAL RIGHTS INSIDE AND OUTSIDE OF THE COURTROOM

In 2005, during his confirmation hearing, then-Judge John Roberts famously explained the proper role of judges. He stated:

Judges and Justices are servants of the law, not the other way around. Judges are like umpires. Umpires don’t make the rules, they apply them. The role of an umpire and a judge is critical. They make sure everybody plays by the rules, but it is a limited role. Nobody ever went to a ball game to see the umpire.¹⁵⁰

By his actions and rulings, Judge Juan Merchan was no umpire, calling balls and strikes. Rather, at the trial of President Trump, he was a key player—pitching, catching, and batting—while draped in the judge’s robe. The legal errors in this case appear to go in only one direction: against President Trump. Stated differently, as former prosecutor Andrew McCarthy pointed out, Judge Merchan put “his thumb on the scale to get Trump convicted.”¹⁵¹

A. Judge Juan Merchan’s Political Bias Prejudiced President Trump

As a threshold matter, Judge Merchan and his family have close ties to the Democrat Party. Not only did his daughter, Lauren Merchan, work on Vice President Kamala Harris’s 2020 presidential campaign, she is currently the president of Authentic Campaigns, a “Chicago-based progressive political consulting firm” that works with Democrat Party candidates, including President Biden and Vice President Harris.¹⁵² According to Judge Merchan, prior to the trial he obtained an opinion from New York’s Advisory Committee on Judicial Ethics regarding his daughter’s employment. The Advisory Committee reportedly stated: “We see nothing in the inquiry to suggest that the outcome of the case could have any effect on the judge’s relative, the relative’s business or any of their interests.”¹⁵³

However, two of Authentic Campaigns’ top clients—Representative Adam Schiff and the Democrat-aligned Senate Majority PAC—have raised “at least \$93 million in campaign donations” while using President Trump’s New York indictments in their solicitation emails.¹⁵⁴ Notably, Rep. Schiff’s campaign for U.S. Senate has received “\$20 million in aid since he began soliciting donations off” Bragg’s indictment of President Trump last April.¹⁵⁵ The Senate

¹⁵⁰ *Confirmation Hearing on the Nomination of John G. Roberts, Jr. to be Chief Justice of the United States Before the S. Comm. on the Judiciary*, 109th Cong. 55 (2005) (statement of John G. Roberts, Jr., Nominee, U.S. Supreme Court).

¹⁵¹ Andrew C. McCarthy, *How Judge Merchan’s Jury Instruction Undermines Trumps’s Defense*, NAT’L REV. (May 30, 2024).

¹⁵² Jon Levine & Rich Calder, *Dem clients of daughter of NY judge in Trump hush-money trial raised \$93M off the case*, N.Y. POST (Mar. 30, 2024); Priscilla DeGregory, *NY judge denies Trump’s bid for recusal in ‘hush money’ case, says he’s ‘certain’ he can be impartial*, N.Y. POST (Aug. 14, 2023).

¹⁵³ Erica Orden, *Judge overseeing Trump’s hush money case won’t recuse himself*, POLITICO (Aug. 14, 2023).

¹⁵⁴ Levine & Calder, *supra* note 152.

¹⁵⁵ *Id.*

Majority PAC has “pocketed \$73.6 million since it also began firing off fundraising emails following the ex-president’s indictment.”¹⁵⁶

In 2020, Judge Merchan made donations to Democrat causes—including to President Biden’s campaign and a group called “Stop Republicans.”¹⁵⁷ According to Judge Merchan, the Advisory Committee found that his donations were “modest political contributions made more than two years ago [that] cannot reasonably create an impression of bias.”¹⁵⁸

Despite these conflicts, Judge Merchan denied President Trump’s recusal request in August 2023.¹⁵⁹ Judge Merchan’s bias was so obvious that one former federal prosecutor, a progressive legal analyst who is not a fan of President Trump, disagreed forcefully with Judge Merchan’s decision not to recuse, stating that he “absolutely should have recused himself” because “judges are not supposed to give any amount” to partisan political organizations.¹⁶⁰ By way of contrast, the former prosecutor observed, “[W]hat if the judge had donated a tiny amount, \$35, to Trump 2020 Would people be fine with that? I think people would be going nuts about that [T]here’s 40-something other judges in that courthouse who never donated, and it would have been safer [to have one of them oversee the trial.]”¹⁶¹

These conflicts of interest did not go unnoticed by one member of the New York congressional delegation, Representative Elise Stefanik. On May 28, 2024, Representative Stefanik filed a complaint with the New York State Commission on Judicial Conduct, requesting an investigation into the circumstances surrounding Judge Merchan’s “repeated assignment” to criminal cases related to President Trump.¹⁶² In her complaint, Representative Stefanik informed the Commission that Judge Merchan, “in violation of New York State Code of Judicial Conduct 100.5(h), donated to President Biden’s 2020 campaign, along with the Progressive Turnout Project and its ‘Stop Republicans’ subsidiary.”¹⁶³ She also highlighted for the Commission that Judge Merchan’s conflict extended to his Democrat-aligned political consultant daughter “whose firm stands to profit greatly if Donald Trump is convicted.”¹⁶⁴

¹⁵⁶ *Id.*

¹⁵⁷ William Rashbaum, *et al.*, *Ethics Panel Cautions Judge in Trump Trial Over Political Donations*, N.Y. TIMES (May 17, 2024); DeGregory, *supra* note 152. *See also* Victor Nava, *Judge Juan Merchan, who is overseeing Trump case, donated to Biden campaign in 2020*, N.Y. POST (Apr. 7, 2023).

¹⁵⁸ Michael R. Sisak, *Judge in Donald Trump’s hush-money case denies bias claim, won’t step aside*, ASSOCIATED PRESS (Aug. 14, 2023).

¹⁵⁹ DeGregory, *supra* note 152.

¹⁶⁰ Kaitlin Lewis, *Judge Merchan Should Have Recused Himself Over Biden Donation: Analyst*, NEWSWEEK (June 10, 2024) (quoting senior CNN legal analyst Elie Honig).

¹⁶¹ *Id.* (internal quotations marks omitted).

¹⁶² Letter from Rep. Elise Stefanik to N.Y. State Commission on Judicial Conduct & Kay-Ann Porter Campbell, Inspector Gen., N.Y. State Unified Court System (May 28, 2024) [hereinafter “Stefanik May 28, 2024 Letter”]. *See also* Letter from Rep. Elise Stefanik to N.Y. State Commission on Judicial (May 21, 2024) (focusing on conflict issue with Judge Merchan’s daughter’s partisan Democrat work).

¹⁶³ Stefanik May 28, 2024 Letter, *supra* note 162.

¹⁶⁴ *Id.*

B. Judge Merchan Unconstitutionally Silenced President Trump

Immediately before trial, Judge Merchan granted Bragg’s request for an unconstitutional gag order on President Trump, thereby prohibiting the presumptive 2024 Republican nominee for president from defending himself to the American people. On February 22, 2024, Bragg’s office filed a motion seeking to restrict President Trump’s “extrajudicial statements . . . for the duration of the trial” following several public comments made by President Trump regarding his pending trial in New York.¹⁶⁵ President Trump argued that as the “presumptive Republican nominee and leading candidate in the 2024 election” he must be able to “criticize these public figures” and respond to their attacks.¹⁶⁶

On March 26, 2024, Judge Merchan prohibited President Trump from making any public statements regarding “witnesses, prosecutors, jurors and court staff.”¹⁶⁷ The gag order did not restrict President Trump’s comments about Bragg or Judge Merchan.¹⁶⁸ On April 1, 2024, Judge Merchan extended the gag order to prohibit comments made by President Trump about the district attorney’s or the judge’s family members.¹⁶⁹

President Trump’s attorneys argued that the amended gag order was unconstitutional because it prohibited him from engaging in political speech, which is a core component of the First Amendment.¹⁷⁰ His campaign spokesman stated, “The voters of America have a fundamental right to hear the uncensored voice of the leading candidate for the highest office in the land.”¹⁷¹ One legal scholar, Professor Jonathan Turley, stated Judge Merchan’s gag orders “raise very serious free speech questions” as the orders prohibited President Trump from criticizing “central figures in this political campaign” such as star witness Michael Cohen, witness Stephanie Clifford, or key prosecutor Matthew Colangelo.¹⁷² During the trial, Judge Merchan fined President Trump \$10,000 for posts on his Truth Social platform and campaign website, ordered President Trump to delete the posts, and threatened him with jail for allegedly violating the gag order.¹⁷³

During the Committee’s June 13 hearing, Missouri Attorney General Andrew Bailey explained the unconstitutional nature of the Bragg-Merchan gag order. He testified:

[T]he prosecutor sought an unconstitutional gag order in this case. There’s a strong presumption against gag orders as violative of individual’s First Amendment rights of free speech. Bear in mind,

¹⁶⁵ Decision and Order, *People v. Donald J. Trump*, No. 71543-34 at 1 (N.Y. Co. Mar. 26, 2024).

¹⁶⁶ *Id.* at 2.

¹⁶⁷ Jesse McKinley, *et al.*, *Gag Order Against Trump Is Expanded to Bar Attacks on Judge’s Family*, N.Y. TIMES (Apr. 1, 2024).

¹⁶⁸ *Id.*

¹⁶⁹ *Id.*

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² Prof. Jonathan Turley, *The Gag and the Goad: Trump Should Appeal Latest Gag Order*, RES IPSA LOQUITUR (Mar. 27, 2024).

¹⁷³ Graham Kates & Katrina Kaufman, *Trump held in contempt for violating gag order in “hush money” trial. Here’s how much he owes.*, CBS NEWS (Apr. 30, 2024). *See also* Jeremy Herb, *et al.*, *Judge finds Donald Trump in contempt for 10th time over gag order and threatens jail time*, CNN (May 6, 2024).

the right to free speech protects not only the speaker, but Americans right to hear from a presidential candidate.¹⁷⁴

Indeed, Judge Merchan’s gag order is not only a constitutional defect but an active lawfare measure according to Robert Costello, a former federal prosecutor and veteran New York criminal defense lawyer. During the Select Subcommittee’s May 15 hearing, Costello testified in an exchange with Representative Stefanik:

Q. And the unconstitutional gag order on President Trump from New York Judge Merchan is unprecedented lawfare?

A. As far as I know, absolutely.¹⁷⁵

Likewise, former federal prosecutor and veteran criminal defense lawyer James Trusty testified at the same hearing as to the unprecedented nature of the gag order issued in President Trump’s case.¹⁷⁶ In an exchange with Representative Harriet Hageman, Trusty stated:

Q. Mr. Trusty, I think that you testified that in all your years of experience, you’ve never seen a circumstance where a defendant had a gag order imposed against them. Is that correct?

A. That’s correct.¹⁷⁷

C. Judge Merchan Permitted DA Bragg to Prejudice President Trump at Trial by Permitting Inadmissible Testimony

During the trial, Judge Merchan allowed Bragg “to spread before the jury in his Manhattan courtroom evidence that is blatantly inadmissible against” President Trump.¹⁷⁸ Generally, evidence is inadmissible if “its probative value is outweighed by the danger that its admission would prolong the trial to an unreasonable extent without any corresponding advantage; or would confuse the main issue and mislead the jury; or unfairly surprise a party; or create substantial danger of undue prejudice to one of the parties.”¹⁷⁹

In particular, as legal scholar Andrew McCarthy subsequently wrote, Bragg intended “to use Cohen’s guilty plea to establish that Trump was complicit in crimes because of the . . . payments [to Stephanie Clifford and Karen McDougal].”¹⁸⁰ Judge Merchan held that neither Cohen’s guilty plea nor prosecution witness David Pecker’s non-prosecution agreement were admissible because “evidence of another party’s guilty plea is not admissible to prove the

¹⁷⁴ Manhattan District Attorney Hearing at 114.

¹⁷⁵ May 15, 2024 Weaponization Hearing at 53-54.

¹⁷⁶ *Id.* at 108-09.

¹⁷⁷ *Id.* at 109.

¹⁷⁸ Andrew C. McCarthy, *Undercover Prosecutor Merchan Helps Bragg Lawlessly Stress Cohen’s Guilty Plea*, NAT’L REV. (May 25, 2024).

¹⁷⁹ *People v. Davis*, 43 N.Y.2d 17 (1977).

¹⁸⁰ Andrew C. McCarthy, *How Judge Merchan Is Orchestrating Trump’s Conviction*, NAT’L REV. (Apr. 29, 2024).

defendant’s guilt.”¹⁸¹ Nevertheless, Judge Merchan “simultaneously ruled that prosecutors could elicit testimony about Cohen’s guilty pleas on the rationale that they are relevant to his credibility as a witness,” which he permitted over President Trump’s objection.¹⁸²

As a result, McCarthy explained, the jury heard testimony about criminal conduct that would have been inadmissible at trial otherwise. He further elaborated:

Michael Cohen’s guilty pleas to two Federal Election Campaign Act (FECA) crimes, which he claimed were established by payments to [Stephanie Clifford] and Karen McDougal for non-disclosure agreements (NDAs); and David Pecker’s non-prosecution agreement with the Justice Department, which he executed out of fear that he’d be indicted over the McDougal NDA (he wasn’t, although his former company, AMI, agreed to pay the Federal Election Commission a fine—a disposition that allowed AMI to get out from under the federal government’s investigation so it could sell the *National Enquirer*.)¹⁸³

Although inadmissible, this was the “evidence” that President Trump violated campaign laws—if Cohen pleaded guilty to violating FECA, and Pecker was concerned that he might be charged with violating FECA, then a juror could infer that President Trump must have violated FECA when he allegedly paid off Clifford and McDougal.¹⁸⁴ Professor Foley expounded on this point during the Committee’s hearing, testifying in an exchange with Representative Scott Fitzgerald:

- Q. So Judge Merchan also ruled that Michael Cohen’s guilty plea for violating FECA was inadmissible at trial. Why do you think he made that ruling? I think we know, but.
- A. Well, because you can’t basically taint one individual by the guilty conduct of another.
- Q. Judge Merchan also ruled that DA Bragg could elicit testimony from Mr. Cohen about his guilty plea to impeach his credibility as a witness. DA Bragg then repeatedly made reference at trial in his [office’s] closing arguments to the jury about Cohen’s FECA guilty plea. Did repeatedly subjecting the jury to this testimony essentially get around the judge’s own ruling that Cohen’s FECA guilty plea was inadmissible as substantive evidence?

¹⁸¹ *United States v. Werne*, 939 F.2d 108, 113 (3rd Cir. 1991). See also *People v. Blades*, 93 N.Y.2d 166, 175-76 (1999) (cautioning that “rubrics must not be extended and applied as a blueprint for generalized admission of guilty plea colloquies into evidence, in lieu of live, confronted, cross-examinable trial testimony”).

¹⁸² McCarthy, *supra* note 180.

¹⁸³ Andrew C. McCarthy, *How Merchan Enabled Prosecutors’ Effort to Convict Trump Based on Improper Evidence*, NAT’L REV. (May 26, 2024).

¹⁸⁴ *Id.*

- A. Yeah, I mean, that should have been reined in. That was clearly trying to . . . taint one person through association with another who was guilty. They also did the same thing I believe with the CFO of Trump Organization and made similar comments because he also entered a guilty plea.¹⁸⁵

Judge Merchan also allowed Clifford to testify gratuitously and extensively about prejudicial matters that had no bearing on the allegations in the indictment. Judge Merchan unfairly prejudiced the jury against President Trump by permitting Clifford to testify about an alleged past encounter she claimed to have had with him—an encounter that had no relevance to the falsified business record-keeping charges at issue in the trial.¹⁸⁶ Indeed, several legal experts expressed “shock[] that the trial judge allowed such potentially damaging testimony into a low-level felony case focused on whether records were manipulated.”¹⁸⁷ This showing of unfair prejudice could be sufficient for the appeals court to vacate the guilty verdict and order a new trial.¹⁸⁸

Cohen’s and Clifford’s testimony unduly prejudiced President Trump and should not have been admitted. Despite this, Judge Merchan permitted both Cohen and Clifford to testify at length. And, as it relates to Clifford, her testimony was, at most, only tangentially related to the issues in dispute.

D. Judge Merchan Deprived President Trump of a Constitutionally Fair Trial by Refusing to Allow Former FEC Commissioner Bradley Smith to Testify as an Expert Witness on President Trump’s Behalf

While Judge Merchan permitted Bragg to elicit testimony from Cohen and Pecker about how they had violated federal election law, Judge Merchan denied President Trump’s request to have former FEC Chairman Bradley Smith testify that none of President Trump’s alleged involvement in these payments violated FECA.¹⁸⁹ This ruling had the effect of precluding President Trump from presenting “key exculpatory evidence” to the jury.¹⁹⁰ According to Professor Foley, this amounted to a due process violation.¹⁹¹ In an exchange with Representative Fitzgerald, she testified:

- Q. Ms. Foley, you argued in a recent *Wall Street Journal* op-ed that Judge Merchan likely denied President Trump a

¹⁸⁵ Manhattan District Attorney Hearing at 123-24.

¹⁸⁶ Swoyer, *supra* note 129.

¹⁸⁷ Shayna Jacobs, *Why Stormy Daniels’s testimony could fuel an appeal, and whether it matters*, WASH. POST (May 13, 2024).

¹⁸⁸ *People v. Weinstein*, No. 24, 2024 WL 1773181, at *1 (Apr. 25, 2024) (reversing guilty verdict and ordering new trial where the defendant “was judged, not on the conduct for which he was indicted, but on irrelevant, prejudicial, and untested allegations of prior bad acts”).

¹⁸⁹ *Id.*

¹⁹⁰ Kenin M. Spivak, *Prosecutor Alvin Bragg and Judge Juan Merchan have reached the pinnacle of selective prosecution and evisceration of due process*, AM. MIND (June 3, 2024).

¹⁹¹ Manhattan District Attorney Hearing at 122-23.

meaningful opportunity to be heard by denying the testimony of former FEC Chairman Brad Smith. Can you please elaborate a little bit on that?

- A. Yeah, I mean there has been a lot . . . of misreporting on what happened here. Yes, Judge Merchan . . . did allow Brad Smith to testify. But the catch was he could not opine at all, either provide his opinion or any personal opinion or legal opinion, regarding whether or not President Trump’s actions had violated FECA, which . . . basically then he was useless. Which is why President Trump didn’t call him as a witness. So the whole point was President Trump wanted an expert witness to put before the jury to show the jury that what he had done did not in fact violate federal election law. And he was denied that opportunity, and that seems like a rather basic thing that he would have the opportunity to be heard on.
- Q. Do you think there was a chance that he could have had success upon appeal?

* * *

- A. Yeah, sure, absolutely [T]he due process issue is a question of law. It gets de novo review, the appellate courts get to look at it fresh with fresh eyes, no deference whatsoever. And more importantly, due process issues are issues that the Supreme Court can ultimately grant cert in here.¹⁹²

Despite Judge Merchan’s decision to allow highly prejudicial testimony that should not have been admitted, Judge Merchan refused to allow former FEC Chairman Smith to testify about relevant issues to the defense. This denied President Trump an opportunity to be heard on an issue at the heart of this case—his alleged violation of federal election law.

Indeed, former FEC Chairman Smith subsequently commented on Judge Merchan’s erroneous ruling on X, observing that “Judge Merchan has so restricted my testimony that [the] defense has decided not to call me.”¹⁹³ Smith’s testimony was intended to assist the jury in navigating the intricacies of FECA, which, as Smith noted, is so complex that “even Antonin Scalia—a pretty smart guy, even if you hate him—once said ‘this campaign finance law is so intricate that I can’t figure it out.’”¹⁹⁴ Smith analogized the FECA discussion at President Trump’s trial to a jury trial “in a product liability case” and expecting jurors “to figure out if a complex machine was negligently designed, based only on a boilerplate recitation of the general

¹⁹² *Id.*

¹⁹³ Brad Smith (@CommishSmith), X (May 20, 2024, 5:45PM).

¹⁹⁴ *Id.* (cleaned up).

definition of ‘negligence.’ They’d be lost without knowing technology & industry norms.”¹⁹⁵ Worse, Smith explained the deleterious practical effect of Judge Merchan’s ruling limiting his putative testimony: “While [the] judge wouldn’t let me testify on [the] meaning of [the] law, he allowed Michael Cohen to go on at length about whether and how this activity violated FECA. So effectively, the jury got its instructions on FECA from Michael Cohen!”¹⁹⁶

The odds of President Trump having a fair trial were stacked against him from the case’s inception. Judge Merchan’s and his family’s close ties to Democrat-aligned interests, on their own, provided sufficient grounds for Judge Merchan to recuse himself—he was clearly conflicted and by remaining on the case presented an appearance of impropriety. Nevertheless, he chose to remain. In the courtroom, Judge Merchan allowed testimony that deprived President Trump of a fair trial. Outside of the courtroom, Judge Merchan sought to hinder President Trump, the presumptive 2024 Republican nominee for president, from defending himself to the American people.

¹⁹⁵ *Id.*

¹⁹⁶ *Id.*

CONCLUSION

Every person admitted to practice law in New York, including elected district attorneys and appointed judges, must take a “constitutional oath of office,” swearing or affirming to “support the constitution of the United States, and the constitution of the State of New York.”¹⁹⁷ By taking that oath, District Attorney Alvin Bragg and Judge Juan Merchan were legally “bound to a constitutional course of conduct.”¹⁹⁸ In their politicized efforts to indict and convict President Trump, they failed their oaths of office. But neither of these faithless officials will have the last word on the travesty of justice that transpired in lower Manhattan on May 30, 2024.¹⁹⁹

The testimony that the Committee and Select Subcommittee have received makes clear that President Trump’s trial was riddled with constitutional defects—defects that should prompt the New York appellate courts to reverse the verdict. The trial violated basic principles of due process.

As an initial matter, President Trump was deprived of the opportunity to defend himself from the alleged underlying crime because prosecutors never disclosed it—and Judge Merchan never forced them to do so. Because President Trump had no notice of the specific charges against him, in particular the underlying crime and its essential elements, he did not have a meaningful opportunity to defend himself from those charges. Then, Judge Merchan instructed the jurors that they “did not have to agree on a singular unlawful act” to convict.²⁰⁰ Rather, he gave the jurors a menu of potential avenues by which they could convict President Trump, instructing them that “they would have to find only that Mr. Trump committed bookkeeping infractions to conceal [1] a campaign finance violation, [2] tax law infraction or [3] falsification of business records,” but they did not have to agree on the underlying crime.²⁰¹ Finally, Judge Merchan permitted gratuitous and prejudicial testimony that should have been inadmissible.²⁰² As a general matter, evidence should be excluded if its prejudice outweighs its probative value.²⁰³ The testimony that Judge Merchan permitted at trial, particularly certain parts of Cohen’s and Clifford’s testimony, was unduly prejudicial and never should have been allowed.

New York appellate courts have been “dubbed the ‘13th juror’ . . . because judges are allowed to make decisions based on the facts of the case—not only the law.”²⁰⁴ One former Manhattan assistant district attorney called it “an underappreciated power that the appellate division has” when reviewing cases on appeal.²⁰⁵ The New York Court of Appeals characterized the intermediate appellate courts power to “review questions of law and questions of fact” as the

¹⁹⁷ N.Y. ST. CONST. art. XIII, § 1; N.Y. JUDICIARY LAW § 466.

¹⁹⁸ Richard M. Re, *Promising the Constitution*, 110 NW. U. L. REV. 299, 315 (2016) (internal quotation marks omitted).

¹⁹⁹ Lynch, *supra* note 14.

²⁰⁰ *Id.*

²⁰¹ Swoyer, *supra* note 129.

²⁰² See Section IV(C).

²⁰³ *Id.*

²⁰⁴ Orden & Feuerherd, *supra* note 126; see also *People v. Rickert*, 58 N.Y.2d 122 (1983) (holding that, in appropriate cases, the appellate court has the power to review facts and substitute its own discretion).

²⁰⁵ Orden & Feuerherd, *supra* note 126 (internal quotation marks omitted).

“linchpin of our constitutional and statutory [appellate] design.”²⁰⁶ Given that President Trump’s indictment was conceived in legal and constitutional error and the trial exacerbated and compounded those errors, an honest review of the facts and the law will likely lead appellate courts to vacate the conviction and dismiss the indictment with prejudice. This will go a long way in restoring the American people’s trust and confidence in our justice system, although more work is ahead. In the meantime, the Committee and Select Subcommittee will continue our oversight of lawfare and its effect on the rule of law in the United States.

²⁰⁶ *People v. Bleakley*, 69 N.Y.2d 490, 493-94 (1987).

FEDERAL GOVERNMENT ELECTION INTERFERENCE OPERATIONS

The federal government's efforts to suppress conservative voices extended to the 2020 presidential election. On October 14, 2020, just days before the 2020 presidential election between President Trump and President Biden, the *New York Post* published a story detailing how Hunter Biden used the position and influence of his father for personal gain with his father's awareness.¹⁸⁸ Almost immediately after the publication of this potentially election-altering story, social media companies and news outlets censored the story, preventing Americans from learning important information as they were heading to the polls. Even after social media companies stopped censoring the stories, 51 former intelligence community officials, using their official titles and citing their national security credentials, released a public statement suggesting that the story "ha[d] all the classic earmarks of a Russian information operation."¹⁸⁹ The Select Subcommittee investigated the censorship decisions and the origins of the public statement by former intelligence officials, revealing how the federal government, social media companies, and the Biden campaign acted in concert to discredit and diminish any negative stories about President Biden and his family.

On May 10, 2023, the Select Subcommittee worked with the Permanent Select Committee on Intelligence to release its a report on its investigation into the coordinated public statement from former high ranking intelligence officials, titled "[The Hunter Biden Statement: How Senior Intelligence Community Officials and the Biden Campaign Worked to Mislead American Voters](#)." As part of its investigation, the Select Subcommittee and the Permanent Select Committee on Intelligence wrote to all 51 former officials who signed the statement, requesting documents and testimony.¹⁹⁰ The investigation revealed that this public statement was politically motivated from the start, designed to, as former CIA Director Michael Morell testified, "help Vice President Biden" in his campaign for president.¹⁹¹ As the emails soliciting signatures made clear, "We think Trump will attack Biden on the issue at this week's debate"¹⁹² and "we want to give the [Vice President] a talking point to use in response."¹⁹³ The interim report further detailed how Morell spearheaded the statement after receiving a call from then-campaign advisor and current Secretary of State Antony Blinken.¹⁹⁴ Importantly, the Biden campaign's fingerprints were all over the public statement, including coordinating its

¹⁸⁸ Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020); see also Emma-Jo Morris & Gabrielle Fonrouge, *Hunter Biden emails show leveraging connections with his father to boost Burisma pay*, N.Y. POST (Oct. 14, 2020).

¹⁸⁹ Jim Clapper, et al., *Public Statement on the Hunter Biden Emails* (Oct. 19, 2020); see also Natasha Bertrand, *Hunter Biden story is Russian disinfo, dozens of former intel officials say*, POLITICO (Oct. 19, 2020).

¹⁹⁰ STAFF OF H. COMM. ON THE JUDICIARY AND SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS* (Comm. Print May 10, 2023) (hereinafter "MISLEAD AMERICAN VOTERS").

¹⁹¹ Transcribed Interview of Mr. Michael Morell at 11 (Apr. 4, 2023) (hereinafter "Morrell Interview").

¹⁹² Email from Kristin Wood to Unnamed Intelligence Officials (Oct. 19, 2020 7:27 AM) (on file with the Committees).

¹⁹³ Email from Michael Morell to Michael Morell, Marc Polymeropoulos, and Bcc'd Recipients (Oct 18, 2020 4:48 PM) (on file with the Committees).

¹⁹⁴ MISLEAD AMERICAN VOTERS, *supra* note 190, at 6-7 (Comm. Print May 10, 2023).

dissemination to the media.¹⁹⁵ After the statement was published, Biden campaign chairman Steve Ricchetti called Morell and “thanked [him] for putting the statement out.”¹⁹⁶

Following continued investigation, the Select Subcommittee and the Permanent Select Committee on Intelligence released a second report on June 25, 2024, “[The Intelligence Community 51: How CIA Contractors Colluded with the Biden Campaign to Mislead American Voters](#).” This report detailed previously nonpublic information about the extent to which the CIA was aware of the statement before publication. Indeed, high-ranking CIA officials, up to and including CIA Director Gina Haspel, were made aware of the statement prior to its approval and publication.¹⁹⁷ Internal CIA documents also showed that employees internally expressed concern about the statement’s politicized content, acknowledging it was not “helpful to the Agency in the long run.”¹⁹⁸

Alarming, the Select Subcommittee learned that some of the statement’s signatories were on active contract with the CIA at the time of the statement’s publication.¹⁹⁹ Although the signatories contended throughout the course of the Select Subcommittee’s investigation that none had access to classified information when asserting that the allegations surrounding Hunter Biden’s laptop were likely Russian disinformation, those on active contract with the CIA were likely earning taxpayer dollars while politicizing intelligence to assist the Biden campaign.

Through the Select Subcommittee’s investigations, it is clear that the intelligence community worked to diminish the reach of stories that could be seen as harmful to President Biden’s 2020 presidential campaign. The American people deserve to have trust that the intelligence community is not working against them or preventing voters from having access to all available information before making an informed decision about the candidate for whom they wished to cast their ballot. Unfortunately, before the 2020 election, the ends seemed to justify the means when it came to defeating President Trump. Stories that could have changed the outcome of the election were censored, those who shared the stories were suspended from social media, and former high ranking intelligence officials, purportedly without any access to official information, told the American people that the Russians were interfering in the election.

¹⁹⁵ *Id.* at 36.

¹⁹⁶ Morrell Interview, *supra* note 191, at 96-97 (Apr. 4, 2023).

¹⁹⁷ STAFF OF H. COMM. ON THE JUDICIARY, SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, AND H. PERMANENT SELECT COMM. ON INTELLIGENCE, 118TH CONG., THE INTELLIGENCE COMMUNITY 51: HOW CIA CONTRACTORS COLLUDED WITH THE BIDEN CAMPAIGN TO MISLEAD AMERICAN VOTERS 5 (Comm. Print June 25, 2024) (hereinafter “CIA CONTRACTORS”).

¹⁹⁸ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 11:05 AM) (Bates CIA000157) (on file with the Committees).

¹⁹⁹ CIA CONTRACTORS, *supra* note 197, at 16-20.



**THE HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY
OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN
VOTERS**

Interim Joint Staff Report of the

Committee on the Judiciary,
Select Subcommittee on the Weaponization
of the Federal Government, and
Permanent Select Committee on Intelligence

U.S. House of Representatives



May 10, 2023

Executive Summary

“Let me tell you, you take on the intelligence community, they have six ways from Sunday to getting back at you.”

– Senator Chuck Schumer (D-NY), January 3, 2017.¹

In the heated days shortly before the 2020 presidential election, a news story appeared in the *New York Post* detailing how Hunter Biden used the position and influence of his father, now-President Joe Biden, for personal gain with President Biden’s awareness.² This article, based on materials obtained from an abandoned laptop once owned by Hunter Biden, called into question statements made by President Biden denying awareness of the international business dealings of his son, Hunter.³ Five days after the *Post* story, 51 former intelligence community officials, using their official titles and citing their national security credentials, released a public statement suggesting the story “ha[d] all the classic earmarks” of Russian disinformation.⁴ Three days after that, Vice President Biden used this public statement in a nationally televised presidential debate to rebut President Trump’s criticisms, asserting “there are 50 former national intelligence folks who said that what this, he’s accusing me of is a Russian plan.”⁵

Much has been written about how social media companies and news outlets improperly censored or ignored allegations on the flimsy basis that it was “hacked” materials;⁶ and “can’t be verified”;⁷ or, in the inspired words of National Public Radio, a “waste of time” and a “pure distraction.”⁸ These censorship decisions were wrong then, but they look even more egregious

¹ Rachel Maddow, *Schumer: Trump ‘being really dumb’ on intel*, MSNBC (Jan. 3, 2017).

² Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020); *see also* Emma-Jo Morris & Gabrielle Fonrouge, *Hunter Biden emails show leveraging connections with his father to boost Burisma pay*, N.Y. POST (Oct. 14, 2020).

³ The Hill (@thehill), Twitter (Sept. 21, 2019, 3:04 PM) (Joe Biden claiming, “I’ve never spoken to my son about his overseas business dealings.”), <https://twitter.com/thehill/status/1175486006348460032>; Press Briefing, Jen Psaki, White House Press Secretary, in Washington, D.C. (Apr. 5, 2022) (explaining how President Biden stands by his statement that he never spoke to Hunter Biden about his overseas business dealings). *See also* Miranda Devine, *Hunter Biden’s biz partner called Joe Biden ‘the Big Guy’ in panicked message after Post’s laptop story*, N.Y. POST (July 27, 2022) (“In an email to Hunter, Jim and other partners on May 13, 2017, Gilliar outlined an equity breakdown in which 10% of the lucrative CEFC joint venture would be held by Hunter ‘for the big guy.’ That email, which was previously revealed by The Post, was found on the laptop Hunter abandoned at a Delaware repair shop in April 2019. Another former associate of the first son, US Navy veteran Tony Bobulinski, publicly declared in October 2020 that ‘big guy’ was a reference to President Biden — and alleged that Biden was aware of, and involved in, the planned CEFC deal.”).

⁴ Jim Clapper et al., *Public Statement on the Hunter Biden Emails* (Oct. 19, 2020). *See also* Natasha Bertrand, *Hunter Biden story is Russian disinfo, dozens of former intel officials say*, POLITICO (Oct. 19, 2020).

⁵ COMM. ON PRESIDENTIAL DEBATES, Presidential Debate at Belmont University in Nashville, Tennessee, October 22, 2020, Participants: Former Vice President Joe Biden (D) and President Donald Trump (R), <https://www.debates.org/voter-education/debate-transcripts/october-22-2020-debate-transcript/>.

⁶ *See, e.g.*, Katie Paul, *Twitter, Facebook restrict users’ dissemination of New York Post story on Biden*, REUTERS (Oct. 15, 2020); Kari Paul, *Facebook and Twitter restrict controversial New York Post story on Joe Biden*, THE GUARDIAN (Oct. 14, 2020).

⁷ Zachary Evans, *60 Minutes Anchor Insists Hunter Biden Emails ‘Can’t Be Verified’ When Pressed by Trump*, NAT’L REV. (Oct. 22, 2020).

⁸ *See, e.g.*, Brian Flood, *NPR issues major correction after falsely claiming Hunter Biden laptop story was ‘discredited’ by intelligence*, FOX NEWS (Apr. 2, 2021); Joe Concha, *Media’s pre-election burial of Hunter Biden story proves dereliction of duty*, THE HILL (Dec. 11, 2020).

with the passage of time. The contents of Hunter Biden’s laptop have since been authenticated and the *Post*’s reporting has been verified by several other news outlets.⁹

What has not been examined, until now, is how 51 former federal employees with intelligence and national security credentials came together to insert themselves into the thick of the presidential campaign. Beginning in April 2022—and renewed earlier this year when Republicans resumed control of the House of Representatives—the Committee on the Judiciary and the Permanent Select Committee on Intelligence have been conducting oversight into the origins of this statement.¹⁰ The Committees wrote to all 51 former officials requesting relevant documents and testimony. Consistent with the obligation to keep the House apprised of investigative activities,¹¹ this interim report summarizes the key information learned to date.

- **The public statement by 51 former intelligence officials was a political operation to help elect Vice President Biden in the 2020 presidential election.** Contemporaneous emails show the organizers’ intent in drafting and releasing the statement: “[W]e think Trump will attack Biden on the issue at this week’s debate and we want to offer perspectives on this from Russia watchers and other seasoned experts,”¹² and “we want to give the [Vice President] a talking point to use in response.”¹³
- **The Biden campaign took active measures to discredit the allegations about Hunter Biden by exploiting the national security credentials of former intelligence officials.** On October 17, 2020, Biden campaign advisor—now Secretary of State—Antony Blinken contacted former Central Intelligence Agency (CIA) Acting Director Michael Morell to discuss the *Post*’s reporting. Morell told Blinken that he was not familiar with the reporting and Blinken later emailed Morell a *USA Today* article alleging the FBI was investigating whether it was Russian disinformation.¹⁴ At the bottom of the email was the signature block of Andrew Bates, then-director of rapid response for the Biden campaign.¹⁵ Following this outreach from the Biden campaign, Morell began the process of drafting the statement—something Morell testified would not have happened but for Blinken’s communication. In addition, following the October 22 presidential debate—during which Vice President Biden used the public statement to rebut President Trump’s criticisms—Biden campaign chairman Steve Ricchetti called Morell to thank him for the statement.

⁹ See, e.g., Katie Benner et al., *Hunter Biden Paid Tax Bill, but Broad Federal Investigation Continues*, N.Y. TIMES (Mar. 16, 2022); Craig Timberg et al., *Here’s how The Post analyzed Hunter Biden’s laptop*, WASHINGTON POST (Mar. 30, 2022).

¹⁰ See Letter from Rep. Jim Jordan, Ranking Member et al., H. Comm. on the Judiciary, to Ms. Nada Bakos, c/o Central Intelligence Agency (Apr. 6, 2022).

¹¹ See, e.g., H. Res. 12, 118th Cong. (2023).

¹² Email from Kristin Wood to Unnamed Intelligence Officials (Oct. 19, 2020, 7:27 AM) (on file with the Committees).

¹³ Email from Michael Morell to Unnamed Intelligence Officials (Oct. 18, 2020, 4:48 PM) (on file with the Committees).

¹⁴ Email from Tony Blinken to Michael Morell (Oct. 17, 2020, 10:53 PM) (on file with the Committees).

¹⁵ *Id.*

- **Blinken’s outreach to Morell was the impetus for the public statement.** Morell testified that he had no intention of drafting the statement until Blinken reached out to him. Morell, who at the time was reportedly under consideration to be appointed CIA Director in the Biden Administration if Biden won the election,¹⁶ conceived the statement and concluded it would have greater credibility if it was supported by a significant number of signatories.¹⁷ Thereafter, Morell contacted several former intelligence officials to help write the statement, solicit cosigners, and help with media outreach.
- **The Biden campaign coordinated dissemination of the statement to members of the media.** Morell tasked Nick Shapiro, his former Deputy Chief of Staff and Senior Advisor at the CIA, with placing the statement in major publications. Specifically, Morell apprised Shapiro that, “[b]etween us, the campaign would like” a specific reporter with the *Washington Post* to run the statement first.¹⁸ Shapiro crafted an email for three separate media outlets and sent the content of the email to the Biden campaign’s Director of Rapid Response, Andrew Bates, stating “This is what I gave them.”¹⁹ After peddling the statement to the *Washington Post* and the *Associated Press* with apparently no result, Shapiro found a willing partner in *Politico*. *Politico* published a story about the statement under the headline: “Hunter Biden story is Russian disinfo, dozens of former intel officials say.”²⁰
- **The Committees have evidence that an employee affiliated with the CIA may have assisted in obtaining signatories for the statement.** One signer of the statement, former CIA analyst David Cariens, disclosed to the Committees that a CIA employee affiliated with the agency’s Prepublication Classification Review Board (“PCRB”) informed him of the existence of the statement and asked if he would sign it.²¹ The Committees have requested additional material from the CIA, which has ignored the request to date.

The Committees’ oversight continues. Notably, the Biden Administration has declined to cooperate with this oversight to date. On March 21, 2023, the Committees wrote to the CIA, requesting documents in the CIA’s possession relating to the statement and interactions between the CIA and the signatories of the statement.²² The Committees requested that the CIA furnish these documents by April 4, 2023.²³ The CIA has so far failed to comply to this oversight request. On April 20, 2023, the Committees wrote to Secretary of State Antony Blinken requesting information in his possession about his role in the origins of the statement.²⁴ On May

¹⁶ Erin Banco, *Biden Weighs Mike Morell as His CIA Chief. A Key Dem Senator Says Don’t Bother*, THE DAILY BEAST (Dec. 2, 2020). See also Transcribed Interview of Mr. Michael Morell at 91 [hereinafter “Morell Interview”].

¹⁷ See Email from Michael Morell to Kristin Wood (Oct. 18, 2020, 8:01 PM) (on file with the Committees). Morell Interview at 44.

¹⁸ Email from Michael Morell to Nick Shapiro (Oct. 19, 2020, 8:21 PM) (on file with the Committees).

¹⁹ Email from Nick Shapiro to Andrew Bates (Oct. 19, 2020, 11:22 PM) (on file with the Committees).

²⁰ Bertrand, *supra* note 4.

²¹ Email from David Cariens to Committee staff (March 5, 2023, 3:02 PM) (on file with the Committees).

²² Letter from Chairman Jim Jordan, H. Comm. on the Judiciary, and Chairman Michael R. Turner, Permanent Select Committee on Intelligence, to Hon. William J. Burns, Dir., Cent. Intel. Agency (Mar. 21, 2023).

²³ *Id.*

²⁴ Letter from Chairman Jim Jordan, H. Comm. on the Judiciary, and Chairman Michael R. Turner, Permanent Select Committee on Intelligence, to Hon. Antony Blinken, Sec., Dep’t of State (Apr. 20, 2023).

4, 2023, via counsel, Secretary Blinken responded.²⁵ Although he denied asking Morell to write the statement, Secretary Blinken did not dispute that his communication was the impetus for the statement.²⁶ Secretary Blinken provided none of the documents that Committee requested. The Committees will continue to pursue additional information about the actions and events described in this report.

Americans deserve to have confidence that their government, particularly its premier intelligence agency, is free from politicization. The infusion of bare-knuckle partisan politics into America's intelligence agencies is cause for grave concern. Former federal employees have a right to engage in the political process—a fundamental right that the Committees do not dispute. Here, however, the signers of the Hunter Biden laptop statement relied on their national security credentials and used their official titles to lend heft to their statement and to insinuate access to secretive information unavailable to other Americans. And these signers did so in coordination with a political campaign for the explicit purpose of giving a candidate for office a “talking point” to dismiss legitimate criticism of his family's business practices.

Consistent with the Committees' obligations to keep the House of Representatives informed of its oversight, this interim report presents what the Committees have learned to date about the origins of the public statement signed by 51 former intelligence officials that falsely discredited public allegations about the Biden family. Although more work remains, this report presents the Committees' findings to date.

²⁵ Letter from Jonathan C. Su, counsel for Secretary Antony Blinken, to Chairman Jim Jordan, H. Comm. on the Judiciary, and Chairman Michael R. Turner, Permanent Select Committee on Intelligence (May 4, 2023).

²⁶ *Id.*

Table of Contents

Executive Summary	1
Table of Contents	5
I. The Biden campaign used the national security credentials of 51 former intelligence community employees to falsely discredit allegations of Biden family influence-peddling. 6	
A. Biden campaign advisor Antony Blinken’s outreach to former CIA Acting Director Michael Morell was the impetus for the public statement, which was intended to give the Biden campaign a “talking point” with which to respond to the Hunter Biden allegations.	6
B. Morell recruited Polymeropoulos to draft the public statement.	12
C. Morell, Polymeropoulos, and former CIA officer Kristin Wood solicited other former intelligence officials and employees to sign the public statement.	17
D. Some former intelligence officials objected to the first draft of the public statement for being too political, one sought to “strengthen the verbiage,” and others refused to sign it altogether.....	20
E. On October 19, 2020, Morell sent the CIA the finalized public statement for review, calling it a “rush job,” and quickly secured its approval.	23
F. Contrary to the signers’ assessment, the intelligence community publicly stated that the Hunter Biden laptop was not part of a Russian disinformation campaign.	27
II. The Committees have evidence that the CIA may have promoted the statement to other intelligence community officials.....	32
III. The Biden campaign coordinated with the organizers to promote the public statement with the media.....	36
A. Morell and Shapiro worked with the Biden campaign to release the statement to the media.....	36
B. <i>Politico</i> ultimately published a story about the statement, falsely calling the Hunter Biden laptop and emails Russian disinformation.	44
C. The <i>Politico</i> article and public statement helped to support the continued suppression of the allegations uncovered from emails on Hunter Biden’s laptop.....	51
IV. The statement had its intended effect of giving Vice President Biden a “talking point” to use in the presidential debate.	53
A. Then-Vice President Biden relied on the public statement in the presidential debate to falsely assert that Hunter Biden allegations were a Russian “plan.”	53
B. The statement’s signatories celebrated after the debate.....	54
C. The Biden campaign called Morell and thanked him for his service to the campaign.	58
V. Some signatories expressed outrage about Congressional oversight into the origins of the statement.	60
Conclusion	62

I. The Biden campaign used the national security credentials of 51 former intelligence community employees to falsely discredit allegations of Biden family influence-peddling.

On October 14, 2020, the *New York Post* published a report detailing how Hunter Biden used the position and influence of his father for personal gain with the apparent awareness of President Biden.²⁷ This article raised doubts about President Biden’s earlier denial of ever speaking to his son about his international business dealings.²⁸ The *Post* reported on an email in which a Ukrainian businessman urged Hunter Biden to “use [his] influence to convey a message / signal, etc. to stop what we consider to be politically motivated actions.”²⁹ In another email, the same businessman thanked Hunter Biden for arranging a meeting with his father, calling it “an honor and pleasure.”³⁰ The *Post* reported that these emails came from a laptop belonging to Hunter Biden that he had abandoned in a Delaware computer shop.³¹

The Biden campaign knew it had a serious political liability with these allegations. This is because then-Vice President Biden’s son had monetized his relationship with his father to secure lucrative, shady opportunities overseas.³² In the days leading up to the 2020 election, Hunter Biden’s laptop and the email trove it contained provided evidence of this arrangement.³³ To prevent President Trump from effectively raising these allegations in the final presidential debate, the Biden campaign sought to discredit the allegations by employing the national security credentials of compliant former intelligence community members.

A. Biden campaign advisor Antony Blinken’s outreach to former CIA Acting Director Michael Morell was the impetus for the public statement, which was intended to give the Biden campaign a “talking point” with which to respond to the Hunter Biden allegations.

On October 17, 2020, senior Biden campaign advisor and now Secretary of State Antony Blinken called Michael Morell, the former CIA Acting Director, and asked him if he had seen the *New York Post* story on the Hunter Biden laptop and emails and whether Morell believed the Russians were involved in disseminating those emails.³⁴ Morell claimed that he had not read the story, but at that point he began researching it.³⁵ Morell testified:

²⁷ Morris & Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, *supra* note 2.

²⁸ See, e.g., Nick Givas, *Joe Biden again denies speaking to son about Ukrainian business dealings*, Fox News, Oct. 10, 2019.

²⁹ Morris & Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, *supra* note 2.

³⁰ *Id.*

³¹ *Id.*

³² See, e.g., Matt Viser et al., *Inside Hunter Biden’s multimillion-dollar deals with a Chinese energy company*, WASHINGTON POST (Mar. 30, 2022) (“But the new documents . . . illustrate the ways in which his family profited from relationships built over Joe Biden’s decades in public service.”).

³³ Morris & Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, *supra* note 2.

³⁴ Morell Interview at 18.

³⁵ Statement of Michael Morell, dated March 28, 2023, at 2 [hereinafter “Morell Statement”]; Morell Interview at 18–20.

Q. In an email to Nick Shapiro, you said that you would, quote, explain tomorrow on the phone how this came to be, meaning this public statement. . . . Can you tell us what you said to Mr. Shapiro during that call? . . .

A. Sure. I told him that I had received a call from Tony Blinken, then a senior official on the Biden campaign, asking me if I had seen *The New York Post* story. . . . I believe he summarized it for me, and he asked me if I thought the Russians may have been involved in any way in the emergence of these emails.

Q. So that was—now—

A. I should also say I don't know whether he called me or whether he sent me an email.

Q. Okay.

A. Just to be clear.

Q. In the production the committee received, we did not get an email from him—

A. Correct.

Q. —initiating that call except—but for a *USA Today* article that he forwarded—

A. Yes.³⁶

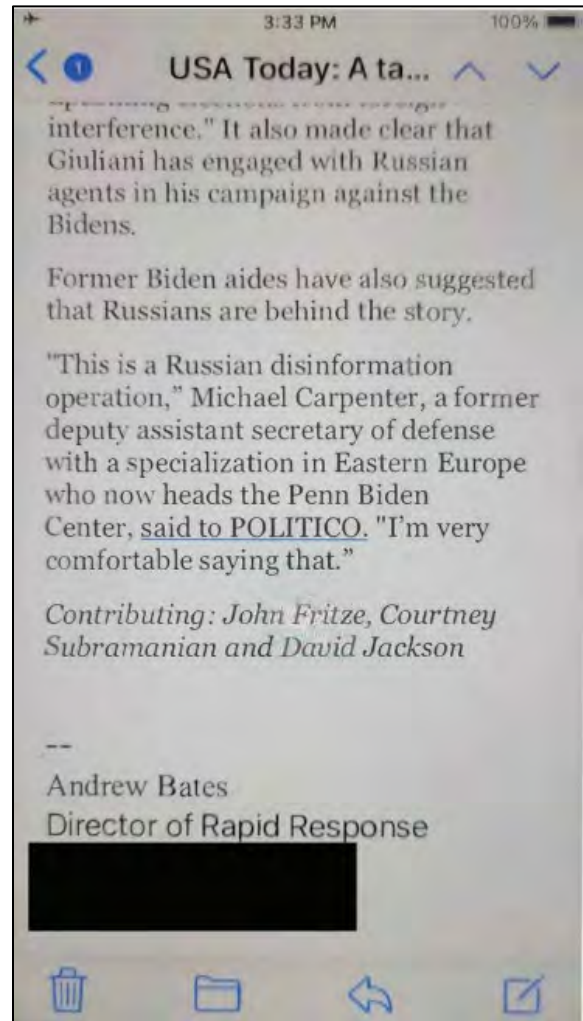
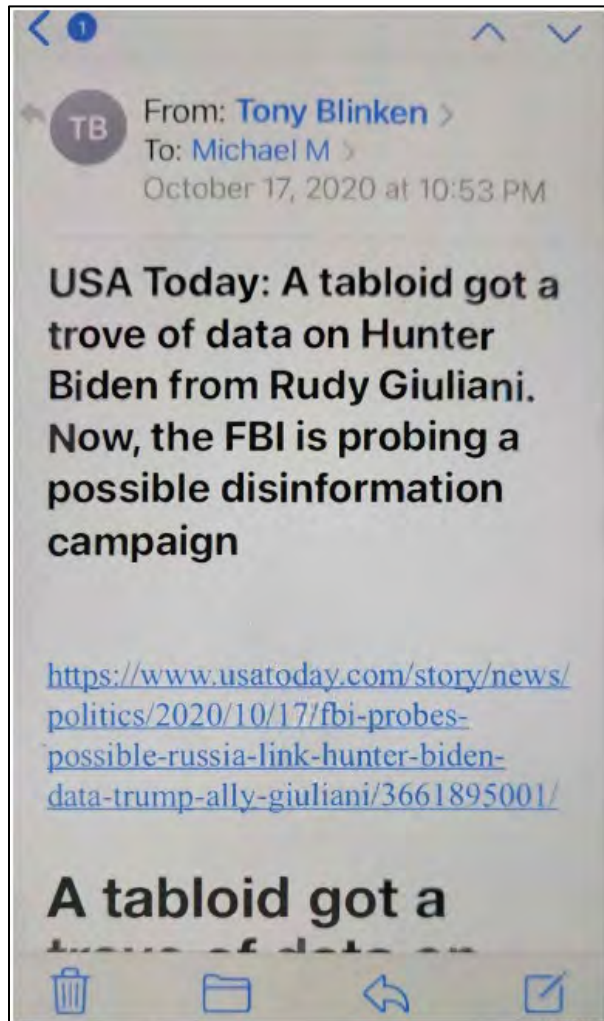
At 10:53 p.m., after his initial call with Morell, Blinken forwarded to Morell a *USA Today* article, titled “A tabloid got a trove of data on Hunter Biden from Rudy Giuliani. Now, the FBI is probing a possible disinformation campaign.”³⁷ Notably, at the bottom of Blinken’s email was the signature block of Andrew Bates, then-Director of Rapid Response for the Biden campaign.³⁸ As the Biden campaign’s Director of Rapid Response, Bates “was charged with

³⁶ Morell Interview at 20.

³⁷ Email from Tony Blinken to Michael Morell (Oct. 17, 2020, 10:53 PM) (on file with the Committees); Morell Statement at 2; Morell Interview at 18–20; *see also* Caren Bohan et al., *A tabloid got a trove of data on Hunter Biden from Rudy Giuliani. Now, the FBI is probing a possible disinformation campaign.*, USA TODAY (Oct. 17, 2020).

³⁸ Morell Statement at 2; *see* Email from Tony Blinken to Michael Morell (Oct. 17, 2020, 10:53 PM) (on file with the Committees).

defending” then-Vice President Biden “and his team against attacks on the campaign trail, while also employing an aggressive offensive strategy against President Trump and his team.”³⁹



Morell confirmed during this transcribed interview that he received two communications from Blinken on October 17, 2020. Morell speculated that the first communication occurred before 2:16 p.m. that day, based on the timestamp in a text message that Morell sent to Marc Polymeropoulos, a former CIA Acting Chief of Operations for Europe and Eurasia. The second communication was via email at 10:53 p.m. Morell testified:

- Q. There were two separate communications. There was the first call or email, and then there was the subsequent email with the *USA Today* article?
- A. Yes, sir. Yes, sir.

³⁹ Brooke Singman, *Meet the Rapid Response director: Top Biden aide on how the 2020 campaign was unlike any other*, FOX NEWS (Nov. 23, 2020).

- Q. What was the time of the email?
- A. So I don't know for sure, Congressman, but I believe he called to ask the question first and then followed up with the email.
- Q. Close together?
- A. I think—you know, given the timestamps [in the text message] on here, I feel that, you know, when I say—Congressman, I say: Just wondering if you guys, if you think the Russians played in the Hunter Biden thing. That was at 2:16 p.m. on the 17th. He sends me the *USA Today* article later that night.
- Q. Right.
- A. Right. I think he called me or sent me an email prior 2:16 p.m. So there's some gap there I think between the first contact and the second.
- Q. Okay. That's what I assumed. When you got the *USA Today* article—and I believe it was at 10:53 that evening—[that] was that the first time you had seen [the] *USA [Today]* article.
- A. So I referenced the FBI investigation in the early afternoon of the 17th in my conversation with Marc Polymeropoulos. I don't remember whether I saw it. The first thing I did when Mr. Blinken called me is I did some research. I had not read *The New York Post* article. I went and read it. I did some internet searches. I did a little bit of research here before I reached out to Marc. It's possible I found it then. It's also possible that, when Mr. Blinken called me, he mentioned it to me. I just don't remember.
- Q. In that timeframe, then, you would have got the call from Mr. Blinken prior to 2:16.
- A. I believe so, sir.
- Q. Excuse me, Mr. Morell, as part of the research that you did in between the contact with Mr. Blinken and the contact with Marc [Polymeropoulos], did you contact any individuals as a part of that research?

A. I did not.

Q. So the full sum of that research involved your internet searches?

A. Yes.⁴⁰

Morell testified that the statement was a direct result of his interactions with the Biden campaign, explaining that the call from Blinken triggered his interest in preparing the statement. He explained:

Q. But, prior to his call, you—you did not have any intent to write this statement?

A. I did not.

Q. Okay. So his call triggered—

A. It did, yes.

Q. —that intent in you?

A. Yes. Absolutely.⁴¹

Although Morell denied in his transcribed interview that the Biden campaign specifically asked that he prepare a statement,⁴² Polymeropoulos, who helped to prepare the initial draft of the statement, told the Committees that Morell “did mention to me that someone in the kind of Biden world had asked about doing this.”⁴³ When asked to elaborate, Polymeropoulos testified: “Morell said that to me, that someone from kind of the Biden world had asked for this. And he did not tell me who it was or any of the other kind of details of it.”⁴⁴

Morell testified repeatedly that his purpose for organizing, drafting, and disseminating the statement was to help Vice President Biden become president. He testified:

Q. What was the intent of the statement?

A. There were two intents. One intent was to share our concern with the American people that the Russians were playing on this issue; and, two, it was [to] help Vice President Biden.⁴⁵

⁴⁰ Morell Interview at 19-20.

⁴¹ *Id.* at 21-22.

⁴² *Id.*

⁴³ Transcribed Interview of Mr. Marc Polymeropoulos at 17 [hereinafter “Polymeropoulos Interview”].

⁴⁴ *Id.* at 21.

⁴⁵ Morell Interview at 11.

Q. So is it fair to say that the text of the letter makes it clear that the focus is actually on Russian interference, not on the political candidates?

A. It's correct. I would just repeat what I said earlier just to be, you know, totally clear, that there were two intentions here, right? One was to make clear to the American people that the Russians were interfering in the election, and the other was to help Vice President Biden in the debate.⁴⁶

Q. You wanted to help the Vice President why?

A. Because I wanted him to win the election.

Q. You wanted him to win; that's why?

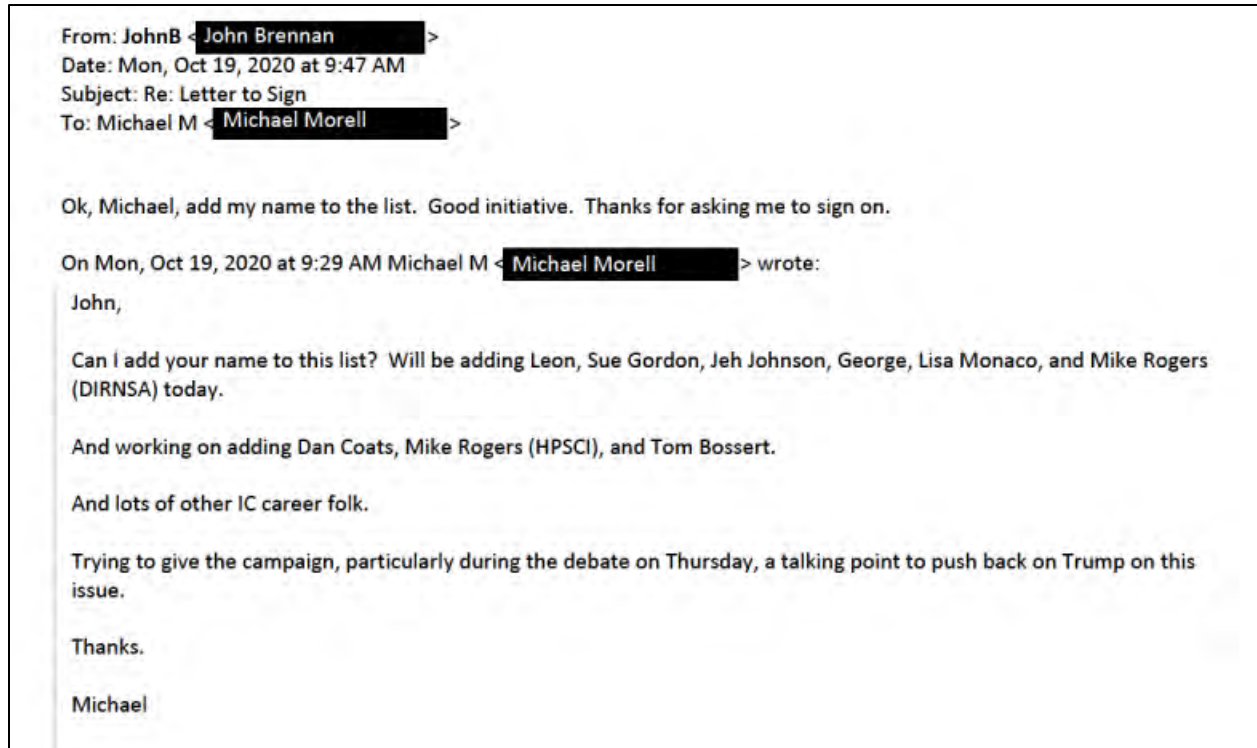
A. Yes, sir.⁴⁷

An October 19, 2020, email exchange between Morell and former CIA Director John Brennan made abundantly clear that Morell's intentions were to "give the [Biden] campaign, particularly during the debate on Thursday, a talking point to push back on [President] Trump on this issue."⁴⁸

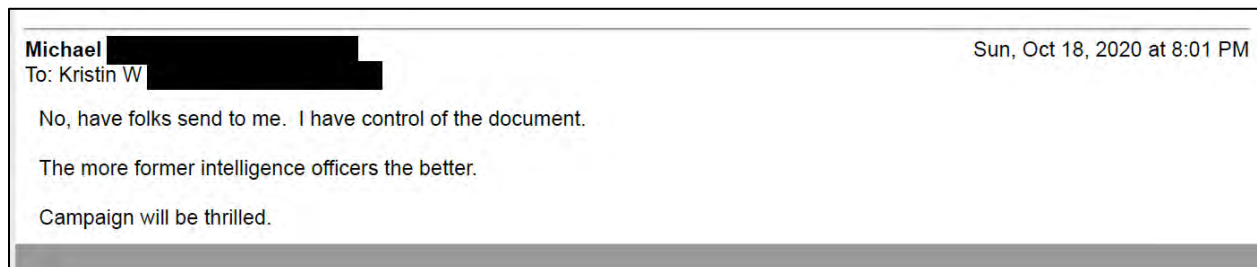
⁴⁶ *Id.* at 78.

⁴⁷ *Id.* at 102.

⁴⁸ Email from Michael Morell to John Brennan (Oct. 19, 2020, 9:29 AM) (on file with the Committees). *See also* Jim Clapper et al., *supra* note 4.



Lastly, an October 18 email from Morell to former CIA senior intelligence officer Kristin Wood shows that the statement was meant to help the Biden campaign. Morell wrote that he had “control of the document. The more former intelligence officers the better. Campaign will be thrilled.”⁴⁹



B. Morell recruited Polymeropoulos to draft the public statement.

Upon concluding his communication with Blinken and performing internet searches, Morell then enlisted Polymeropoulos to begin preparing the statement. Morell recruited Polymeropoulos because, in Morell’s wording, he was a former “acting chief of operations for the part of the world that covers Russia,” “had a very good understanding of what the Russians did in [the] 2016 [election],” and is an expert “in Russian disinformation.”⁵⁰

In a text message exchange, Morell asked Polymeropoulos if he thought “the Russians

⁴⁹ Email from Michael Morell to Kristin Wood (Oct. 18, 2020, 8:01 PM) (on file with the Committees).

⁵⁰ Morell Interview at 56-57.

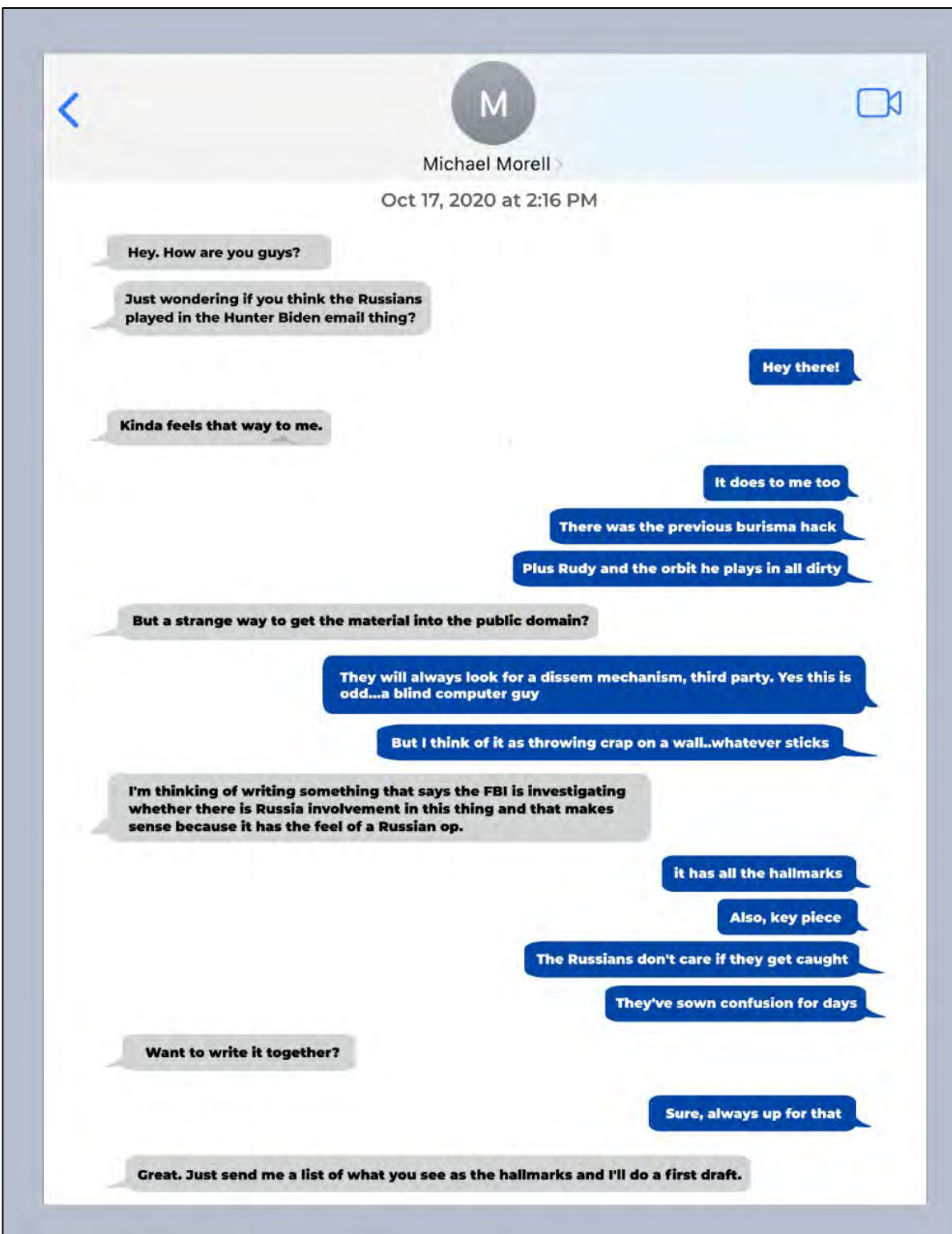
played in the Hunter Biden email thing,” opining that it “[k]inda feels that way to me.”⁵¹ Polymeropoulos responded, “It does to me too.”⁵² Morell then expressed some doubt about the “strange” way in which the emails were placed “into the public domain,” with Polymeropoulos responding: “They,” presumably referring to the Russians, “will always look for a dissem[ination] mechanism third party. Yes this is odd . . . a blind computer guy.”⁵³ After Polymeropoulos agreed to work with Morell on the draft, Morell asked Polymeropoulos to “send me a list of what you see as the hallmarks” of Russian involvement in the story.⁵⁴

⁵¹ Text message exchange between Michael Morell to Marc Polymeropoulos (Oct. 17, 2020, 2:16 PM) (on file with the Committees).

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Id.* See also Email from Marc Polymeropoulos to Michael Morell (Oct. 17, 2020, 8:01 PM) (on file with the Committees).



Text message between Michael Morell and Marc Polymeropoulos (Oct. 17, 2020)⁵⁵

⁵⁵ Text message graphics in this report were generated by the Committee from screen shots produced by Marc Polymeropoulos. The graphics were created to assist in reading the messages.

Morell explained that Polymeropoulos wrote the first draft of the statement. Morell testified:

- Q. Okay. What was your role in the creation of the statement?
- A. I organized it.
- Q. So you drafted that?
- A. I did not do the first draft.
- Q. Okay.
- A. Marc Polymeropoulos did the first draft. Then I redrafted it. Yeah, I'm the organizer, and I played a major role in drafting it.⁵⁶

Polymeropoulos similarly testified:

- Q. And what role did Mike Morell play in the creation of the statement?
- A. . . . I think Mike Morell on the—I think it was on the 17th—had wrote me a text asking me if I thought there was any—kind of any Russian involvement in this. I said that I thought that there was, based on my professional background. He asked if I would be willing to write something with him on this. And that's how this began.⁵⁷

Polymeropoulos explained that he and Morell initially discussed preparing an op-ed, which eventually morphed into a statement. He testified:

- Q. Did you say you had a conversation with Mr. Morell?
- A. About?
- Q. About this letter. Or was it only over text message?
- A. So I think from what I recall, two—a couple things happened. First, he wrote me the text. I then—I believe he asked, and I looked at my records and I just don't have the exact date, but shortly after that he asked me to come over to his house.

⁵⁶ Morell Interview at 11.

⁵⁷ Polymeropoulos Interview at 10.

Q. Okay.

A. And we discussed this there.

I don't recall how it morphed from what I thought was an op-ed into a letter. He did mention to me that someone in the kind of Biden world had asked about doing this.

Q. But he didn't—

A. He did not tell me who it was, and I did not ask.

Q. So you prepared the backgrounder that's exhibit 4.⁵⁸

A. Right.

Q. Was that before or after you went to Morell's house?

A. I believe it was after, but I actually don't recall. I see that text was on the 17th, and I think I sent the backgrounder on the 17th as well. But I actually don't recall if this was before or after.

Q. And as you understand it, Mr. Morell took your backgrounder and turned it into the letter?

A. That's right.

Q. And do you know if any other person helped him do that?

A. I don't know.

Q. Or whether he did it himself?

A. I don't know.⁵⁹

Morell kept Polymeropoulos in the dark about his interactions with Blinken and the Biden campaign. Polymeropoulos was not aware of these facts until the Committees informed him during his transcribed interview. He testified:

Q. Are you aware that now Secretary of State Antony Blinken

⁵⁸ The "backgrounder" refers to a document Polymeropoulos created that contains the purported reasons why he believed the Hunter Biden laptop and emails were part of a Russian information operation to interfere in the 2020 presidential election. See Email from Marc Polymeropoulos to Michael Morell (Oct. 17, 2020, 8:01 PM) (on file with the Committees).

⁵⁹ *Id.* at 17-18.

called Mr. Morell some time on or about October 17th, 2020, to inquire as to whether Mr. Morell believed Russia might have been involved in the Hunter Biden email story in some way?

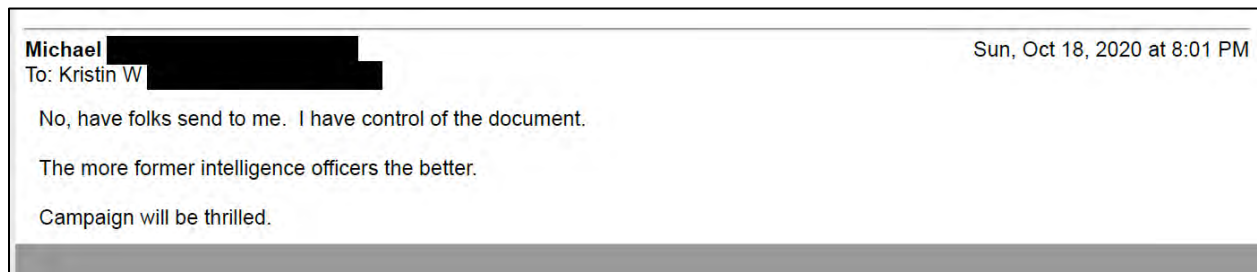
A. That's the first I heard of that. I was not aware of that at all.

Q. Were you aware that Secretary Blinken also sent an article to Mr. Morell from *USA Today* titled "A tabloid got a trove of data on Hunter Biden from Rudy Giuliani. Now, the FBI is probing a possible disinformation campaign"?

A. No.⁶⁰

C. Morell, Polymeropoulos, and former CIA officer Kristin Wood solicited other former intelligence officials and employees to sign the public statement.

As Morell testified, a goal of writing a statement was to "help Vice President Biden" win the election.⁶¹ To achieve this goal, Morell wanted to affix as many signatures from former intelligence officials and employees as he could. For Morell, "The more former intelligence officers the better."⁶²



Morell seemed to believe that the statement would have a great effect with more signatories. Morell admitted this fact to Nick Shapiro, his former Deputy Chief of Staff and Senior Advisor at the CIA, who was tasked with pushing the public statement to the media, writing: "The real power is the number of former, working-level IC officers who want the American people to know."⁶³

⁶⁰ *Id.* at 16.

⁶¹ See Morell Interview at 11, 78, 102.

⁶² Email from Michael Morell to Kirstin Wood (Oct. 18, 2020, 8:01 PM) (on file with the Committees).

⁶³ Email from Michael Morell to Nick Shapiro (Oct. 19, 2020, 8:21 PM) (on file with the Committees).

From: Michael M [REDACTED]
Sent: 10/19/2020 8:21:10 PM
To: Nick Shapiro [REDACTED]
Subject: The Letter

Will send to you shortly.

Some thoughts when dealing with reporters:

1. Between us, the campaign would like Shane Harris to go first. Please share with the campaign when you share with Shane. But, by all means, get it to other reporters as well.
2. On the record from you: What is this? A large group of former career intelligence officers, many specializing in Russia, joined by a group of former IC leaders, all saying that the Russians were somehow involved here. The IC leaders who have signed here are diverse in that they worked for the past four Presidents, including Trump. The real power here is the number of former, working-level IC officers who want the American people to know.
3. OTR: Make sure reporters know that we are not making a call on whether the materials are true or not, just that Moscow played a role in getting the information out. I'm afraid people might miss this point and say that we are saying that this is all disinformation.
4. If asked: On background from you: Why Michael? In talking to people, outside of government, who he worked with and who know Russia, he was struck by the fact that all of them thought Russia is involved here. Michael thought people should know that.
5. Also on background from you: We did not speculate on how the Russians played in this particular case because there are so many different possibilities.

Morell testified:

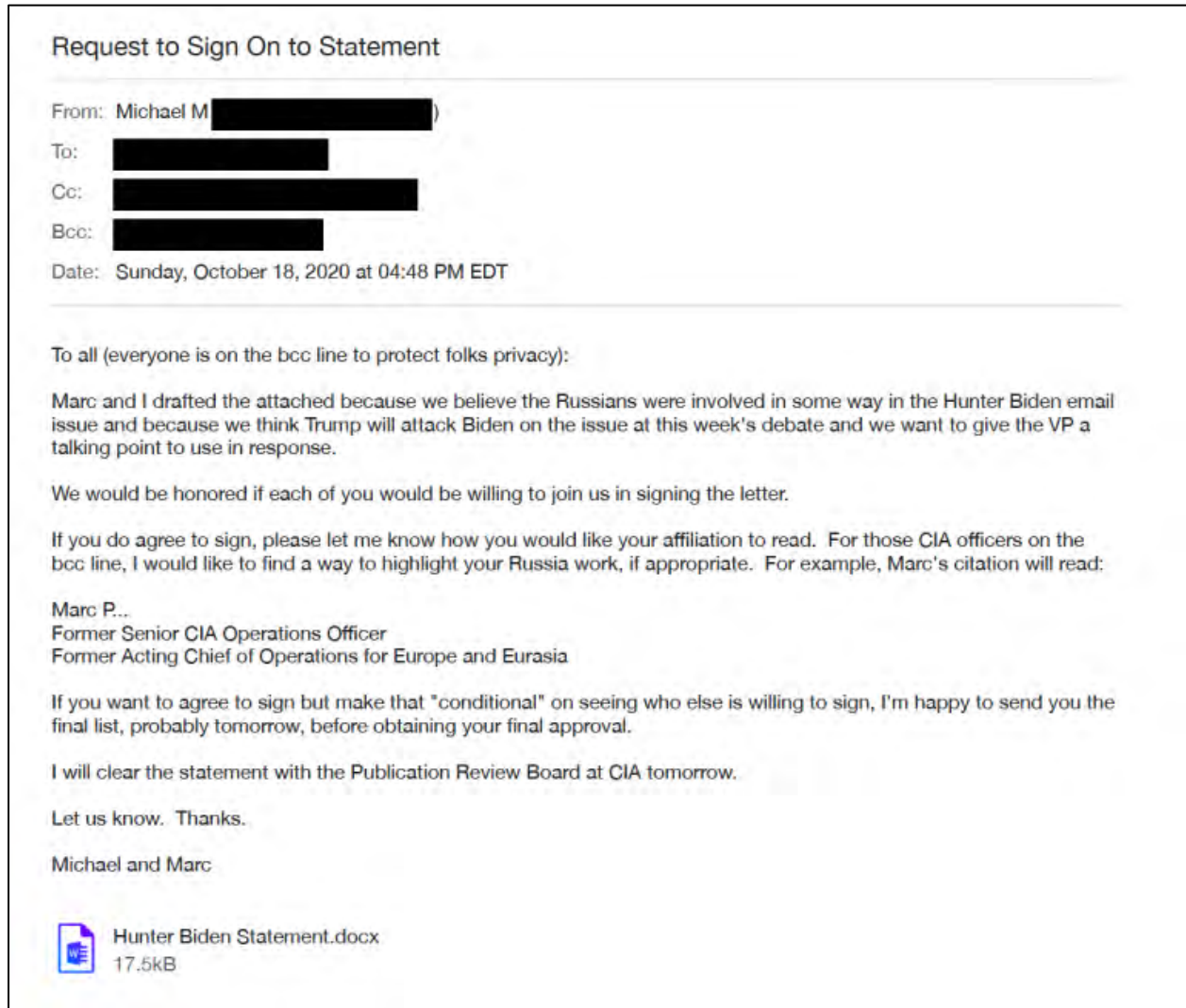
So, breaking into two pieces here, the first piece is that three of us took responsibility for sending it out to officials to try to get signatories. Myself, Marc Polymeropoulos, and a woman named Kristin Wood. Kristin worked for me at the [Central Intelligence] Agency. She worked directly for me at the Agency as my aide. We were very close friends. I asked her to do that. She agreed. And then, in terms of getting it to the media, that was entirely Nick Shapiro's responsibility here. So he took that responsibility on.⁶⁴

On October 18, Morell sent an email to several former intelligence personnel, writing about helping to give Vice President Biden "a talking point to use in" the final presidential debate.⁶⁵ Specifically, Morell wrote, "because we think Trump will attack Biden on the issue at this week's debate and we want to give the VP a talking point to use in response," Morell pleaded, "[w]e would be honored if each of you would be willing to join us in signing the

⁶⁴ Morell Interview at 15-16.

⁶⁵ Email from Michael Morell to Unnamed Intelligence Officials (Oct. 18, 2020, 4:48 PM) (on file with the Committees).

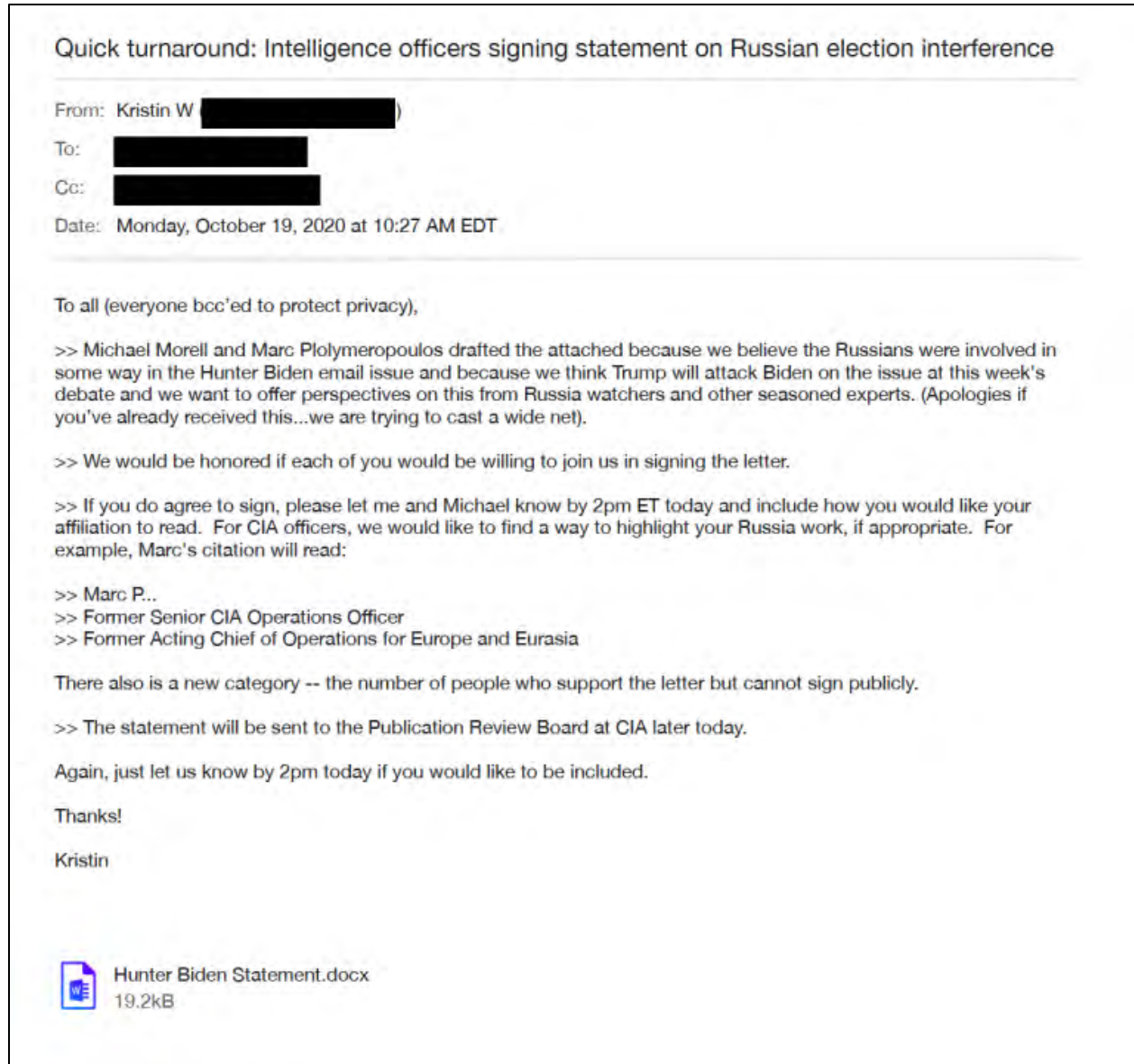
letter.”⁶⁶



The next day, Wood sent an email to several former intelligence personnel within her network, using language from Morell's email the previous day.⁶⁷

⁶⁶ *Id.*

⁶⁷ Email from Kristin Wood to Unnamed Intelligence Officials (Oct. 19, 2020, 10:27 AM) (on file with the Committees).



Like Morell, Wood wrote that the group intended for the public statement to help then-Vice President Biden's candidacy, specifically in regards to the upcoming debate: "[W]e think Trump will attack Biden on the issue at this week's debate and we want to offer perspectives on this from Russia watchers and other seasoned experts."⁶⁸

D. Some former intelligence officials objected to the first draft of the public statement for being too political, one sought to "strengthen the verbiage," and others refused to sign it altogether.

The initial statement was so nakedly partisan that some of the former intelligence officials refused to sign it until portions of it were removed. In the initial draft, Morell and Polymeropoulos included two paragraphs about Vice President Biden's relationship with

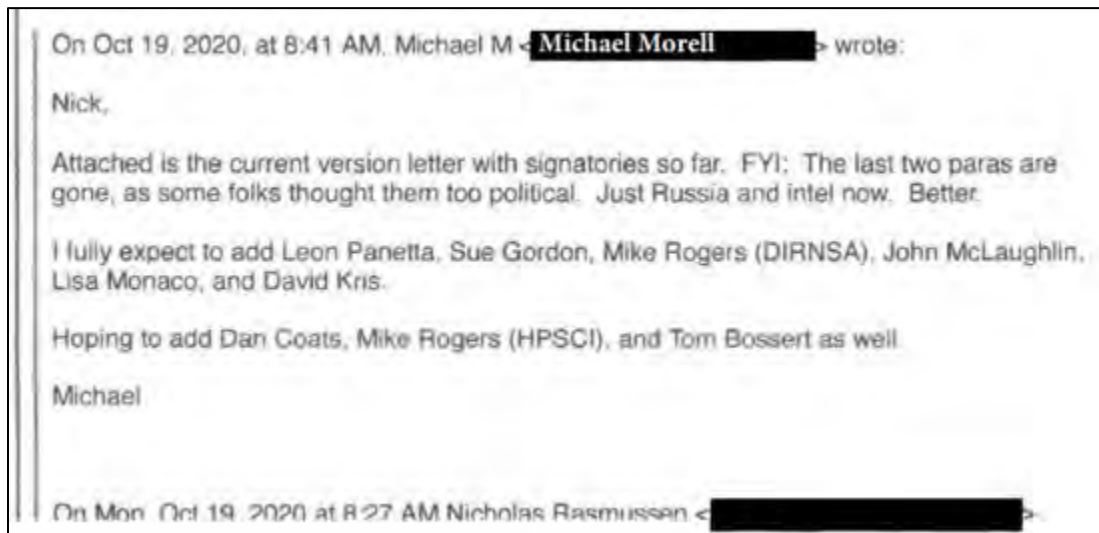
⁶⁸ *Id.*

Ukraine, which were later omitted from the final version of the public statement:

For those who argue that it is important for the truth to come out – even if it comes at the cost of foreign interference – let us share our understanding of the what [*sic*] transpired between Vice President Biden and the Ukrainians. It is not what Biden’s opponents want Americans to think.

When the Vice President took a private and public stand against the then Prosecutor General of Ukraine Victor Shokin, he did so as a matter of Obama Administration policy, because Shokin was corrupt, because he was not investigating corruption in Ukraine, and because the Obama Administration wanted a prosecutor who would. This included any corruption at Burisma. Shokin was not investigating Burisma. Biden was not protecting Burisma. Indeed, by arguing that Ukraine needed an aggressive prosecutor, Biden was arguing for just the opposite. The Russians want you to think otherwise.⁶⁹

Some of the signatories objected to these paragraphs as “too political,” as shown in an email exchange between Morell and Nick Rasmussen, former Director of the National Counterterrorism Center. Morell explained to Rasmussen that “some folks thought [the two paragraphs] too political. Just Russia and intel now. Better.”⁷⁰



In addition to the edits removing reference to Ukraine, other emails show that former Director of National Intelligence James Clapper offered editorial advice to “strengthen the verbiage.”⁷¹ On October 18, after reviewing the draft statement, Clapper emailed Morell that he

⁶⁹ Email from Michael Morell to Unnamed Intelligence Officials (Oct. 19, 2020, 1:38:31 AM) (on file with the Committees).

⁷⁰ Email from Michael Morell to Nick Rasmussen (Oct. 19, 2020, 8:41 AM) (on file with the Committees).

⁷¹ Email from James Clapper to Michael Morell (Oct. 18, 2020, 6:10 PM) (on file with the Committees).

would “gladly sign on,” having “said as much [about the Hunter Biden laptop and emails] on CNN Friday evening.”⁷² He also offered an editorial suggestion to a key phrase in the statement:

I have one editorial suggestion for the letter: I think it would strengthen the verbiage if you say this has all the classic earmarks of a Soviet/Russian information operation rather than the “feel” of a Russian operation.⁷³

On Sun, Oct 18, 2020 at 6:10 PM James Clapper <[REDACTED]> wrote:

Michael:

I'll gladly sign on; I said as much on CNN Friday evening.

I have one editorial suggestion for the letter: I think it would strengthen the verbiage if you say this has all the classic earmarks of a Soviet/Russian information operation rather than the “feel” of a Russian operation.

Jim

Morell responded that Clapper’s “editorial suggestion has been made. It was a good one.”⁷⁴

From: Michael M <Michael Morell >
 Sent: Sunday, October 18, 2020 7:47 PM
 To: James Clapper <[REDACTED]>
 Subject: Re: Request to Sign On to Statement

Jim,

Thanks.

And, your editorial suggestion has been made. It was a good one.

Michael

Other former national security officials were approached and declined to sign the statement.⁷⁵ By his own account, Morell solicited the signatures of 36 former intelligence officials,⁷⁶ 26 of whom did not sign. Ultimately, the following individuals agreed to add their name to the statement:

Jim Clapper;
 Mike Hayden;
 Leon Panetta;

John Brennan;
 Thomas Finger;
 Rick Ledgett;

⁷² *Id.*

⁷³ *Id.*

⁷⁴ Email from Michael Morell to James Clapper (Oct. 18, 2020, 7:47 PM) (on file with the Committees).

⁷⁵ Morell Interview at 14.

⁷⁶ See Morell Statement at 3 n.9.

John McLaughlin;
 Michael Morell;
 Mike Vickers;
 Doug Wise;
 Nick Rasmussen;
 Russ Travers;
 Andy Liepman;
 John Moseman;
 Larry Pfeiffer;
 Jeremy Bash;
 Rodney Snyder;
 Glenn Gerstell;
 David B. Buckley;
 Nada Bakos;
 Patty Brandmaier;
 James B. Bruce;
 David Cariens;
 Janice Cariens;
 Paul Kolbe;
 Peter Corsell;
 Brett Davis;
 Roger Zane George;
 Steven L. Hall;

Kent Harrington;
 Don Hepburn;
 Timothy D. Kilbourn;
 Ron Marks;
 Jonna Hiestand Mendez;
 Emile Nakhleh;
 Gerald A. O'Shea;
 David Priess;
 Pam Purcilly;
 Marc Polymeropoulos;
 Chris Savos;
 Nick Shapiro;
 John Sipher;
 Stephen Slick;
 Cynthia Strand;
 Greg Tarbell;
 David Terry;
 Greg Treverton;
 John Tullius;
 David A. Vanell;
 Winston Wiley; and
 Kristin Wood.⁷⁷

E. On October 19, 2020, Morell sent the CIA the finalized public statement for review, calling it a “rush job,” and quickly secured its approval.

On October 19, 2020, at 6:34 a.m., Morell sent the final version of the statement to the CIA’s Prepublication Classification Review Board (PCRB) for review.⁷⁸ According to Morell, the PCRB consists of CIA officers—“not contractors”—and their sole function is to determine whether former and current CIA personnel are disclosing classified information in any materials they may release publicly.⁷⁹ This is because “[a]ll CIA officers, as a condition of employment, sign the standard CIA secrecy agreement when entering on duty . . . [and this] **lifelong** obligation which exists to help avoid the damage to national security” requires they submit any materials they intend to publicize to the PCRB for approval.⁸⁰

Morell directed the PCRB that “[t]his is a rush job, as it need to get out as soon as possible.”⁸¹ Morell wanted the public statement released before the October 22, 2020, presidential debate. Specifically, he testified:

⁷⁷ Jim Clapper et al., *supra* note 4; Bertrand, *supra* note 4.

⁷⁸ Email from Michael Morell to PCRB staff (Oct. 19, 2020, 6:34 AM) (on file with the Committees).

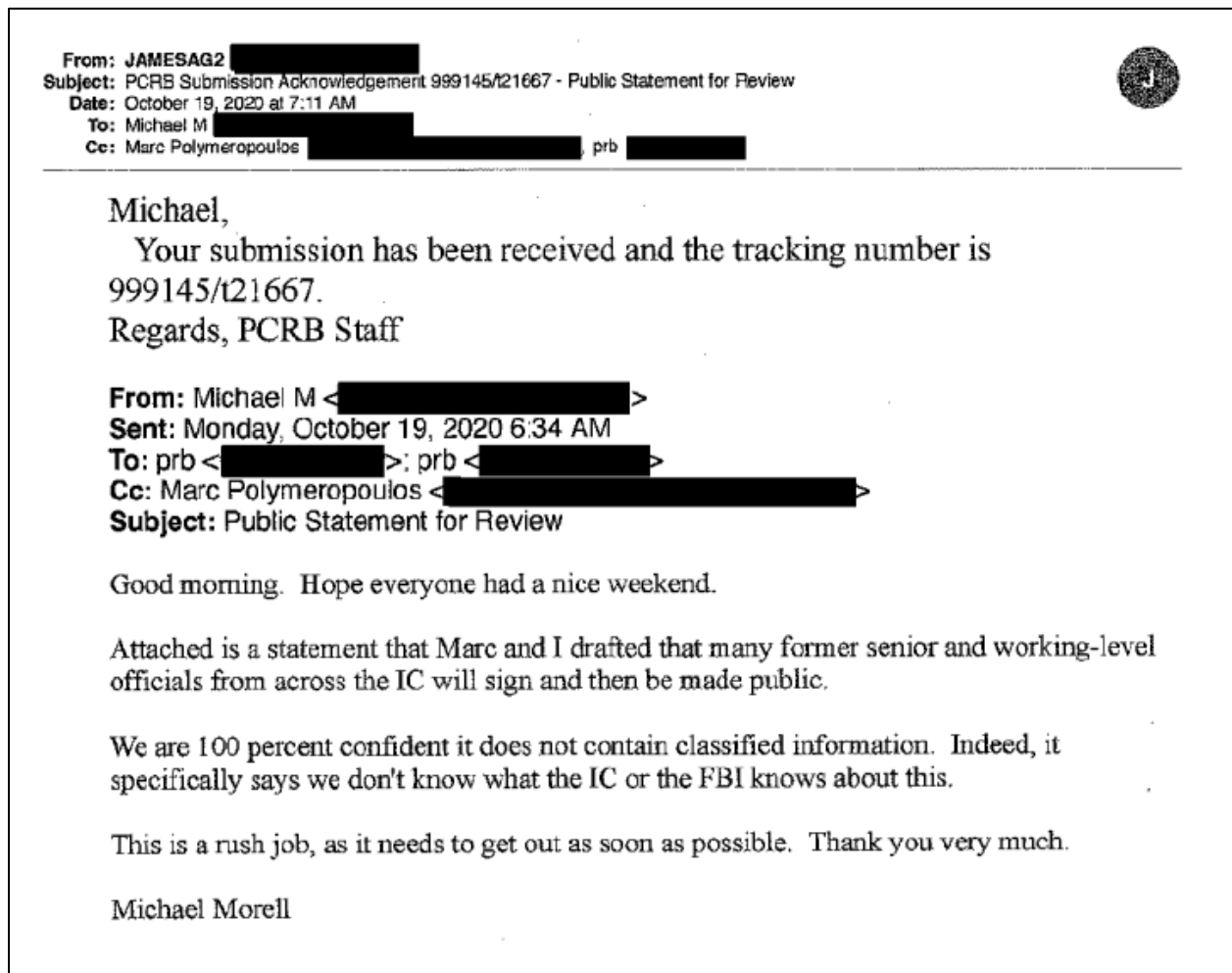
⁷⁹ Morell Interview at 29.

⁸⁰ CIA, PREPUBLICATION CLASSIFICATION REVIEW BOARD, <https://www.cia.gov/about/organization/prepublication-classification-review-board/> (emphasis in original).

⁸¹ Email from Michael Morell to PCRB Staff (Oct. 19, 2020, 6:34 AM).

- Q. And, in this, you described . . . it as a rush job to the officials at the CIA. Why? Were you trying to get it out?
- A. We were trying to get it out before the debate, yes.
- Q. Before the debate?
- A. Yes, ma'am.⁸²

The PCRB responded on October 19, 2020, at 7:11 a.m., that it received the submission.⁸³



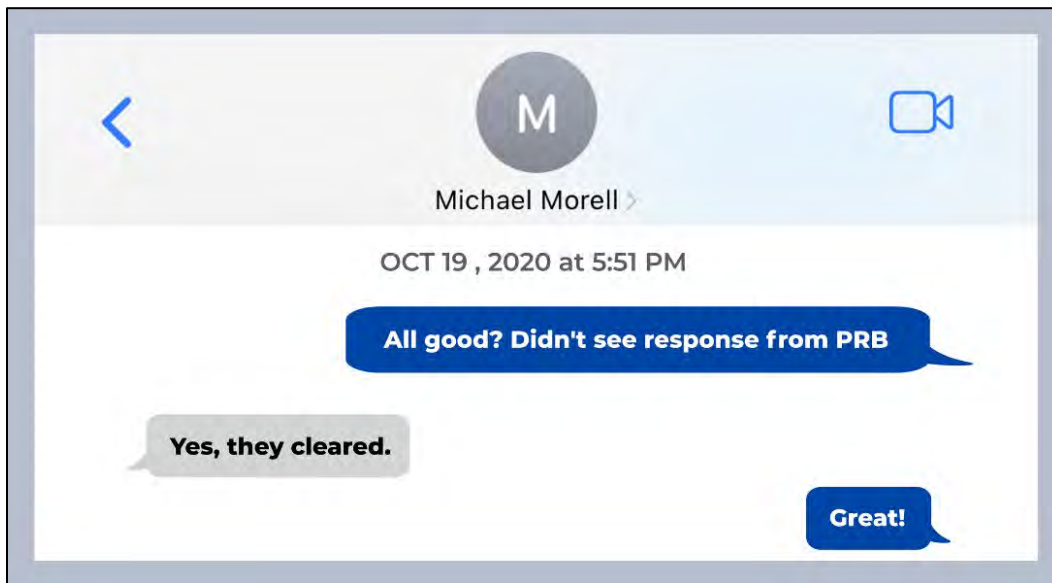
Morell testified the statement was “approved . . . as written.”⁸⁴ Although the timing of the PCRB’s approval is uncertain, it appears to have come before 5:51 p.m. In response to a text message at that time from Polymeropoulos, who “[d]idn’t see” a response from PCRB, Morell

⁸² Morell Interview at 28. COMM. ON PRESIDENTIAL DEBATES, *supra* note 5.

⁸³ Email from JAMESAG2 to Michael Morell (Oct. 19, 2020, 07:11 AM) (on file with the Committees) (“Michael, [y]our submission has been received and the tracking number is 999145/t21667. Regards, PCRB Staff.”);

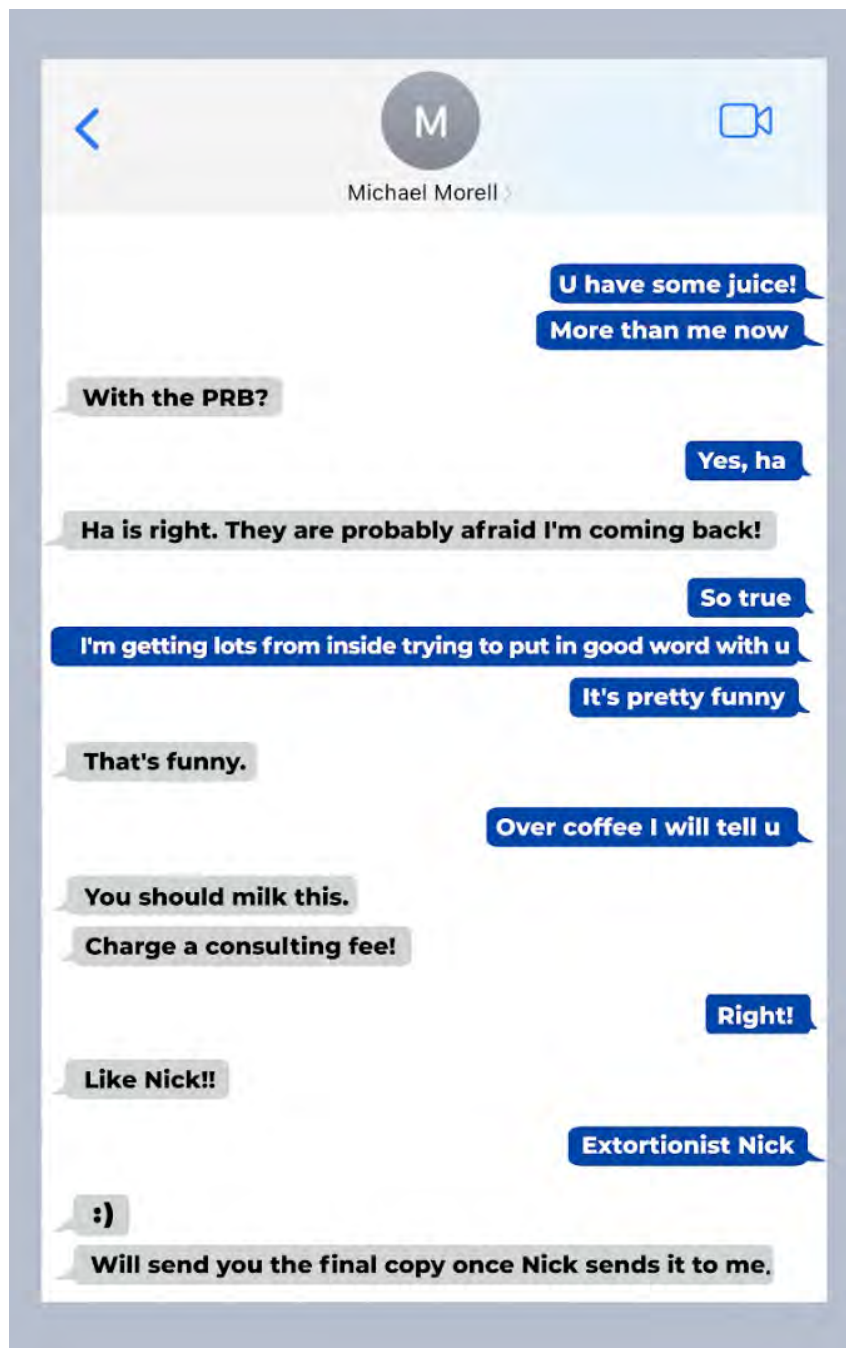
⁸⁴ Morell Interview at 28.

texted that the PCRB “cleared” the statement.⁸⁵ Notably, none of the former intelligence officials who signed the letter and produced documents to the Committees, including Morell, have produced the PCRB’s email approving the statement.



Text message between Michael Morell and Marc Polymeropoulos (Oct. 19, 2020)

⁸⁵ Text message from Marc Polymeropoulos to Michael Morell (Oct. 19, 2020, 5:51 PM) (on file with the Committees).



Text message between Michael Morell and Marc Polymeropoulos (Oct. 19, 2020)

Morell testified:

- Q. And was the email the only communication you had with the CIA?
- A. Yes.
- Q. You did not speak to any of the officials on the phone?

A. I did not. I did not.⁸⁶

F. Contrary to the signers' assessment, the intelligence community publicly stated that the Hunter Biden laptop was not part of a Russian disinformation campaign.

On October 19, while Morell and others worked procuring more signatories for the statement, Director of National Intelligence John Ratcliffe—who, unlike the statement's signatories, was in government as the top intelligence official in the United States and privy to all classified information—stated publicly that “Hunter Biden’s laptop is not part of some Russian disinformation campaign.”⁸⁷ He further stated: “Let me be clear: The intelligence community doesn’t believe that because there is no intelligence that supports that.”⁸⁸ Director Ratcliffe issued this statement in response to Congressman Adam Schiff’s claim that Hunter Biden’s laptop and emails came “from the Kremlin. That’s been clear for well over a year now that they’ve been pushing this false narrative about the vice president and his son.”⁸⁹



⁸⁶ Morell Interview at 28. Morell has not produced the email from the PRCB approving the public statement. In his statement to the Committees, Morell stated that his document production is incomplete because, since 2015, he began “to regularly delete all communications in his personal email account.” Morell Statement at 1.

⁸⁷ Mark Moore, *DNI John Ratcliffe says info on Hunter Biden laptop isn’t Russian disinformation*, N.Y. POST (Oct. 19, 2020).

⁸⁸ *Id.*

⁸⁹ Olivia Beavers & Joe Concha, *Ratcliffe, Schiff battle over Biden emails, politicized intelligence*, THE HILL (Oct. 19, 2020).

Rather than give the then-Director of National Intelligence's statement credence or at least a modicum of deference, Morell rejected it wholesale. He testified:

Q. So did the statement put out by the Director of National Intelligence that day or earlier that morning, did that have any influence on your decision with the letter, specifically, what Mr. Ratcliffe said?

A. No.

Q. Even though he said . . . the emails were not part of some Russian disinformation operation.

A. It did not because, as a former intelligence officer with much more experience than Mr. Ratcliffe, I don't know how he could have come to that conclusion. How could he know . . . it wasn't part of Russian disinformation?

Q. So you were obviously aware of Mr. Ratcliffe's statement that morning before you sent the letter out?

A. Yes.

Q. And, as you sit here today, do you believe the Russians were involved in the Hunter Biden laptop matter?

A. I don't know. I mean, I still have suspicions, Congressman.

Q. Would you organize such a letter today knowing what you know now?

A. I would have to write it differently because we now know the emails are authentic, right? So you couldn't say anymore we don't know whether it's information or disinformation. But I still have suspicions about a Russian role in these emails getting to *The New York Post*.⁹⁰

The Federal Bureau of Investigation (FBI) ratified Director Ratcliffe's statement. In a letter to Senator Ron Johnson, then-Chairman of the Senate Committee on Homeland Security and Governmental Affairs, the FBI stated, "we have nothing to add at this time to the October 19th public statement by the Director of National Intelligence about the available actionable intelligence" on Hunter Biden's laptop and emails.⁹¹

⁹⁰ Morell Interview at 37, 39.

⁹¹ Even Perez, *FBI says it has 'nothing to add' to Ratcliffe's claim on Russian disinformation*, CNN (Oct. 21, 2020).



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

October 20, 2020

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Johnson:

This responds to your letter, dated October 17, 2020, to the Federal Bureau of Investigation (FBI) regarding the authenticity of certain information provided to your Committee, including whether such information is linked to a foreign adversary's influence operation or is otherwise fraudulent. You also ask several questions about a laptop computer reportedly produced pursuant to a grand jury subpoena.

As you may know, the Office of the Director of National Intelligence has advised the American public that, in advance of the 2020 election, a number of nation-states plan to use covert and overt influence measures in an attempt to sway voter preferences and perspectives, sow discord in the United States, and undermine the confidence of Americans in our democratic process. The FBI is the primary investigative agency responsible for the integrity and security of the 2020 election, and as such, we are focused on an array of threats, including the threat of malign foreign influence operations. Regarding the subject of your letter, we have nothing to add at this time to the October 19th public statement by the Director of National Intelligence about the available actionable intelligence. If actionable intelligence is developed, the FBI in consultation with the Intelligence Community will evaluate the need to provide defensive briefings to you and the Committee pursuant to the established notification framework.

Finally, as the FBI advised the Committee in its letter, dated October 5, 2020, consistent with longstanding Department of Justice (Department) policy and practice, the FBI can neither confirm nor deny the existence of any ongoing investigation or persons or entities under investigation, including to Members of Congress. As the Inspector General firmly reminded the Department and the FBI in recent years, this policy is designed to preserve the integrity of all Justice Department investigations and the Department's ability to effectively administer justice without political or other undue outside influences. Therefore, the FBI cannot provide any additional information in response to the enumerated questions in your letter.

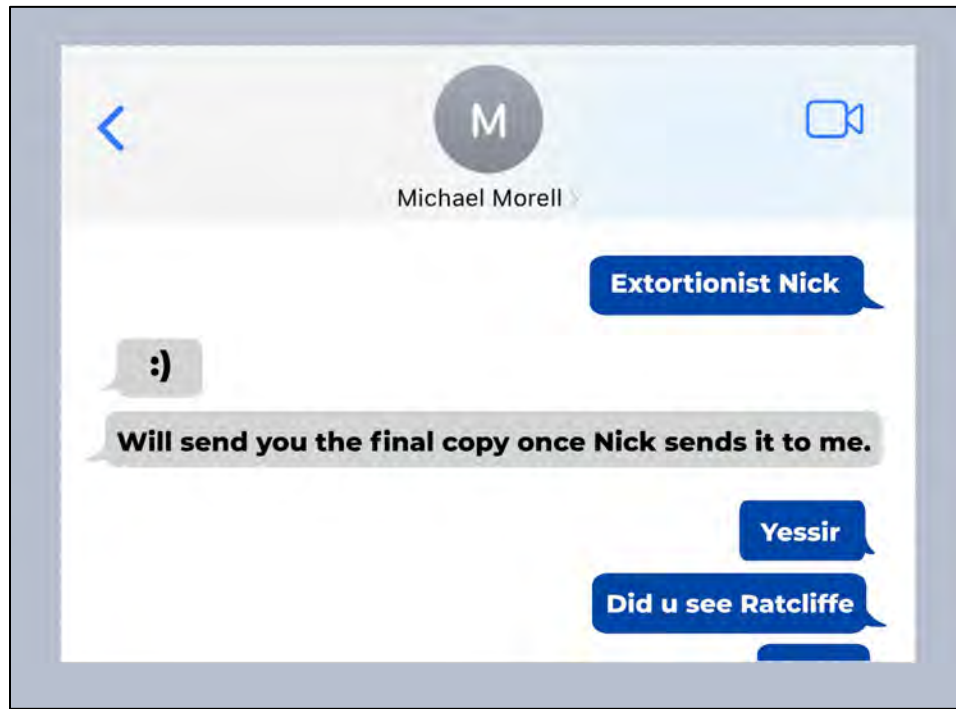
Thank you for your support of the FBI, its mission, and its people.

Sincerely,

Jill C. Tyson
Assistant Director
Office of Congressional Affairs

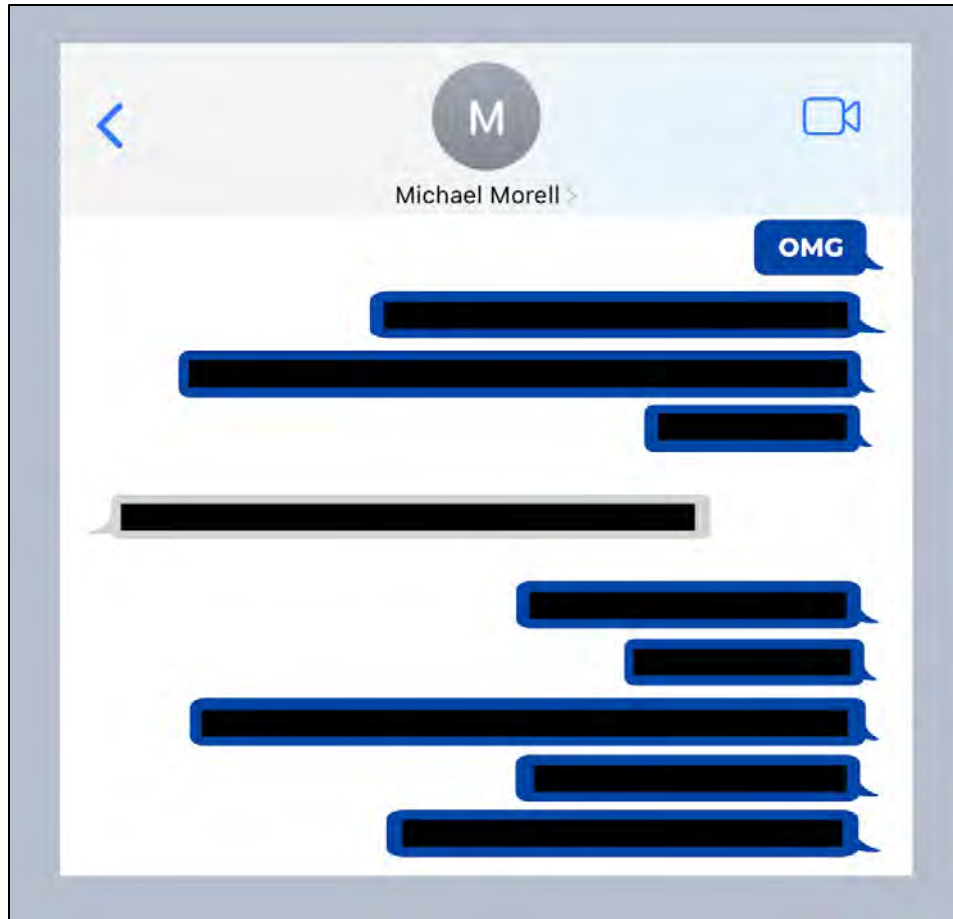
Letter from FBI to Senator Ron Johnson (Oct. 20, 2020)

Even after learning of Ratcliffe’s statement that the laptop and emails were not Russian disinformation, Morell and Polymeropoulos were not dissuaded. In one text exchange on October 19, Polymeropoulos remarked to Morell: “Did u see Ratcliffe[?] Omg[.]”⁹²



Text message between Michael Morell and Marc Polymeropoulos (Oct. 19, 2020)

⁹² Text message from Marc Polymeropoulos to Michael Morell (Oct. 19, 2020, 5:51 PM) (on file with the Committees). Polymeropoulos produced these text messages to the Committees with redactions, including what follows “OMG.”



Text message between Michael Morell and Marc Polymeropoulos (Oct. 19, 2020)

II. The Committees have evidence that the CIA may have promoted the statement to other intelligence community officials.

According to a written statement provided to the Committees by former CIA official David Cariens, the CIA—or at least an employee of the CIA—may have helped in the effort to solicit signatures for the statement. Cariens explained that he spoke with the PCRB in October 2020 regarding the review of his memoir and during that call the CIA employee “asked” him if he would sign the statement.⁹³ As Cariens explained:

When the person in charge of reviewing the book called to say it was approved with no changes, I was told about the draft letter. The person asked me if I would be willing to sign. . . . After hearing the letter’s contents, and the qualifiers in it such as, “We want to emphasize that we do not know if the emails provided to the *New York Post* by President Trump’s personal attorney, Rudy Giuliani, are genuine or not and that we do not have evidence of Russian involvement . . .” I agreed to sign.⁹⁴

From: David Cariens [REDACTED]
 Sent: Sunday, March 5, 2023 3:02 PM
 To: [REDACTED]
 Subject: Re: FW: Letter for Mr. David Cariens

[REDACTED]—Thank you for acknowledging my response. My wife and I are happy to help in any way possible.

To put our position in proper perspective, my wife retired from the CIA in 1995 and has not had security clearances after that time. I retired in 1997 and continued to do contract work for the CIA and other members of the Intelligence Community. I teach intelligence and crime analysis. My contract work for the CIA ended in 2017 and I no longer had security clearances after that.

The answer to the two questions posed in the April 6, 2022 letter are:

1. I am the author of nine books, including two text books on intelligence and crime analysis. All my work is passed through the CIA’s Publications Review Board (PRE) for approval. My last book, a memoir, entitled *Escaping Madness*, was before the PRB in October, 2020. When the person in charge of reviewing the book called to say it was approved with no changes, I was told about the draft letter. The person asked me if I would be willing to sign. (I do not recall the person’s name or the exact date of the phone call.) After hearing the letter’s contents, and the qualifiers in it such as, “We want to emphasize that we do not know if the emails provided to the *New York Post* by President Trump’s personal attorney, Rudy Giuliani, are genuine or not and that we do not have evidence of Russian involvement . . .” I agreed to sign. I had been following the Hunter Biden laptop issue, and as a former director of CIA University’s course in deception analysis (with a heavy emphasis on all forms of Soviet/KGB deception), I felt there was enough circumstantial evidence to raise the suspicion that Russian intelligence was involved. I shared these views with my wife, also a former CIA officer, and she agreed to sign as well.
2. We have no documents because all of the above was done in a phone call. Neither my wife nor I have discussed the letter with any of the other signatories or any member of the U.S. policy or intelligence communities.

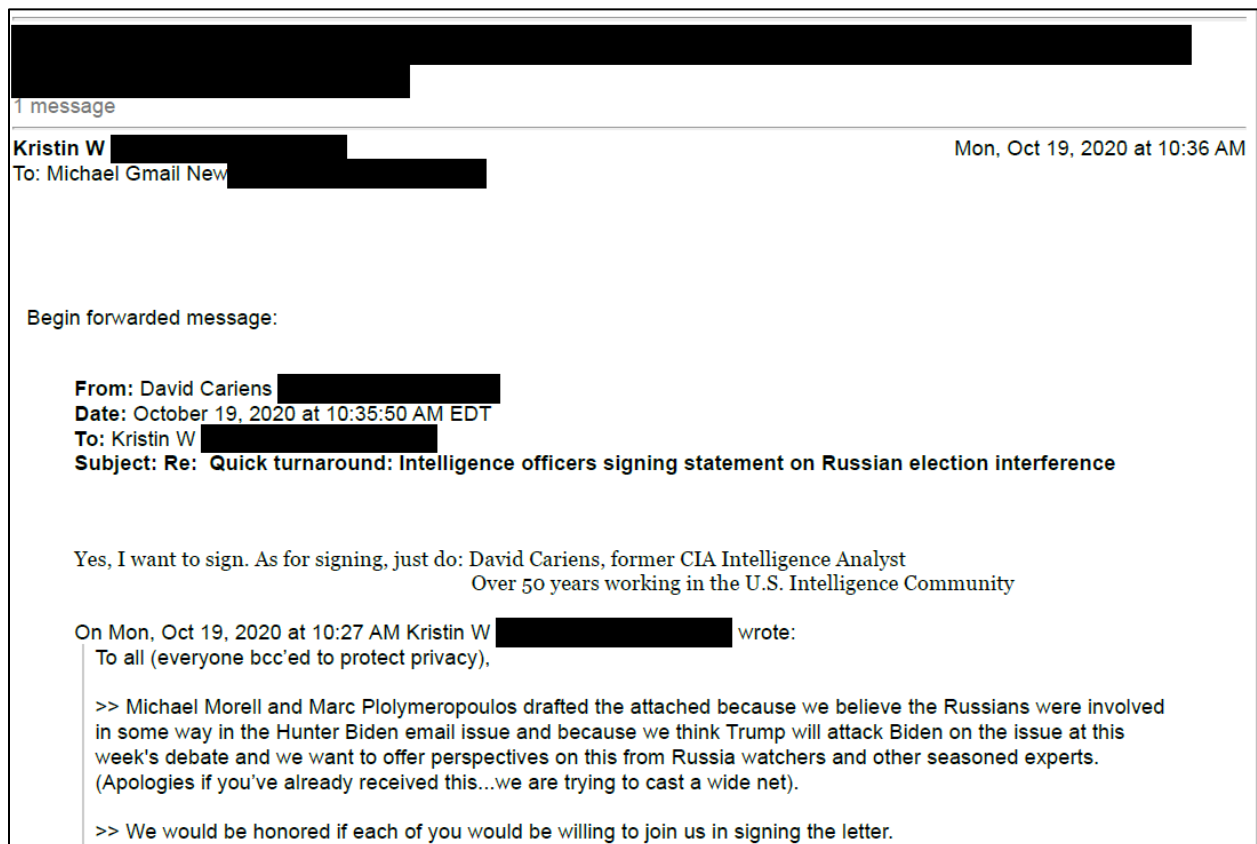
If you have any other questions, please do not hesitate to contact us. Regards, David and Janice Cariens

www.davecariens.com

⁹³ Email from David Cariens to Committee staff (March 5, 2023, 3:02 PM) (on file with the Committees).

⁹⁴ *Id.*

Cariens’s statement did not provide the precise timing of his communication with the PCRB. However, the Committees received an email exchange, produced by Kristin Wood, in which Cariens wrote, “Yes, I want to sign,” on October 19, at 10:35 a.m.—eight minutes after Wood sent the mass distribution email soliciting signatures.⁹⁵ PCRB was in possession of the statement since 6:34 a.m. on October 19, when Morell emailed it to the unit for approval.⁹⁶ PCRB acknowledged receipt of the statement, at 7:11 a.m. that same day.⁹⁷



Cariens’s revelation is potentially shocking. As he recounted, a CIA employee informed him about the statement, the CIA employee read the text of the statement to him, and the CIA employee asked Cariens if he would like to join.

Indeed, even Morell testified that such an action by a CIA employee would be “inappropriate.” Morell explained:

- A. I did not coordinate with the CIA. I would have—had I known [Cariens’s allegation], I would have reacted very negatively to this. This might—you know, had I known at the time this might have been in the letter, then I certainly would have reported this to then

⁹⁵ Email from David Cariens to Kristin Wood (Oct. 19, 2020, 10:35:50 AM) (on file with the Committees).

⁹⁶ Email from Michael Morell to PCRB staff (Oct. 19, 2020, 6:34 AM) (on file with the Committees).

⁹⁷ Email from JAMESAG2 to Michael Morell (Oct. 19, 2020, 07:11 AM) (on file with the Committees).

the Director of the Agency.

Q. And why would you have done this?

A. Because this is inappropriate.

Q. And why is it inappropriate?

A. It's inappropriate for a currently serving staff officer or contractor to be involved in the political process.

Q. Do you know the people who were engaged in this review for the CIA?

A. I do not.

Q. You don't know any of the people who work in that process.

A. I do not, sir.⁹⁸

Similarly, Polymeropoulos testified that such an action from the CIA would be “incredibly unprofessional”:

Q. Does what Mr. Cariens described there, that interaction with the PCRB, sound like a quid pro quo to you?⁹⁹

A. I can't comment on this. This is—to me, this is something that the PCRB in my experience would never engage in something like that. They are just straightforward back and forth in terms of approval. The idea they would have a comment on any other thing that they were working on, that to me is not even close to what I've experienced with them.

Q. Does that concern you?

A. If it's true, it would concern me, for sure. But I just—I have a hard time believing that occurred. If it did, that's incredibly unprofessional.¹⁰⁰

Likewise, upon being confronted with Cariens's statement, Shapiro testified:

No. I mean, I have no idea what happened here, to be very—this is

⁹⁸ Morell Interview at 30-31.

⁹⁹ *Quid pro quo*, Merriam Webster's Collegiate Dictionary, (11th ed. 2020) (“something given or received for something else.”).

¹⁰⁰ Polymeropoulos Interview at 24.

the first I'm hearing of this.

But my guess—and lawyers would probably tell me not to guess or defend the PRB, but what I could've seen happen is someone in the PRB being inappropriate and asking, hey, are you signing this thing? Which, PRB shouldn't be sharing, like, materials they get from one former with other formers. Like, that shouldn't be.

Because, as a former, if you send something—I've never sent something, but I know people who have—you're doing that because you're supposed to, but you're also hoping it stays within confidence. Like, usually, if you're going to send something to the PRB, you're sending it elsewhere, and you don't want the PRB spreading that.

So my guess for this was that it was someone who acted inappropriately and was just stupidly outing it and asking these folks if they were going to sign it.

I can't imagine the PRB trying to get someone to sign it by offering to clear something else. That would be really bad.¹⁰¹

Given the gravity of this allegation, the Committees sent a letter to CIA Director William J. Burns, on March 21, 2023, requesting documents about the CIA's review of the statement and its interactions with former CIA employees, such as Cariens, about the statement.¹⁰² The Committees requested that the CIA furnish these documents by April 4, 2023.¹⁰³ To date, the CIA has failed to respond to this request. The Committees have also sought to follow up with Cariens for additional information.

¹⁰¹ Transcribed Interview of Mr. Nick Shapiro at 26 [hereinafter "Shapiro Interview"].

¹⁰² Letter from Chairman Jim Jordan, H. Comm. on the Judiciary, and Chairman Michael R. Turner, Permanent Select Committee on Intelligence, to Hon. William J. Burns, Dir., Cent. Intel. Agency (Mar. 21, 2013).

¹⁰³ *Id.*

III. The Biden campaign coordinated with the organizers to promote the public statement with the media.

The Committees' oversight has also revealed that the Biden campaign worked with Morell and the other organizers of the statement to promote the statement publicly. Specifically, in coordination with the Biden campaign, Morell enlisted Shapiro, a long-time "national security and strategic communications" aide, to coordinate dissemination efforts with the media.¹⁰⁴

A. Morell and Shapiro worked with the Biden campaign to release the statement to the media.

According to testimony provided to the Committees, Morell worked with Shapiro to disseminate it publicly. Morell testified that, "in terms of getting [the statement] to the media, that was entirely Nick Shapiro's responsibility here. So he took that responsibility on."¹⁰⁵ Email correspondence between Morell and Shapiro, Shapiro and journalists, and Shapiro and the Biden campaign reveal the extent of this effort.

On October 19, as Morell continued to recruit former intelligence officials to affix their names to the statement, he emailed Shapiro that he "[s]hould have something to give to the media through you tomorrow afternoon."¹⁰⁶ Morell promised Shapiro that he would "explain on the phone tomorrow how this came to be."¹⁰⁷

¹⁰⁴ See 10th Avenue Consulting, <https://www.10thavenueconsulting.com/> (last visited May 4, 2023) ("Founder and CEO, Nick Shapiro has more than 15 years of crisis management, national security and strategic communications experience in the White House, at the CIA and in the private sector. Previously, Shapiro was the CIA's Deputy Chief of Staff and Senior Advisor to the Director. Shapiro also served in the White House as a Senior Counterterrorism and Homeland Security Aide on the National Security Council, and he was a National Security Spokesperson for President Obama.").

¹⁰⁵ Morell Interview at 16.

¹⁰⁶ Email from Michael Morell to Nick Shapiro (Oct. 19, 2020, 6:36:42 AM) (on file with the Committees). In emails that Mr. Shapiro produced to the Committees, the timestamps are inconsistent with the times and, in one instance, the date, in which events unfolded. When the Committees inquired about these discrepancies, Mr. Shapiro's counsel provided the following response: "[I]t appears that such timestamp inaccuracies are a common issue faced by individuals, like Mr. Shapiro, who use the Gmail email server. The primary cause for these discrepancies appears to be the result of inaccurate time zone settings in the Gmail application, the web browser, and/or the computer settings itself. Unless the user manually corrects the time zone settings in Gmail, the computer's setting, and/or their web browser, the emails will continue to reflect an inaccurate time zone – regardless of where the user may have sent the email. Although we cannot rule out other technical issues, various online publications suggest that this is the most common reason for these discrepancies." Email from Timothy Sini, counsel for Nick Shapiro, to Committee staff (May 3, 2023, 10:00 PM) (on file with the Committees). Mr. Shapiro's counsel affirmed that, despite the timestamp discrepancies, Mr. Shapiro "emailed the *Washington Post*, the *AP*, and *Politico*, prior to the publication being run in the *Politico*. He emailed [Andrew] Bates at some point after contacting at least one of these media companies and prior to *Politico* running the story." Email from Timothy Sini, counsel for Nick Shapiro, to Committee staff (May 5, 2023, 11:53 AM) (on file with the Committees).

¹⁰⁷ Email from Michael Morell to Nick Shapiro (Oct. 19, 2020, 6:36:42 AM) (on file with the Committees).

From: Michael Gmail New [REDACTED]
Sent: 10/19/2020 6:36:42 AM
To: Nick Shapiro [REDACTED]
Subject: Re: Request to Sign Statement

Great and great. I will explain tomorrow on the phone how this came to be.

I've sent the draft to David Kris and Lisa Monaco but have not yet heard back. They should sign.

I'm looking for two things — pairs of senior who served in the same position from different administrations (Hayden and Panetta, Jeh Johnson and Mike Chertoff, Lisa and Ken Wainstein, Clapper and Coats, etc) and then a slew of former IC and national security who worked Russia.

Should have something to give to the media through you tomorrow afternoon. Let's talk when you get a chance in the morning.

Sent from my iPad

On Oct 18, 2020, at 11:55 PM, Nick Shapiro [REDACTED] wrote:

happy to sign and will also send around to folks if you want me to

Nick Shapiro
 Former CIA Deputy Chief of Staff and Senior Advisor to the Director

Later on October 19, Morell sent Shapiro “some thoughts when dealing with reporters.”¹⁰⁸ Specifically, Morell informed Shapiro that, “[b]etween us,” the Biden campaign preferred that a certain reporter with the *Washington Post* run the statement first.¹⁰⁹ Morell asked Shapiro to “share with the campaign when you share with” the reporter.¹¹⁰ Morell also sent Shapiro a lengthy script of information to share on various levels of sourcing—on the record, off the record, and on background.¹¹¹

¹⁰⁸ Email from Michael Morell to Nick Shapiro (Oct. 19, 2020, 8:21:10 PM) (on file with the Committees).

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

From: Michael M [REDACTED]
Sent: 10/19/2020 8:21:10 PM
To: Nick Shapiro [REDACTED]
Subject: The Letter

Will send to you shortly.

Some thoughts when dealing with reporters:

1. Between us, the campaign would like [REDACTED] to go first. Please share with the campaign when you share with [REDACTED]. But, by all means, get it to other reporters as well.
2. On the record from you: What is this? A large group of former career intelligence officers, many specializing in Russia, joined by a group of former IC leaders, all saying that the Russians were somehow involved here. The IC leaders who have signed here are diverse in that they worked for the past four Presidents, including Trump. The real power here is the number of former, working-level IC officers who want the American people to know.
3. OTR: Make sure reporters know that we are not making a call on whether the materials are true or not, just that Moscow played a role in getting the information out. I'm afraid people might miss this point and say that we are saying that this is all disinformation.
4. If asked: On background from you: Why Michael? In talking to people, outside of government, who he worked with and who know Russia, he was struck by the fact that all of them thought Russia is involved here. Michael thought people should know that.
5. Also on background from you: We did not speculate on how the Russians played in this particular case because there are so many different possibilities.

In the background information that Morell gave Shapiro to tell reporters, Morell claimed the genesis of the public statement came from feedback from other Russia experts: “In talking to people, outside of government, who [Morell] worked with and who know Russia, [Morell] was struck by the fact that all of them thought Russia is involved here. [Morell] thought people should know that.”¹¹² This assertion is disingenuous for several reasons.

First, Morell admitted in testimony to the Committees that he spearheaded the effort to publish the public statement for overtly political reasons—to help Vice President Biden in the debates and ultimately win the election.¹¹³ Second, other than soliciting thoughts from and collaborating with Polymeropoulos,¹¹⁴ Morell testified he did not speak to anyone about potential Russian involvement with Hunter Biden’s laptop, but rather researched the issue himself following his conversation with Blinken. He explained:

- A. The first thing I did when Mr. Blinken called me is I did some research. I had not read *The New York Post* article. I went and read it. I did some internet searches. I did a little

¹¹² *Id.*

¹¹³ See Morell Interview at 11, 78, 102.

¹¹⁴ See text message exchange between Michael Morell to Marc Polymeropoulos (Oct. 17, 2020, 2:16 PM) (on file with the Committees).

bit of research here before I reached out to [Polymeropoulos].

- Q. [A]s part of the research that you did in between the contact with Mr. Blinken and the contact with [Polymeropoulos], did you contact any individuals as a part of your research?
- A. I did not.¹¹⁵

Finally, Morell’s claim is undercut by his disclosure that a majority of the people who he asked to sign the statement declined to do so.¹¹⁶ Although the precise reasons they declined are not yet known, these facts cast doubt on Morell’s intended perception that a groundswell of Russia experts organically concluded that the Hunter Biden laptop was a Russian intelligence operation.

Shapiro emailed the *Washington Post* reporter the statement, along with scripted on-the-record comments and background information.¹¹⁷ It is important to note that Shapiro kept one of the most important elements of this story off the record—namely, “We are not making a call on whether the materials are true or not, just that Moscow played a role in getting the information out.”¹¹⁸

¹¹⁵ Morell Interview at 20

¹¹⁶ See Morell Statement at 3 n.9. Bertrand, *supra* note 4. Morell solicited the signatures of 36 former intelligence officials, and 26 of those individuals did not sign the public statement.

¹¹⁷ Email from Nick Shapiro to *Washington Post* reporter (Oct. 19, 2020, 9:25 PM) (on file with the Committees).

¹¹⁸ *Id.*

From: Nick Shapiro [REDACTED]
Sent: 10/19/2020 9:25:33 PM
To: [REDACTED]
Subject: The Letter
Attachments: Former IC Officers Public Statement.docx

Ok - here you go.

Giving this to you exclusively first if you guys want to run with it. Then will give to others once you post.

You can also use this **on the record** from me (Nick Shapiro, Former CIA Deputy Chief of Staff and Senior Advisor to the Director) describing what this is:

"A large group of former career intelligence officers, many specializing in Russia, joined by a group of former intelligence community leaders, are all saying that they believe the Russians were somehow involved here. The IC leaders who have signed this letter worked for the past four Presidents, including Trump. The real power here however is the number of former, working-level IC officers who want the American people to know that once again the Russians are interfering."

Off The Record: We are not making a call on whether the materials are true or not, just that we believe Moscow played a role in getting the information out.

On Background: We did not speculate on how exactly the Russians played in this particular case because there are so many different possibilities.

Appearing not to receive a favorable response from their preferred *Washington Post* journalist, Shapiro sent the public statement and an identical email to an *Associated Press* reporter about two hours later.¹¹⁹

¹¹⁹ Email from Nick Shapiro to *Associated Press* reporter (Oct. 19, 2020, 11:15 PM) (on file with the Committees).

From: Nick Shapiro [REDACTED]
Sent: 10/19/2020 11:15:06 PM
To: [REDACTED]
Subject: The Letter
Attachments: Former IC Officers Public Statement.docx

Ok - here you go.

Giving this to you exclusively first if you guys want to run with it. Then will give to others once you post.

You can also use this **on the record** from me (Nick Shapiro, Former CIA Deputy Chief of Staff and Senior Advisor to the Director) describing what this is:

"A large group of former career intelligence officers, many specializing in Russia, joined by a group of former intelligence community leaders, are all saying that they believe the Russians were somehow involved here. The IC leaders who have signed this letter worked for the past four Presidents, including Trump. The real power here however is the number of former, working-level IC officers who want the American people to know that once again the Russians are interfering."

Off The Record: We are not making a call on whether the materials are true or not, just that we believe Moscow played a role in getting the information out.

On Background: We did not speculate on how exactly the Russians played in this particular case because there are so many different possibilities.

Shapiro made sure to update the Biden campaign—specifically, Andrew Bates, Director of Rapid Response—after reaching out to the *Washington Post* and the *Associated Press*, stating, “This is what I gave them.”¹²⁰

¹²⁰ Email from Nick Shapiro to Andrew Bates (Oct. 19, 2020, 11:22 PM) (on file with the Committees).

From: Nick Shapiro [REDACTED]
Sent: 10/19/2020 11:22:24 PM
To: Andrew Bates [REDACTED]
Subject: Fwd: The Letter
Attachments: Former IC Officers Public Statement.docx

This is what I gave them -

Ok - here you go.

Giving this to you exclusively first if you guys want to run with it. Then will give to others once you post.

You can also use this **on the record** from me (Nick Shapiro, Former CIA Deputy Chief of Staff and Senior Advisor to the Director) describing what this is:

"A large group of former career intelligence officers, many specializing in Russia, joined by a group of former intelligence community leaders, are all saying that they believe the Russians were somehow involved here. The IC leaders who have signed this letter worked for the past four Presidents, including Trump. The real power here however is the number of former, working-level IC officers who want the American people to know that once again the Russians are interfering."

Off The Record: We are not making a call on whether the materials are true or not, just that we believe Moscow played a role in getting the information out.

On Background: We did not speculate on how exactly the Russians played in this particular case because there are so many different possibilities.

After apparently not receiving a favorable response from the *Associated Press* reporter, Shapiro later sent the email with the public statement to *Politico* about an hour later.¹²¹ *Politico*, of course, eventually published the story.

¹²¹ Email from Nick Shapiro to Natasha Bertrand (Oct. 20, 2020, 12:27 AM) (on file with the Committees).

From: Nick Shapiro [REDACTED]
Sent: 10/20/2020 12:27:59 AM
To: Natasha Bertrand [REDACTED]
Subject: The Letter
Attachments: Former IC Officers Public Statement.docx

Ok - here you go.

Giving this to you exclusively first. Then will give to others once you post your story.

You can also use this **on the record** from me (Nick Shapiro, Former CIA Deputy Chief of Staff and Senior Advisor to the Director) describing what this is:

"A large group of former career intelligence officers, many specializing in Russia, joined by a group of former intelligence community leaders, are all saying that they believe the Russians were somehow involved here. The IC leaders who have signed this letter worked for the past four Presidents, including Trump. The real power here however is the number of former, working-level IC officers who want the American people to know that once again the Russians are interfering."

Off The Record: We are not making a call on whether the materials are true or not, just that we believe Moscow played a role in getting the information out.

On Background: We did not speculate on how exactly the Russians played in this particular case because there are so many different possibilities.

In his transcribed interview, Shapiro testified about the process of soliciting the statement to the media. He testified:

Q. And we understand from your productions that there were three journalists that you sent the statement to: [REDACTED] of *The Washington Post*, [REDACTED] of the *Associated Press*, and Natasha Bertrand of *Politico*?

A. Yep.

Q. Why those three?

A. [REDACTED] because I was asked to go to [REDACTED] first. And then the *AP* is a really good outlet you want stories in. And then *Politico* – I don't know why I went to *Politico* after that.

Q. We know that Natasha Bertrand is the one that ultimately ran with the article. Why did [REDACTED] and [REDACTED] decline to do so?

A. I don't remember. I know we – I'm sure we spoke. But you'd have to ask them. Reporters decline things all the time.

Q. Okay. But they did get back to you, I assume, over the phone?

A. Yeah.

Q. Because we didn't have any of those records and –

A. Yeah. I looked back at the emails, and it's clear that I spoke to them before I emailed them, which is normal. When I'm talking to a reporter, I'll call them and say, "Hey, you know, I've got this idea. What do you want to do?" And then, considering it was a letter, I'm sure I said, "I'll follow up and send it to you," which is what I did with each of them.

And then, for each of them, we got back on the phone. And *Washington Post* and *AP* said no. And *Politico* I think I probably just reiterated these points to Natasha.¹²²

B. *Politico* ultimately published a story about the statement, falsely calling the Hunter Biden laptop and emails Russian disinformation.

On October 19, 2020, at 10:30 p.m., *Politico* published the public statement it received from Shapiro, with an accompanying article titled: "Hunter Biden story is Russian disinfo, dozens of former intel officials say."¹²³

¹²² Shapiro interview at 20-22.

¹²³ Bertrand, *supra* note 4.

NATIONAL SECURITY

Hunter Biden story is Russian disinfo, dozens of former intel officials say

More than 50 former intelligence officials signed a letter casting doubt on the provenance of a New York Post story on the former vice president's son.



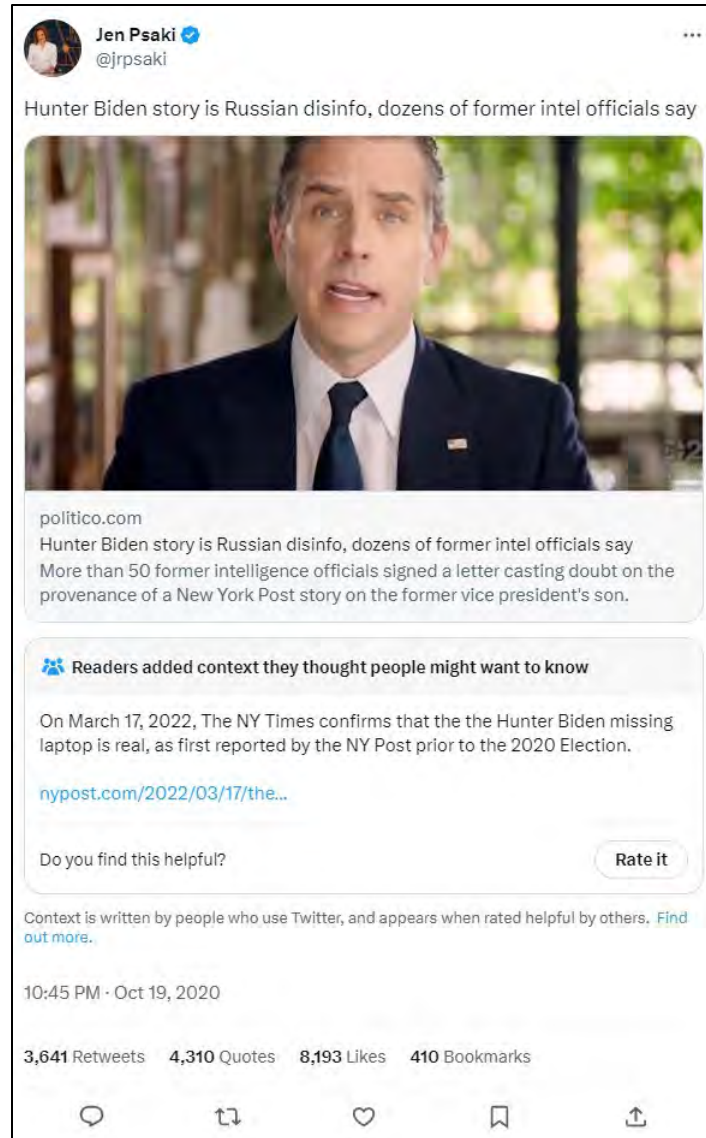
More than 50 former senior intelligence officials have signed on to a letter outlining their belief that the recent disclosure of emails allegedly belonging to Hunter Biden, pictured here, "has all the classic earmarks of a Russian information operation." | Handout/DNCC via Getty Images

By NATASHA BERTRAND
10/19/2020 10:30 PM EDT

Supporters of the Biden campaign immediately promoted the article, including Jen Psaki, who would later become the White House Press Secretary under President Biden.¹²⁴

¹²⁴ Jen Psaki (@jrpsaki), Twitter (Oct. 19, 2020, 10:45 PM), <https://twitter.com/jrpsaki/status/1318382779659411458>.



Despite *Politico*'s conclusory headline, Morell, Polymeropoulos, and Shapiro all testified that their statement was not intended to make a conclusive determination about whether the Hunter Biden allegations were disinformation. Morell testified that “the statement clearly says that we’re not saying this is disinformation.”¹²⁵ Polymeropoulos testified that, at the presidential debate, “Vice President Biden” had “mischaracterize[ed]” the statement by calling “it disinformation, which is not what the letter said.”¹²⁶ And Shapiro testified:

Q How do you feel now that you know that the contents on the laptop were not Russian disinformation?

A Meaning that they were real?

¹²⁵ Morell Interview at 26.

¹²⁶ Polymeropoulos Interview at 28.

Q Yes.

A I'm sure glad that we put that in the letter, saying that we don't know if this is real or not.¹²⁷

Notwithstanding these recent protestations, there is no evidence that the statement's signers attempted to correct *Politico's* misleading headline. Indeed, Morell "knew" the media would not run the letter's caveats. He testified:

Q. Do you regret that those caveats [in the statement] that you seem to be relying on heavily today weren't really part of the public discourse and the political discourse around this letter?

A. I knew they wouldn't be. I knew they wouldn't be, as much as we tried, right? As you guys know better than anybody, right, politics is hyperbole and particularly debates. There's a lot of hyperbole around, a lot of people taking things and taking them a little bit further, right? You know that better than I do. So I wasn't surprised at all that – you know, when President Biden – when Vice President Biden talked about this at the debate that he didn't say, "Hey, I have to put some caveats on this." That's not what happens at debates.

Q. So you knew when you put this product out with caveats that its utilization politically likely wouldn't include those caveats?

A. I guessed that politicians would not use the caveats. I was hoping that fact-checkers and I was hoping the media – disappointed in that regard – would pay more attention to them.

Q. But you testified earlier that you were accelerating – you were requesting an acceleration of the review of this material so it could be used in a debate, right?

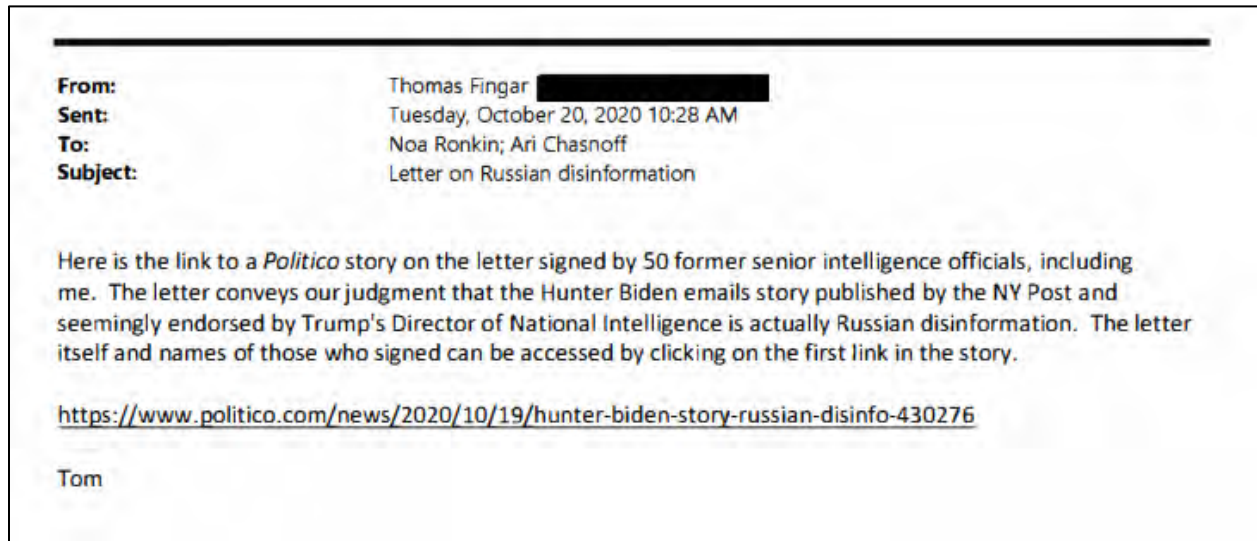
A. Yes, sir.¹²⁸

Indeed, contemporaneous documents show that some of the signatories adopted *Politico's* framing that the laptop was Russian disinformation. One of the intelligence officials who signed onto the statement, Thomas Fingar, the former Deputy Director of National Intelligence for Analysis and Chair of the National Intelligence Council, wrote to colleagues at Stanford University that the statement "conveys our judgment that the Hunter Biden emails story

¹²⁷ Shapiro Interview at 28.

¹²⁸ Morell Interview at 88-89.

published by the NY Post and seemingly endorsed by Trump’s Director of National Intelligence is actually Russian disinformation.”¹²⁹



Fingar, in sharing the *Politico* story with Stanford’s public affairs team, appeared intent on having the university promote the story among its networks.¹³⁰ But Fingar’s Stanford colleagues did not seem willing. One Stanford employee immediately grasped the statement was nothing more than a political document.¹³¹ Indeed, she used the word “political” four times in her terse response to Fingar explaining that Stanford cannot endorse these sorts of “political opinions.”¹³²

¹²⁹ Email from Thomas Fingar to Noa Ronkin and Ari Chasnoff (Oct. 20, 2020, 10:28 AM) (on file with the Committees).

¹³⁰ STANFORD-FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES, All FSI People / Staff, <https://fsi.stanford.edu/people/noa-ronkin-0>; <https://fsi.stanford.edu/people/ari-chasnoff> (last visited May 4, 2023).

¹³¹ Email from Noa Ronkin to Thomas Fingar (Oct. 20, 2020, 1:00 PM) (on file with the Committees).

¹³² *Id.*

From: Noa Ronkin [REDACTED]
Sent: Tuesday, October 20, 2020 1:00 PM
To: Thomas Fingar
Cc: Ari Chasnoff
Subject: Re: Letter on Russian disinformation

Thank you, Tom, but this is something that we are advised not to promote, per the guidelines for political activities the University released last month. While all members of the University community may express their political opinions and engage in political activities in their individual capacities using personal resources, we must avoid even the appearance that they are speaking or acting for the University in political matters.

Thanks for your understanding,
 Noa

Noa Ronkin, DPhil
 Associate Director for Communications and External Relations
 Walter H. Shorenstein Asia-Pacific Research Center (APARC)
 Freeman Spogli Institute for International Studies
 Stanford University
 [REDACTED]
aparc.fsi.stanford.edu | [REDACTED]

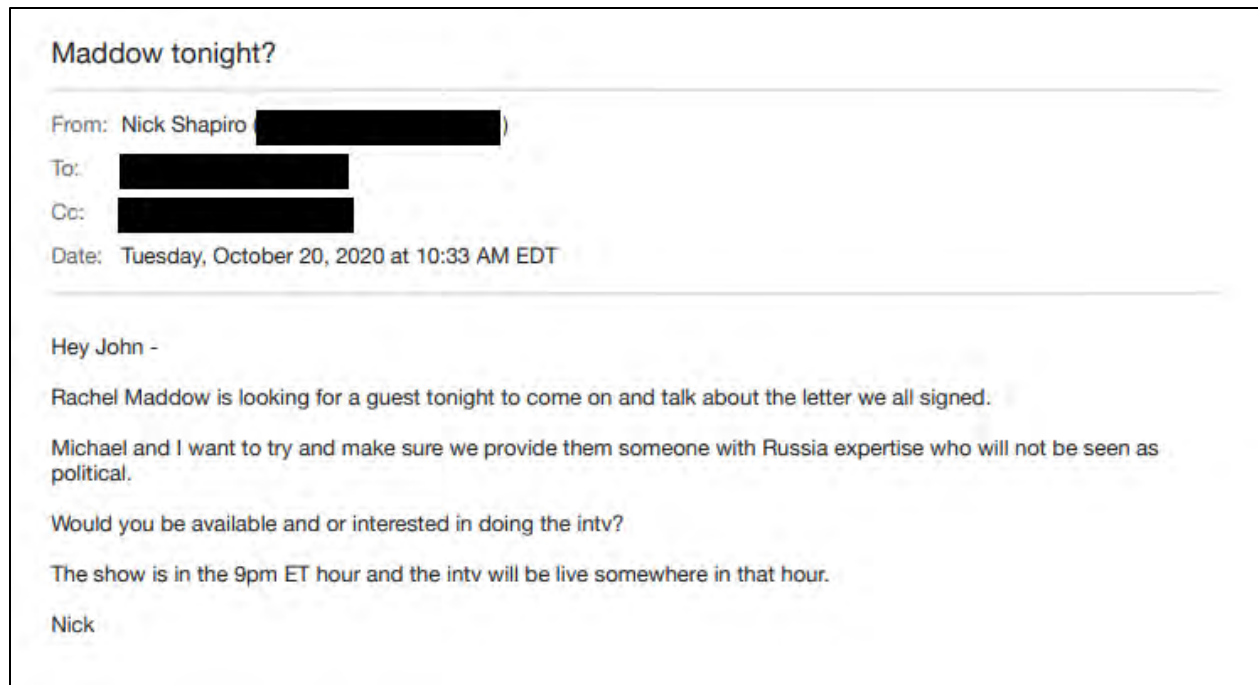
In an October 20 email to the signers of the statement, Morell wrote that “*Politico* did a nice job getting out the story of our letter.”¹³³ Morell, however, expressed no concern about the story’s conclusory headline that the laptop was Russian disinformation.

Similarly, on October 20, a day after *Politico* ran its story about the statement, Shapiro emailed another signatory, John Sipher, a former career CIA officer, to sit for an interview with MSNBC commentator Rachel Maddow.¹³⁴ Shapiro noted an interest in placing a statement signatory before a friendly talk show host and ensuring that signatory had “Russia expertise” and “will not be seen as political.”¹³⁵ Here, too, there was no mention about nuancing *Politico*’s headline or caveating the assertions in the statement.

¹³³ Email from Michael Morell to Unnamed Intelligence Officials (Oct. 20, 2020, 1:40 PM) (on file with Committees).

¹³⁴ Email from Nick Shapiro to John Sipher (Oct. 20, 2020, 10:33 AM) (on file with the Committees).

¹³⁵ *Id.*



Likewise, Jeremy Bash,¹³⁶ another former intelligence community official, appeared on MSNBC the same day the statement was released. His assertions about Hunter Biden’s laptop and emails were unambiguous and did not include nuanced caveats in the statement. He said:

We need to talk about it, Nicole. [The Hunter Biden allegations] looks like Russian intelligence, this walks like Russian intelligence, this talks like Russian intelligence. This effort by Rudy Giuliani and the *New York Post* and Steve Bannon to cook up supposed dirt on Joe Biden looks like a classic Russian playbook disinformation campaign.¹³⁷

¹³⁶ President Biden appointed Bash to the President’s Intelligence Advisory Board in August 2022. White House, *President Biden Announces Key Appointments to Boards and Commissions* (Aug. 26, 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/26/president-biden-announces-key-appointments-to-boards-and-commissions-6/>.

¹³⁷ Nicole Wallace, *Bash On Pushing Of Disinformation On Biden: This Looks, Walks, & Talks Like Russian Intelligence*, MSNBC (Oct. 19, 2020); *see also* Deadline: White House, MSNBC (Oct. 19, 2020).



The MSNBC host then amplified the falsehood: “I think Jeremy has made clear we shouldn’t look at [the statement] as anything other than a Russian disinformation operation.”¹³⁸ If these intelligence officials were concerned about *Politico*’s misrepresentation of their public statement, there has been no contemporaneous indication of such a concern.

C. The *Politico* article and public statement helped to support the continued suppression of the allegations uncovered from emails on Hunter Biden’s laptop.

In a recent retrospective, the *New York Post* explained how the public statement contributed to the continued suppression of the underlying allegations contained in the emails on Hunter Biden’s laptop—namely, Hunter Biden’s pattern of monetizing his familial relationship with Vice President Biden’s likely knowledge. The *Post* piece reasoned:

Yes, that letter from the Dirty 51 had “all the classic earmarks” of a disinformation operation, all right — one designed to ensure Joe Biden won the presidency. And it was essentially a CIA operation, considering 43 of the 51 signatories were former CIA.

In the two years since, not one of them has admitted they are wrong.

¹³⁸ *Id.*

[One signer] David Priess at least gets marks for subjecting himself to a cross-examination on Fox News one recent afternoon. He tried to defend the letter by saying people were too stupid to understand it. The letter was “still true” because it did not use the words “Russian disinformation,” but concocted the weasel phrase “earmarks of a Russian information operation.”

He knows perfectly well that Biden and the media drew no distinction, that the letter he signed was used to censor and deride *The Post*’s accurate story and deny the American people the truth about one of the two candidates for president.¹³⁹

Similarly, an opinion writer with the *Washington Post* observed:

In addition to these meetings with current officials, a group of 51 former intelligence officials released a public letter when the story broke in which they alleged that the release of Hunter Biden’s emails “has all the classic earmarks of a Russian information operation,” adding, “If we are right, this is Russia trying to influence how Americans vote in this election.”

They were not right. But together, these warnings by current and former national security officials gave Twitter the pretext to censor the story — and mainstream news outlets the excuse to dismiss or ignore it, which many of them did.¹⁴⁰

¹³⁹ Miranda Devine, *It’s been two years since 51 intelligence agents interfered with an election — they still won’t apologize*, N.Y. POST (Oct. 19, 2022).

¹⁴⁰ Marc A. Thiessen, *The suppression of Hunter Biden’s laptop is a huge scandal*, THE WASHINGTON POST (Dec. 9, 2022).

IV. The statement had its intended effect of giving Vice President Biden a “talking point” to use in the presidential debate.

The public statement signatories had a common goal: “to help Vice President Biden in the debate” and to help him win the presidency.¹⁴¹ Indeed, some of the former intelligence officials who signed the public statement were deeply satisfied that Vice President Biden referred to the statement in the final presidential debate before the election. After the debate, the signers congratulated themselves on a job well done, and the Biden campaign even called to thank Morell for organizing the effort.

A. Then-Vice President Biden relied on the public statement in the presidential debate to falsely assert that Hunter Biden allegations were a Russian “plan.”

On October 22, 2020, the last debate between then-Vice President Biden and President Trump took place at Belmont University in Nashville, Tennessee.¹⁴² After President Trump pressed Vice President Biden about his son’s laptop and emails, Biden called the American people’s attention to the statement, noting the significance of the intelligence community officials who signed the statement:

President Trump: It’s the laptop from hell.

Moderator: President Trump, we’re talking about race right now and I do want to stay on the issue of race. President Trump –

Vice President Biden: Nobody – Kristen, I have to respond to that.

Moderator: Please, very quickly.

Vice President Biden: Look, there are 50 former national intelligence folks who said that what this, he’s accusing me of is a Russian plan. They have said that this has all the characteristics — four– five former heads of the CIA, both parties, say what he’s saying is a bunch of garbage. Nobody believes it except him and his good friend Rudy Giuliani.

President Trump: You mean, the laptop is now another Russia, Russia, Russia hoax? You gotta be –

Vice President Biden: That’s exactly what — That’s exactly what –

¹⁴¹ Morell Interview at 78, 102.

¹⁴² COMM. ON PRESIDENTIAL DEBATES, *supra* note 5.

President Trump: Is this where you're going? This is where he's going.
The laptop is Russia, Russia, Russia?¹⁴³

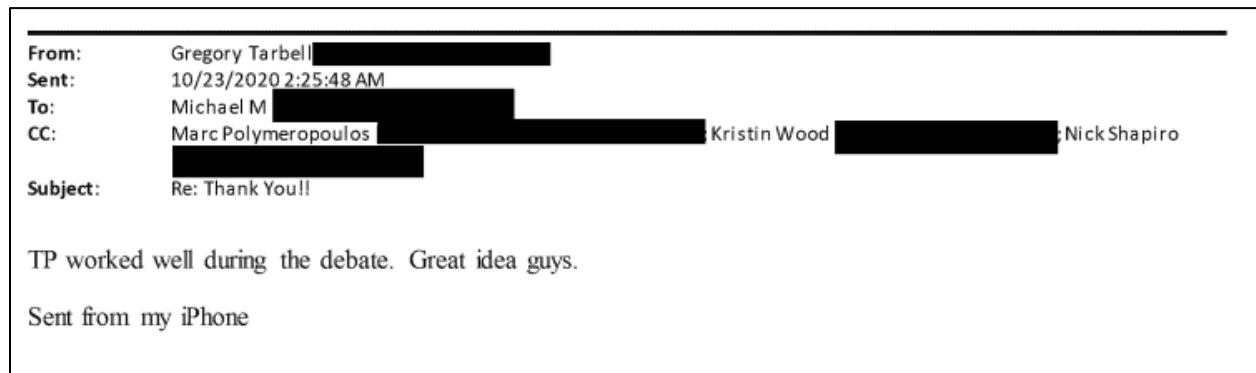
Two days later, the *Washington Post* took note of Vice President Biden's reliance upon the public statement, noting critically:

Joe Biden leaned heavily on a letter from former U.S. intelligence and defense officials in Thursday night's debate to argue that Russia orchestrated a disinformation operation allegedly involving damaging information obtained from his son's laptop that was promulgated by President Trump's personal attorney, Rudolph W. Giuliani.

The Biden campaign's decision to lean into accusations of Russian involvement in the episode, despite lacking specific proof, risks eroding public trust in U.S. allegations of foreign election interference if the suspicions in this case turn out to be unfounded, according to intelligence and foreign policy experts.¹⁴⁴

B. The statement's signatories celebrated after the debate.

The signers of the statement were pleased with Vice President Biden's response and his reliance upon the statement during the debate, as emails between them make clear. One signer, Gregory Tarbell, former CIA Deputy Executive Director, wrote that the talking points "worked well during the debate" and applauded Morell, Polymeropoulos, Wood, Shapiro, and others on what the "[g]reat idea" for the statement.¹⁴⁵

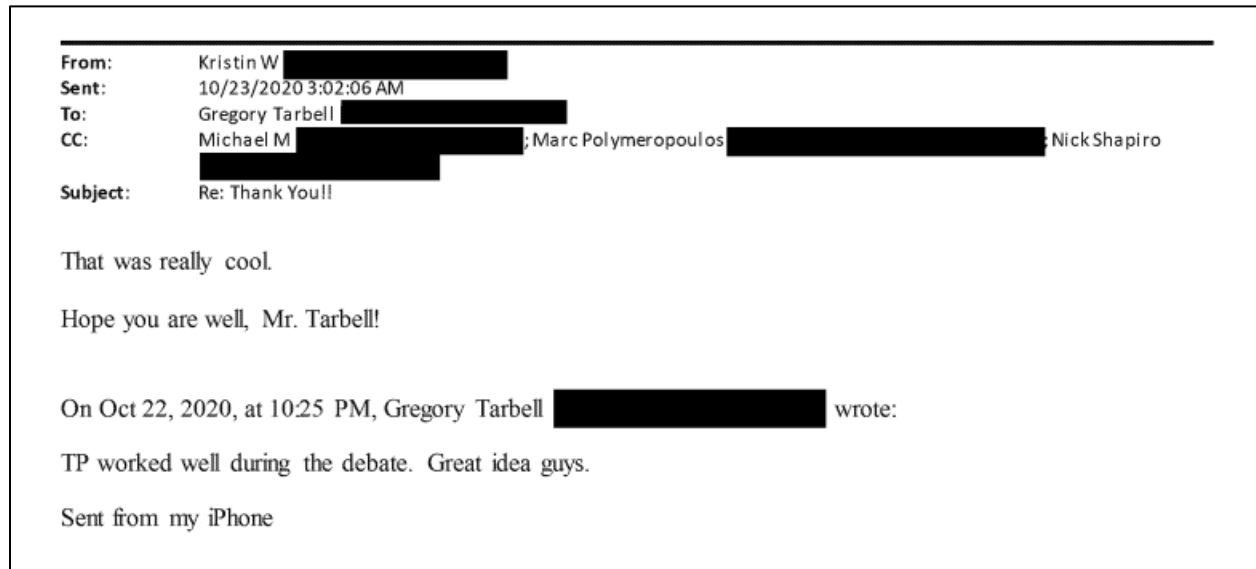


¹⁴³ *Id.*

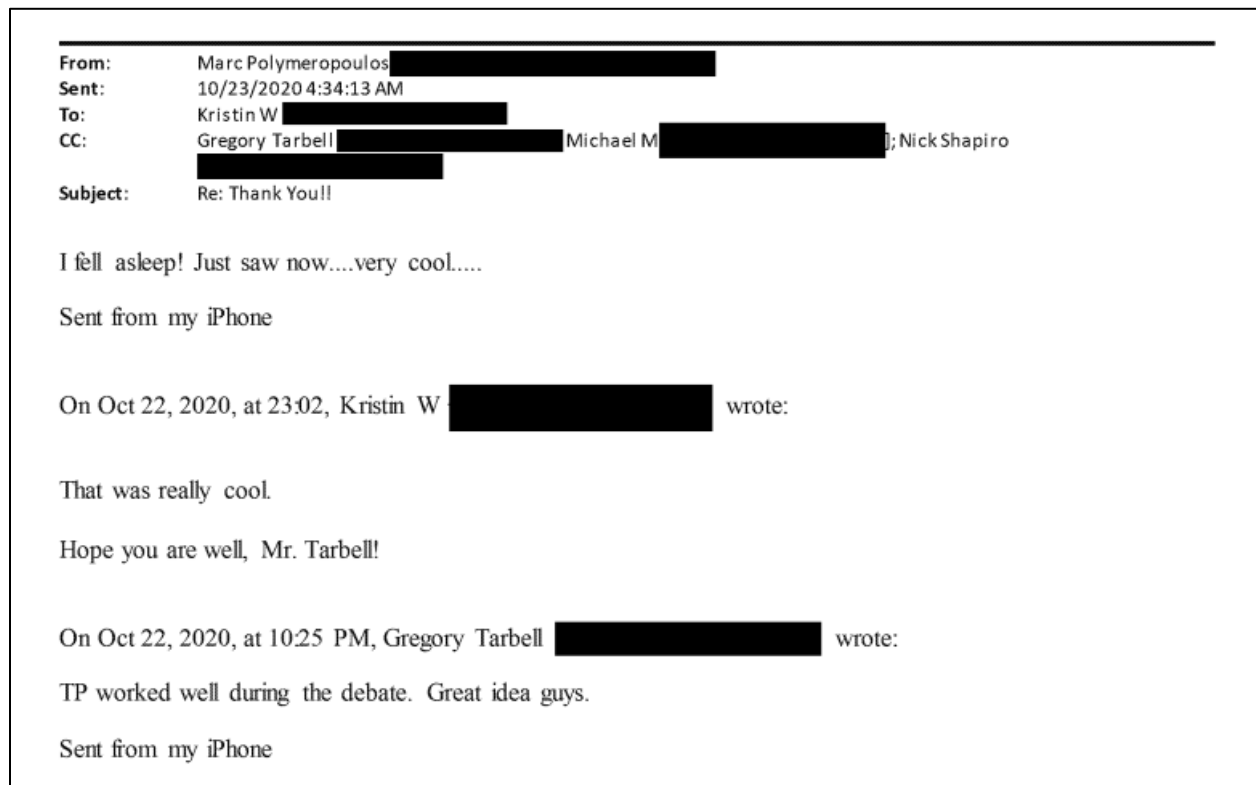
¹⁴⁴ Annie Linskey & Paul Soone, *Biden relies on pattern of activity to blame Russia for release of data from what is said to be his son's laptop*, THE WASHINGTON POST (Oct. 24, 2020).

¹⁴⁵ Email from Gregory Tarbell to Michael Morell (Oct. 23, 2020, 2:25 AM) (on file with the Committees).

In response, Wood stated that Vice President Biden’s mention of the statement during the debate “was really cool.”¹⁴⁶



Polymeropoulos voiced similar sentiments, calling it “very cool.”¹⁴⁷

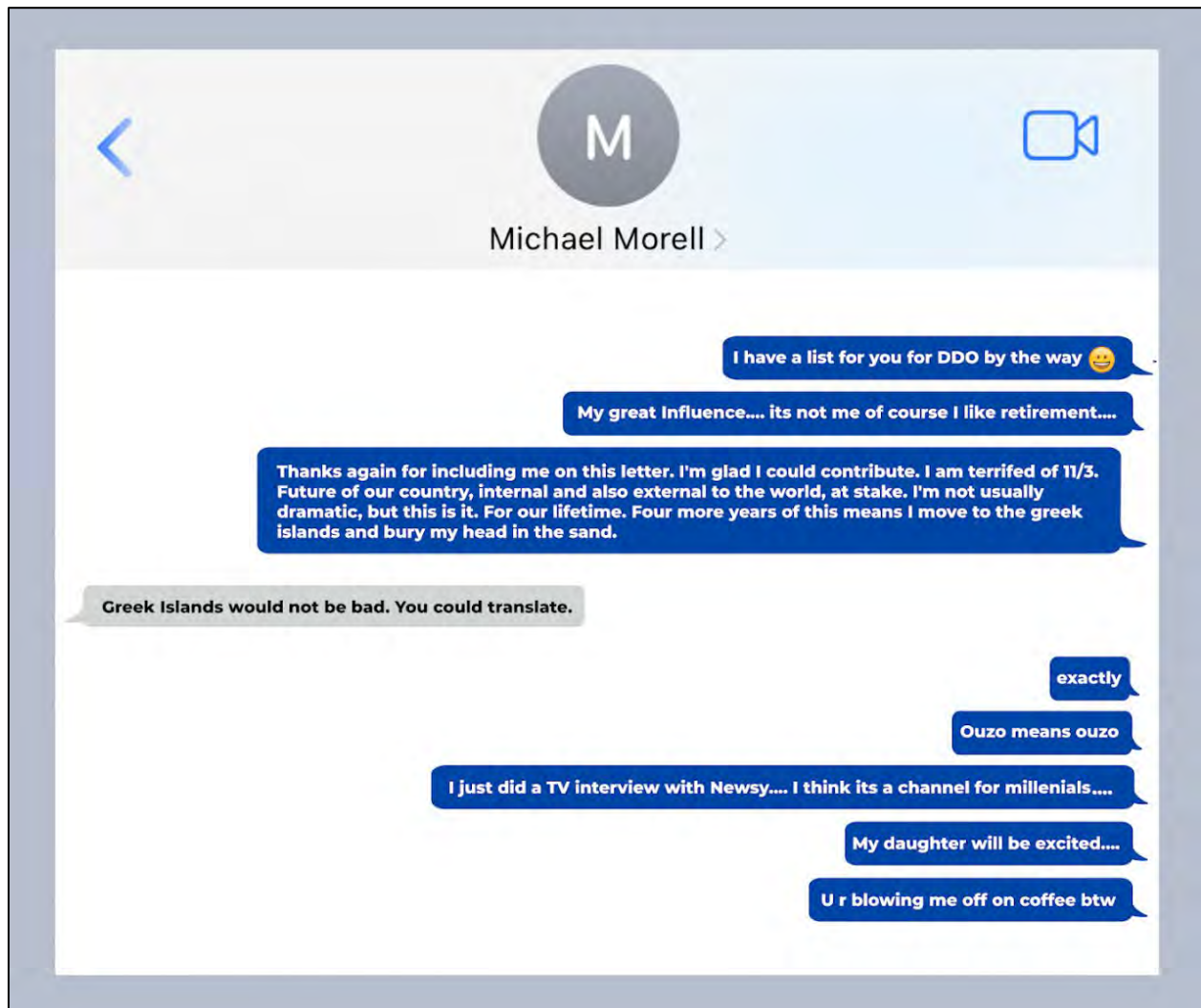


¹⁴⁶ Email from Kristin Wood to Gregory Tarbell (Oct. 23, 2020, 3:02 AM) (on file with the Committees).

¹⁴⁷ Email from Marc Polymeropoulos to Kristin Wood (Oct. 23, 2020, 4:34 AM) (on file with the Committees).

Four day earlier, in a private exchange with Morell, Polymeropoulos expressed his appreciation for “including me on this letter.” He wrote:

Thanks again for including me on this letter. I’m glad I could contribute. I am terrified of 11/3. Future of our country, internal and also external to the world, at stake. I’m not usually dramatic, but this is it. For our lifetimes. Four more years of this means I move to the greek [sic] islands and bury my head in the sand.¹⁴⁸



Text message between Michael Morell and Marc Polymeropoulos (Oct. 19, 2020)

Morell testified to the self-satisfaction the signatories felt for their involvement in the presidential debate. He testified:

Q. And then we also have a number of emails that have been produced

¹⁴⁸ Text message from Marc Polymeropoulos to Michael Morell (Oct. 19, 2020, 5:51 PM) (on file with the Committees).

to the committee where the people on – a number of the people who signed it were sort of congratulating each other for the fact that it was, in fact, used in the debate.

A. Yes, sir.¹⁴⁹

In a final email to the signatories, Morell expressed his own satisfaction in successfully getting the statement published. He wrote to his co-signatories:

I think this is the most important election since 1860 and 1864 when the very existence of the country was on the ballot. Now, it is our democracy and the Constitution that are on the ballot. We all, of course, took an oath to “preserve, protect, and defend” the Constitution. I think all of you did that yesterday by signing this letter.¹⁵⁰

¹⁴⁹ Morell Interview at 99.

¹⁵⁰ Email from Michael Morell to Unnamed Intelligence Officials (Oct. 20, 2020, 1:40 PM) (on file with the Committees).

From: Michael M [REDACTED]
Sent: Tuesday, October 20, 2020 9:40 AM
To: Michael M
Cc: Marc Polymeropoulos; Kristin Wood; Nick Shapiro
Subject: Thank You!!

To all,

[I put most everyone on the bcc line to protect email addresses]

I just want to thank everyone for signing the letter on the Hunter Biden emails. We ended up with over 50 signatories.

Politico did a nice job getting out the story of our letter. Here is a link to the article for those who have not seen it. <https://www.politico.com/news/2020/10/19/hunter-biden-story-russian-disinfo-430276>

We will monitor how much media coverage it gets and will let you know.

I also want to thank Marc for helping to draft the letter, Kristin for helping to spread the word, and Nick for working with the media.

By the way, if any reporters reach out to you, feel free to either talk to them or to send them Nick's way. Nick has the final version of the letter, if any reporters are looking for that (although there is a link to the letter itself in the Politico piece).

I think this is the most important election since 1860 and 1864 when the very existence of the country was on the ballot. Now, it is our democracy and the Constitution that are on the ballot. We all, of course, took an oath to "preserve, protect, and defend" the Constitution. I think all of you did that yesterday by signing the letter. Thank you.

Michael

C. The Biden campaign called Morell and thanked him for his service to the campaign.

After the October 22, 2020, presidential debate, Biden campaign chairman Steve Ricchetti called Morell and thanked him for the statement. Morell testified:

Q. Did you talk to [Steve Ricchetti] at all regarding the statement that you helped organize and put out?

A. Yes, sir.

Q. When did you talk with him?

A. After the debate – I think it was after the debate – in fact, I'm pretty sure it was after the debate – I got a phone call from Jeremy Bash, who I work with at Beacon and who is active politically. And Jeremy said: Do you have a minute to talk to Steve Ricchetti? I said: Of course. He was the head of the Biden campaign at the time. And

Jeremy got him on the line, and Steve thanked me for putting the statement out.¹⁵¹

¹⁵¹ Morell Interview at 96-97.

V. Some signatories expressed outrage about Congressional oversight into the origins of the statement.

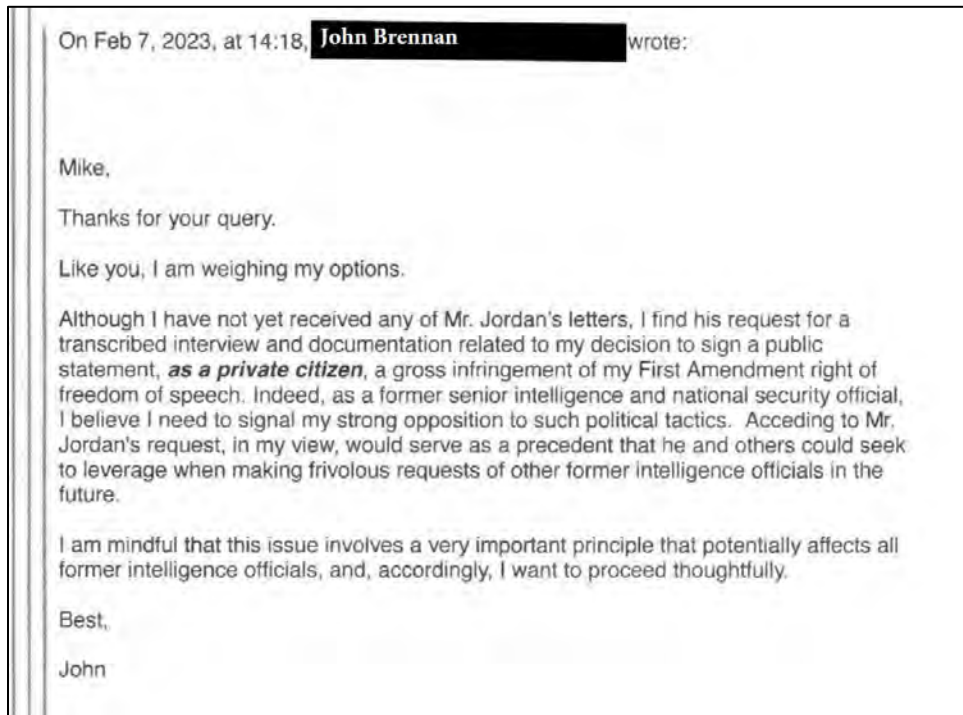
The Committees are in possession of emails exchanged among some of the senior former intelligence officials following the Committees’ oversight requests regarding the origins of the statement. While the Committees fully recognize and respect every Americans’ right to engage in the political process, the Committees have a legitimate legislative purpose in understanding how these officials used their intelligence credentials and official titles to mislead American voters about serious Biden family allegations in the final days before the 2020 election.

The emails exchanged following the Committees’ oversight suggest outrage among some signatories for having to explain the origins of the statement. Former National Security Agency Director Michael Hayden asked some co-signers—including Morell, John Brennan, Jeremy Bash, Thomas Fingar, and others—if they “should have a coordinated response.”¹⁵² Brennan responded that he would voice his “strong opposition to such political tactics,” asserting that complying with the Committees’ request for documents and testimony “would serve as a precedent that [Chairman Jordan] and others could seek to leverage when making frivolous requests of other former intelligence officials in the future.”¹⁵³

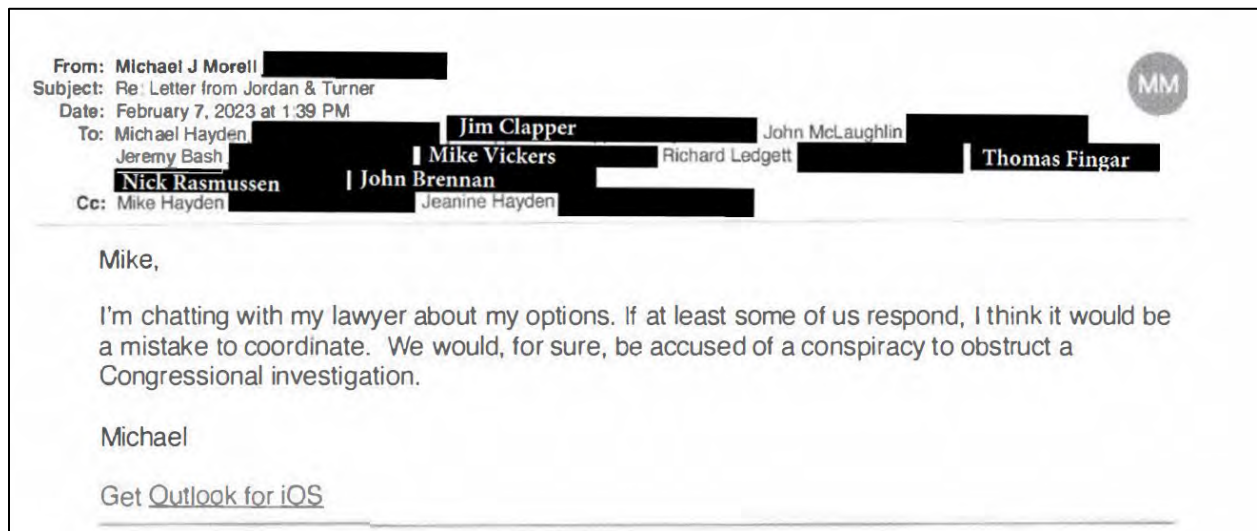


¹⁵² Email from Michael Hayden to Jim Clapper et al. (Feb. 7, 2023, 1:11 PM) (on file with the Committees).

¹⁵³ Email from John Brennan to Michael Hayden (Feb. 7, 2023, 2:18 PM) (on file with the Committees).



Morell, to his credit, rejected Hayden's suggestion to coordinate a response, counseling his former colleagues: "If at least some of us respond, I think it would be a mistake to coordinate. We would, for sure, be accused of a conspiracy to obstruct a Congressional investigation."¹⁵⁴



¹⁵⁴ Email from Michael Morell to Michael Hayden et al. (Feb. 7, 2023, 1:39 PM) (on file with the Committees).

Conclusion

The American people deserve to know that Hunter Biden’s laptop and emails were real. They always were real. The allegations that they were the product of Russian disinformation were false. Even the *New York Times* was forced to acknowledge, almost two years after the 2020 election, “a cache of files that appears to have come from a laptop abandoned by [Hunter] Biden in a Delaware repair shop” was “authenticated by people familiar with them and with the investigation.”¹⁵⁵

On the morning of October 19, 2020, at least 12 hours before the statement was released by *Politico*, then-Director Ratcliffe publicly stated, on behalf of the intelligence community, that Hunter Biden’s laptop and emails were not Russian disinformation.¹⁵⁶ Within 24 hours of then-Director Ratcliffe’s statement, the Department of Justice and the FBI confirmed his declaration.¹⁵⁷

Reflecting on that moment, former-Director Ratcliffe recently stated:

You had the intelligence community and the law enforcement community on behalf of the United States of America saying this is not Russian disinformation. . . . You have literally had the Bidens lie about it—Hunter Biden, Joe Biden, the Biden administration, Biden White House officials, the Democratic Party, Democratic politicians, the left-leaning media. . .

The gaggle of former intelligence and law enforcement officials—you know—the famous 51 All of this was really a domestic disinformation campaign for political reasons. . . . There is no other explanation for it.

The people that had access to the intelligence and had possession of Hunter Biden’s laptop . . . all of the people in a position to talk about the evidence and the intelligence told the American people the truth.¹⁵⁸

As the *Wall Street Journal* opined, the American people will “never know what effect the ‘October Surprise’ of 2020, the *New York Post*’s reporting of the discovery of a laptop belonging to Hunter Biden containing all sorts of embarrassing emails, might have had on the election that year if it had received wider circulation.”¹⁵⁹ Former Attorney General William Barr

¹⁵⁵ Katie Benner et al., *Hunter Biden Paid Tax Bill, but Broad Federal Investigation Continues*, N.Y. TIMES (Mar. 16, 2022).

¹⁵⁶ Moore, *supra* note 87.

¹⁵⁷ Perez, *supra* note 91.

¹⁵⁸ Brooke Singman, *Ratcliffe: Hunter Biden laptop was a partisan domestic 'disinformation campaign'*, FOX NEWS (Feb. 2, 2023).

¹⁵⁹ Gerard Baker, *Hunter Biden’s Laptop and America’s Crisis of Accountability*, WALL ST. J. (Mar. 21, 2022).

believes the suppression of the Hunter Biden laptop story “probably affected the outcome” of the 2020 election, “given how close the election was.”¹⁶⁰

On November 3, 2020, the American people went to the polls to elect the president of the United States with the false impression that Hunter Biden’s laptop was Russian disinformation. The American people cannot get back the 2020 election, but they have every right to demand reforms from Congress so that the 2024 election will not be similarly compromised.

The United States is witnessing in real time the growth of a censorship industrial complex, in which partisan “experts”—like the former intelligence officials who signed the statement—reserve for themselves the right to determine what is and is not true and what Americans can and cannot hear. Indeed, in the weeks leading up to the 2020 election, a writer for the *New York Times* observed that, in the United States, “[f]ree speech threatens democracy as much as it also provides for its flourishing.”¹⁶¹ To address this threat, progressive “experts prescribe[] two critical steps: [1] America must become less free and [2] less democratic. . . .”¹⁶² These goals, in their view, will only be achieved by “following the wisdom of disinformation experts and outgrowing our parochial attachment to the Bill of Rights.”¹⁶³ This is frightening and shows why the Committees’ oversight is so important.

There is a direct line between Twitter’s continued suppression of the *New York Post* story on Hunter Biden’s laptop and the statement by the former intelligence officials. One disinformation commentator captured the significance of the censorship of the Hunter Biden laptop and emails story to American democracy and self-government:

The laptops are real. The FBI has known this since 2019, when it first took possession of them. When the *New York Post* attempted to report on them, dozens of the most senior national security officials in the United States lied to the public, claiming the laptops were likely part of a Russian “disinformation” plot. Twitter, Facebook, and Google, operating as fully integrated branches of the state security infrastructure, carried out the government’s censorship orders based on that lie. The press swallowed the lie and cheered on the censorship.

The story of the laptops has been framed as many things, but the most fundamental truth about it is that it was the successful culmination of the yearslong effort to create a shadow regulatory bureaucracy built specifically to prevent a repeat of Trump’s 2016 victory.

¹⁶⁰ Jerry Dunleavy, *Barr says Hunter Biden Russian disinformation claims ‘probably affected’ election outcome*, WASHINGTON EXAMINER (Mar. 22, 2022).

¹⁶¹ Emily Bazelon, *The Problem of Free Speech in an Age of Disinformation*, N.Y. TIMES (Oct. 13, 2020) (internal quotations marks and citation omitted).

¹⁶² Jacob Siegel, *A Guide to Understanding the Hoax of the Century*, TABLET (Mar. 28, 2023).

¹⁶³ *Id.*

It may be impossible to know exactly what effect the ban on reporting about Hunter Biden's laptops had on the 2020 vote, but the story was clearly seen as threatening enough to warrant an openly authoritarian attack on the independence of the press. The damage to the country's underlying social fabric, in which paranoia and conspiracy have been normalized, is incalculable.¹⁶⁴

This interim report presents the material facts the Committees have learned to date about the origins of the public statement signed by 51 former intelligence officials that falsely discredited—on the eve of the 2020 presidential election—legitimate allegations about the Biden family's influence-peddling operation. The Committees present this information now to keep the House of Representatives apprised of our oversight work. The Committees' oversight into this matter continues in earnest.

¹⁶⁴ *Id.*



**THE INTELLIGENCE COMMUNITY 51: HOW CIA CONTRACTORS
COLLUDED WITH THE BIDEN CAMPAIGN TO MISLEAD AMERICAN
VOTERS**

Second Interim Joint Staff Report of the

Committee on the Judiciary,
Select Subcommittee on the Weaponization
of the Federal Government, and
Permanent Select Committee on Intelligence

U.S. House of Representatives



June 25, 2024

Executive Summary

The Committee on the Judiciary, its Select Subcommittee on the Weaponization of the Federal Government, and the Permanent Select Committee on Intelligence have revealed how, in the final weeks before the 2020 presidential election, 51 former intelligence officials coordinated with the Biden campaign to discredit serious allegations about Biden family influence peddling.¹ In issuing a public statement using their official titles, these former intelligence officials sought to cast an explosive *New York Post* story and Hunter Biden’s abandoned laptop as “Russian disinformation.”² President Biden even cited to the statement in a televised debate with President Trump shortly before the election to accuse President Trump of leveling false accusations.³ As a result, the explosive allegations about Biden family misconduct were buried and millions of Americans cast their votes for president without a full set of facts.

The 51 former intelligence officials’ Hunter Biden statement was a blatant political operation from the start. It originated with a call from top Biden campaign official—and now Secretary of State—Antony Blinken to former Deputy Central Intelligence Agency (CIA) Director Michael Morell. The Committees’ investigation revealed that without this outreach from Blinken, Morell would not have written the statement.⁴ Indeed, Morell told the Committees that the Blinken phone call “triggered” his intent to write the statement.⁵ The statement’s drafters were open about the goal of the project: “[W]e think Trump will attack Biden on the issue at this week’s debate”⁶ and “we want to give the [Vice President] a talking point to use in response.”⁷

The details as revealed by the Committees to date are concerning enough, but as the Committees have continued to investigate the origins of the Hunter Biden statement, new information has come to light. Through newly obtained internal CIA emails and testimonial evidence, the Committees have uncovered more information on the extent to which the intelligence community was involved in the statement. Specifically, the evidence shows:

¹ STAFF OF H. COMM. ON THE JUDICIARY, ET AL., 118TH CONG., REP. ON THE HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS (2023); see also Jim Clapper et al., *Public Statement on the Hunter Biden Emails* (Oct. 19, 2020).

² See Natasha Bertrand, *Hunter Biden story is Russian disinfo, dozens of former intel officials say*, POLITICO (Oct. 19, 2020).

³ COMM. ON PRESIDENTIAL DEBATES, Presidential Debate at Belmont University in Nashville, Tennessee, October 22, 2020, Participants: Former Vice President Joe Biden (D) and President Donald Trump (R), <https://www.debates.org/voter-education/debate-transcripts/october-22-2020-debate-transcript/> (“[T]here are 50 former national intelligence folks who said that what this, he’s accusing me of is a Russian plan. They have said this has all the characteristics—four- five former heads of the CIA, both parties, say what he’s saying is a bunch of garbage.”).

⁴ Transcribed Interview of Mr. Michael Morell at 21-22 (Apr. 4, 2023) (hereinafter “Morell Interview”).

⁵ *Id.*

⁶ Email from Kristin Wood to Unnamed Intelligence Officials (Oct. 19, 2020, 7:27 AM) (on file with the Committees).

⁷ Email from Michael Morell to Michael Morell, Marc Polymeropoulos, and Bcc’d Recipients (Oct. 18, 2020, 4:48 PM) (on file with the Committees).

- **High ranking CIA officials, up to and including then-CIA Director Gina Haspel, were made aware of the Hunter Biden statement prior to its approval and publication.**⁸ Because several former senior intelligence officials signed the statement, the PCRB sent the draft statement to the CIA’s then-Chief Operating Officer (COO) Andrew Makridis, who said he subsequently informed then-Director Haspel or then-Deputy Director Vaughn Frederick Bishop that the statement would be published soon.⁹ Senior CIA leadership had an opportunity at that time to slow down the CIA’s process for reviewing publication submissions and ensure that such an extraordinary statement was properly vetted.¹⁰
- **Some of the statement’s signatories, including Michael Morell, were on active contract with the CIA at the time of the Hunter Biden statement’s publication.**¹¹ Throughout the course of the Committees’ investigation, the signatories claimed to not have had access to any classified information when asserting that the allegations surrounding Hunter Biden’s laptop had “all the hallmarks” of Russian disinformation.¹² However, at the time of the statement’s publication, at least two signatories—Morell and former CIA Inspector General David Buckley—were on the CIA’s payroll as contractors. Due to purported operational concerns, the CIA declined to declassify the entire universe of signatories who were on active contract. In addition, some signatories to the Hunter Biden statement also had special “Green Card” access to the CIA at the time of the statement’s publication, allowing them to gain entry to secure CIA facilities.
- **After publication of the Hunter Biden statement, CIA employees internally expressed concern about the statement’s politicized content, acknowledging it was not “helpful to the Agency in the long run.”**¹³ At least one employee found it “[i]nteresting to see what was submitted and approved” when discussing media talking points that the statement’s co-author, former Senior Intelligence Service Officer Marc Polymeropoulos, submitted related to the statement.¹⁴ When discussing Polymeropoulos’s talking points, another CIA official stated, “It appears [Polymeropoulos] is actively involved in a pro-Biden campaign and may be disclosing classified information in his

⁸ See Transcribed Interview of Andrew Makridis at 13-16 (Apr. 10, 2024) (hereinafter “Makridis Interview”).

⁹ *Id.*

¹⁰ *Id.* at 14-15 (“It would come up to my office, at least initially, for a heads-up, a situational awareness kind of thing. . . . The general rule of thumb or the general procedure was anything written by a former senior, I would alert the director or the deputy director, depending on the day and who was available, and then the process would move forward. . . . I would have stepped across the hall and said, here’s an article. It’s come from the Prepublication Classification Review Board. They said there is no classified in it. It’s going to run.”).

¹¹ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 11:05 AM) (Bates CIA000157) (“I also love that at least a few of the random signatures belong to individuals currently working here on contracts. . .”).

¹² See Clapper, et al., *supra* note 1 (“We want to emphasize that we do not know if the emails . . . are genuine or not and that we do not have evidence of Russian involvement[.] . . . There are a number of factors that make us suspicious of Russian involvement.”).

¹³ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 11:05 AM) (Bates CIA000157) (on file with the Committees).

¹⁴ See Email from [Redacted], Branch Chief of Nontraditional Intelligence Threats, CIA to CIMC_RAD_NITB, CIA (Oct. 20, 2020, 10:11 AM) (Bates CIA-000232).

efforts.”¹⁵ The CIA’s internal review board, known as the Prepublication Classification Review Board (PCRB), determined that Polymeropoulos’s talking points contained classified information that had to be removed prior to publication.¹⁶

The new information included in this report, based on new testimony and declassified documents, shows the potential dangers of a politicized intelligence community. In the waning days before the 2020 presidential election, 51 intelligence community officials rushed to draft and release a statement using their official titles, presumably to convey access to specialized information unavailable to other Americans. The statement was conceived following a conversation with a senior Biden campaign official and designed explicitly to provide talking points to the Biden campaign to discredit politically damaging allegations. Some of the signatories of the statement were on the CIA payroll at the time as contractors and others had special access to CIA facilities. Even Michael Morell—before the Committees learned of his contract with the CIA—acknowledged, “It’s inappropriate for a currently serving staff officer or contractor to be involved in the political process.”¹⁷

The infamous Hunter Biden statement had all the hallmarks of an intelligence community influence operation. But rather than carrying it out against our adversaries on foreign soil, this operation was directed at the American people and our democratic processes. It is impossible to know for certain how events would have played out differently if these 51 intelligence community officials never sought to influence the 2020 election. All the Committees may do now is present the facts as known to inform legislative reforms to protect our democratic ideals and prevent future abuse of the intelligence community for partisan political benefit.

¹⁵ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 10:45 AM) (Bates CIA000178) (on file with the Committees).

¹⁶ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 9:49 AM) (Bates CIA-000233) (on file with the Committees) (“PCRB has determined the manuscript contains classified information, the removal of which would enable publication.”).

¹⁷ Morell Interview at 31.

Table of Contents

Executive Summary	1
Table of Contents	4
I. The CIA, at its highest levels, was aware of the Hunter Biden statement prior to its approval and publication.	5
A. Then-CIA Director Haspel instituted a review process ensuring she would have seen the Hunter Biden statement prior to its approval.	5
B. The CIA alerted the Office of the Director of National Intelligence about the draft of the Hunter Biden statement.	8
C. The CIA’s Office of Chief Operating Officer informed the PCRB that it could approve the Hunter Biden statement.	10
II. Some of the signatories of the Hunter Biden statement were on active CIA contracts at the time of the statement.	14
A. The signatories of the Hunter Biden statement claimed to not access classified information in the course of drafting the statement.	14
B. Several signatories of the Hunter Biden statement had active contracts with the CIA on the statement’s publication date.	16
III. Officials inside the CIA recognized that the Hunter Biden statement was political.	21
Conclusion	30

I. The CIA, at its highest levels, was aware of the Hunter Biden statement prior to its approval and publication.

The drafters of the public statement about Hunter Biden’s laptop have long maintained that the CIA had no part in the approval of the statement beyond confirming that the statement contained no classified information.¹⁸ Evidence obtained by the Committees shows, however, that both then-Director Gina Haspel or then-Deputy Director Vaughn Frederick Bishop were made aware of the statement prior to its publication.¹⁹ Their awareness came via the PCRB, the internal CIA office responsible for reviewing and clearing publications by intelligence community officials.²⁰ Although the PCRB routinely reviews a manuscript without elevating it, in this case, the PCRB took the unique step of alerting the CIA’s Office of the Chief Operating Officer (COO) about the draft statement.²¹ The Office of the COO later directed the PCRB that it may “notify” Morell that the PCRB approved the statement.²²

A. Then-CIA Director Haspel instituted a review process ensuring she would have seen the Hunter Biden statement prior to its approval.

According to testimony from then-CIA COO Andrew Makridis, Director Haspel instituted a policy requiring the PCRB to flag for her review all submissions from current and former senior CIA officials prior to the PCRB’s final approval.²³ Director Haspel did so after several former intelligence officials penned publications that garnered significant news coverage without her awareness.²⁴ Under Director Haspel’s policy, Makridis explained, the PCRB would send documents submitted by current and former senior intelligence officers to the COO’s office and Makridis would personally bring the document to the Director or Deputy Director for review.²⁵ Consequently, when Morell submitted the draft of the Hunter Biden statement in the early hours of October 19, 2020, it followed this same track, albeit on an apparently expedited process. In his initial submission to the PCRB, Morell described the statement as a “rush job,” and the PCRB appeared to acquiesce to his sense of urgency.²⁶

¹⁸ See, e.g., Morell Interview at 28.

¹⁹ See Makridis Interview at 13-14 (“So the process that the Agency operated under, the director of CIA at the time, Gina Haspel, was concerned sometimes that things would appear in the press that she was not aware of. And so she asked for articles that went through the Prepublication Classification Review Board. . . . The general rule of thumb or the general procedure was anything written by a former senior, I would alert the director or the deputy director, depending on the day and who was available, and then the process would move forward.”).

²⁰ Makridis Interview at 12-14.

²¹ See Makridis Interview at 14 (“[B]ook manuscripts, things like that typically didn’t come up.”).

²² See Email from Executive Assistant, Office of the Chief Operating Officer, to [Redacted] DIR_COO_EAS; DDI-EA; DDI_ADO_EAs; DIR_OPA_FO; DDI3; [Redacted] (Oct. 19, 2020, 11:43 AM) (Bates CIA-000230) (on file with the Committees).

²³ Makridis Interview at 13-15.

²⁴ *Id.*

²⁵ *Id.*

²⁶ Email from Michael Morell to PCRB Staff (Oct. 19, 2020, 6:36 AM) (on file with the Committees).

From: Michael M
 To: [REDACTED]
 Cc: Marc Polymeropoulos
 Subject: [AIN] Public Statement for Review - [Link to Attachment(s)]
 Date: Monday, October 19, 2020 6:36:21 AM
 Attachments: Public Statement converted.pdf
 Public Statement converted.docx

CLASSIFICATION: UNCLASSIFIED

AIN EMAIL

This email originated on the AIN (U) and has been forwarded to the Agency Data Network (TS/SCI). *This is only a copy of the original message.* This email has been virus scanned, and the message body has been converted to text-only format. If the message is from someone unfamiliar to you (especially if it contains an attachment) do NOT open it; instead, contact your ISSM (<http://security.cia/infosec/programs/issm>). The original message in its original format can be viewed in your AIN email inbox. Questions can be emailed to GLIDE_HELP.

[ANTE Up Info](#) [GLIDE File Security](#)

Message ID: 667199641/glide-ain-ecds-ap01-low-ain-adn-anteup

Good morning. Hope everyone had a nice weekend. Attached is a statement that Marc and I drafted that many former senior and working-level officials from across the IC will sign and then be made public. We are 100 percent confident it does not contain classified information. Indeed, it specifically says we don't know what the IC or the FBI knows about this.

This is a rush job, as it needs to get out as soon as possible. Thank you very much.
 Michael Morell

&* ORIGINAL EMAIL ATTACHMENTS HAVE BEEN QUARANTINED ***

The following original attachment(s) are awaiting your approval:

- Public Statement.docx

If you trust the sender, click the following to have your message and original attachments resent to you:

Quarantine link ---> <https://glide.cia/glide/Quarantine/Quarantine.html?id=913489705>

These attachment(s) will be available for retrieval for 14 days (Mon Nov 02 06:36:07 EST 2020). For additional information regarding the attachment removal (quarantine) function, please visit the following site: <https://confluence.devops.cia.ic.gov/display/ECDSUP/ANTE+Up+Overview>.

HJC_2-23 0001

This is a rush job, as it needs to get out as soon as possible.

The PCRB staff acknowledged receipt of the Hunter Biden statement in less than 40 minutes,²⁷ and at 8:01 AM, the PCRB sent the statement to the COO's office, marking the submission as of high importance.²⁸ After receiving the notification from the PCRB—and in accordance with Director Haspel's policy—Makridis walked the statement to the CIA Director's

²⁷ Email from PCRB Staff to Michael Morell (Oct. 19, 2020, 7:11 AM) (on file with the Committees).

²⁸ See Email from [Redacted] to DIR_COO_EAS, et al. (Oct. 19, 2020, 8:01 AM) (Bates CIA-000230 - CIA-000231) (on file with the Committees).

or Deputy Director's office to flag it for their awareness.²⁹ Makridis testified during his transcribed interview:

Q. So then after you determined that the article that you received was written by a former senior official, then you would alert either the director and deputy director. Is that correct?

A. Correct.

Q. And what did that process look like? Was that just, hey, heads-up, this is coming? Was there a conversation? How did that typically look?

A. So the typical process was . . . once I saw it and sort of saw that it was from a former senior, I would bring it to the attention of either the director or deputy director. It would depend on the day, who was available.

* * *

Q. And how did it work in this case with the statement?

A. You know, I don't recall exactly, but the process that I just described is probably . . . the way it worked. I would have stepped across the hall and said, here's an article. It's come up from the Prepublication Classification Review Board. They said there is no classified [information] in it. It's going to run. . . .

Q. And since this statement was being signed by Director Brennan, Director Clapper, Director Panetta, Director Morell, do you know if you flagged this for the awareness of the director or deputy director?

A. They would have seen—you know, if I provided them a copy, which is probably the—which is my normal process, they would have seen . . . who the authors were.³⁰

The Hunter Biden statement drew significant attention at the CIA senior staff level. Makridis, as COO, was the third highest-ranking official at the CIA, with over 37-years of

²⁹ Makridis Interview at 15.

³⁰ Makridis Interview at 15-16.

experience at the Agency.³¹ In his testimony before the Committees, Makridis stated that he had never seen a statement of this nature come across his desk before. Makridis testified:

Q. Have you seen anything like the public statement in all of your years of experience?

A. Like? You mean with that many . . .

Q. . . . [W]ith that many signatories, of that caliber, who had all held prestigious positions within the Intelligence Community, especially in the CIA, people you knew personally.

A. No, I had not seen anything of that nature.³²

Despite acknowledging the extraordinary nature of the Hunter Biden statement, none of the top three CIA officials paused the statement's review process within the CIA or seemed to raise any concerns about the statement or its effect on the Agency's credibility.

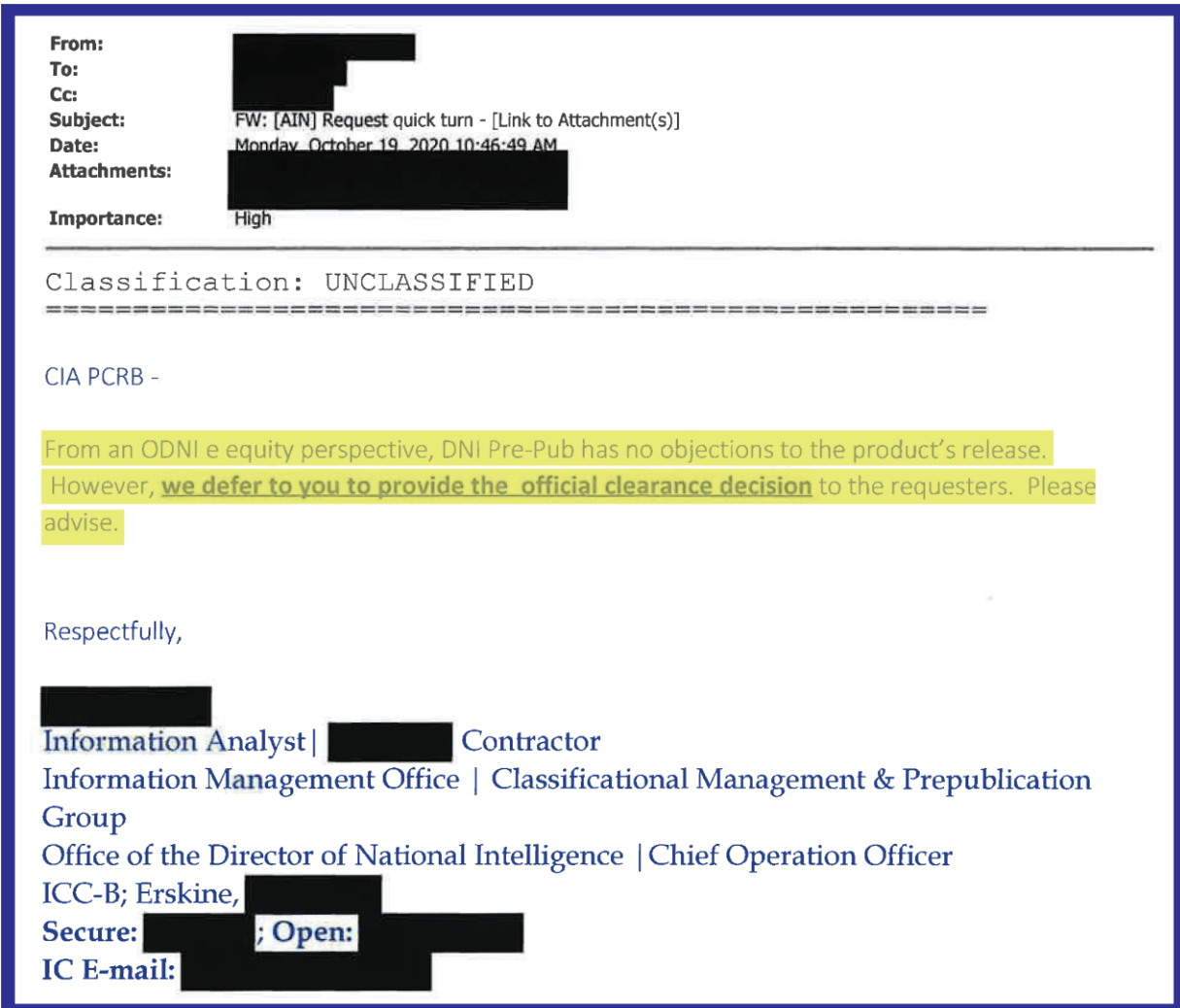
B. The CIA alerted the Office of the Director of National Intelligence about the draft of the Hunter Biden statement.

As CIA officials circulated the Hunter Biden statement to the highest levels of the Agency, the PCRB also felt compelled to share the statement with the Office of the Director of National Intelligence (ODNI), requesting a quick turn on ODNI's assessment. After exchanging emails, ODNI deferred to the CIA's judgement regarding the approval of the statement and stated it had no objections to the statement's release.³³

³¹ Andrew Makridis, Biography, Beacon Global Strategies, <https://bgsdc.com/team/andrew-makridis/> (last visited Jun. 12, 2024).

³² Makridis Interview at 35.

³³ See Email from the ODNI's Office of the Chief Operating Officer to PCRB Staff (Oct. 19, 2020, 10:46 AM) (Bates CIA000067) (on file with the Committee).



On the same day that ODNI cleared the Hunter Biden statement—which alleged that stories about Hunter Biden’s laptop had all the “hallmarks” of Russian disinformation—then-Director of National Intelligence John Ratcliffe issued an official statement that the laptop story was “not part of some Russian disinformation campaign . . . the intelligence community doesn’t believe that because there is no intelligence that supports that.”³⁴ Notably, as the senior most intelligence community official, Director Ratcliffe would have been the most informed individual on this subject and the best equipped to make any judgments about whether the Hunter Biden laptop was Russian disinformation.³⁵

It is unclear why the PCRB felt it was necessary to consult with ODNI regarding the Hunter Biden statement. Makridis testified that he had never reached out to his counterpart at ODNI about a submission from current or former senior staff.³⁶ Makridis could not explain why

³⁴ Brooke Singman, *Ratcliffe says Hunter Biden laptop, emails ‘not part of some Russian disinformation campaign,’* FOX NEWS (Oct. 19, 2020).

³⁵ Makridis Interview at 72 (“Someone who sits in the role of DNI has access to all the classified information the intelligence community has.”).

³⁶ *Id.* at 95.

the PCRB felt the statement merited this unusual interaction.³⁷ Simultaneously, Makridis also could not refute the possibility that the political nature of the statement spurred this outreach.³⁸ Makridis testified:

- Q. Have you ever interacted with any of your counterparts at ODNI regarding . . . these kinds of statements when you are . . . notifying for your director at the time. Did you also occasionally . . . reach over to ODNI, so to speak, to let them know that this was also coming down the pike?
- A. I don't recall reaching over to ODNI on—on any of these.
- Q. Do you think that the review of this submission rose to ODNI's COO's level due to the impact the statement could have had on the 2020 presidential election? Is that at all possible?
- A. I don't know the DNI process. They may have a similar process in place that we did. Anything written by a former senior would rise up to the chief operating officer to inform . . . their principals. So they may have had a similar process in place.³⁹

The Hunter Biden statement garnered enough interest within the CIA that it felt compelled to flag the statement for its counterparts at ODNI. This was a unique procedure that the third in command of the CIA had never followed. The decision to share the statement with ODNI widened the circle of impact the statement had on the U.S. intelligence community and therefore widened the circle of responsible individuals who could have—and should have—considered the effects of the politicized statement on the integrity of the intelligence community. In failing to do so, employees at both agencies put the American election system at risk.

C. The CIA's Office of Chief Operating Officer informed the PCRB that it could approve the Hunter Biden statement.

In his testimony before the Committees, Makridis repeatedly stated that the COO's office was not involved in the approval or disapproval of submissions to the PCRB.⁴⁰ Furthermore, he stated that the PCRB has no role beyond looking to see if submissions contained classified information.⁴¹ However, just hours after Morell submitted the draft Hunter Biden statement, Makridis's Executive Assistant sent an email to the PCRB stating that it “may notify Former DDCIA Morell.”⁴²

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *See generally* Makridis Interview.

⁴¹ *Id.* at 48.

⁴² *See* Email from Executive Assistant, Office of the Chief Operating Officer, to [Redacted]; DIR_COO_EAS, et al. (Oct. 19, 2020, 11:43 AM) (Bates CIA-000230) (on file with the Committees).

Monday, October 19, 2020 11:43:57 AM

From: [REDACTED]
To: [REDACTED]; [DIR COO EAS](#); [DDI-EA](#); [DDI ADO EAs](#); [DIR OPA FO](#); [DDI3](#); [REDACTED]
Cc: [Michelle Y. Murphy-Bell](#); [REDACTED]; [PCRB SENIOR STEERING GROUP](#)
Subject: RE: Publications Alert 19 October
Date: Monday, October 19, 2020 11:43:57 AM

Classification: UNCLASSIFIED//FOUO
=====

[REDACTED],

You may notify Former DDCIA Morell.

Thank you,

[REDACTED]

[REDACTED]
Executive Assistant, Office of the Chief Operating Officer
[REDACTED] (s) [REDACTED] (u)
[REDACTED]

You may notify Former DDCIA Morell.

One hour later, the PCRB notified Morell that he could publish the Hunter Biden statement.⁴³ The CIA and its PCRB completed this entire process—which included notifying top CIA officials and coordinating with ODNI—in a mere six-hour time period.

⁴³ Email from PCRB Staff to Michael Morell (Oct. 19, 2020, 12:44 PM) (on file with the Committees).

Monday, October 19, 2020 12:44:00 PM

From: [REDACTED]
To: "Michael M"
Cc: [REDACTED]
Subject: [AIN] PCRB Submission 999145/t21667 Determination - Approved
Date: Monday, October 19, 2020 12:44:00 PM

CLASSIFICATION: UNCLASSIFIED

AIN EMAIL

This email originated on the AIN (U) and has been forwarded to the **Agency Data Network** (TS/SCI). *This is only a copy of the original message.* This email has been virus scanned, and the message body has been converted to text-only format. If the message is from someone unfamiliar to you (especially if it contains an attachment) do NOT open it; instead, contact your ISSM (<http://security.cia/infosec/programs/issm>). The original message in its original format can be viewed in your AIN email inbox. Questions can be emailed to GLIDE_HELP.

[ANTE Up Info](#) [GLIDE File Security](#)

Message ID: 667403261/glide-ain-ecds-ap02-low-ain-adn-anteup

Dear Michael,

The Prepublication Classification Review Board completed its review of your article titled "Public Statement on the Hunter Biden Emails." The Board determined that it contains no classified information and can be published. Agency approval for publication of this material does not represent Agency endorsement or verification of this work.

If you add new material, please re-submit it before sharing, highlighting the new language to expedite our review. The PCRB appreciates your cooperation with prepublication review. You may reach out to us via PRB@ucia.gov with questions or concerns.

Kind regards,
 PCRB Staff

Dear Michael,

The Prepublication Classification Review Board completed its review of your article titled "Public Statement on the Hunter Biden Emails." **The Board determined that it contains no classified information and can be published.** Agency approval for publication of this material does not represent Agency endorsement or verification of this work.

* * *

The documents and testimony available to the Committees suggest that the CIA treated the Hunter Biden statement specially. The communications among the PCRB, CIA leadership, and ODNI staff indicated that the statement's review required a quick response. The PCRB's own subject line demarcations displayed its compliance with Morell's request that the

statement’s review be a “rush job.”⁴⁴ The CIA’s COO alerted the CIA Director or the Deputy Director about the draft statement. The PCRB appeared to believe the unique nature of the statement merited raising the draft to ODNI for review, in a process unfamiliar to the third in command at the CIA.⁴⁵ The PCRB notified Morell that it had approved the statement for publication *only after* the CIA COO’s office greenlit the statement.

In the ODNI’s analytic standards for the intelligence community, it notes the importance of analytic objectivity and sound intelligence tradecraft.⁴⁶ Every individual who came in contact with the Hunter Biden statement—from the PCRB and ODNI staff all the way up to then-Director Gina Haspel—had the opportunity to raise a concern about how the politicized Hunter Biden statement would hurt the integrity and credibility of the U.S. intelligence community. What happened instead was the publication of a politicized statement about Hunter Biden’s laptop—signed by senior former officials using their official titles—that included assertions now known to be untrue. The draft Hunter Biden statement was reviewed and passed around the highest levels of the U.S. intelligence community and still allowed to influence the public discourse surrounding the 2020 presidential election.

⁴⁴ See Email from [Redacted] to DIR_COO_EAS, et al. (Oct. 19, 2020, 8:01 AM) (Bates CIA-000230 - CIA-000231) (on file with the Committees); see also Email from the ODNI’s Office of the Chief Operation Officer to PCRB Staff (Oct. 19, 2020, 10:46 AM) (Bates CIA000067) (on file with the Committee).

⁴⁵ Makridis Interview at 95.

⁴⁶ OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, OBJECTIVITY, <https://www.dni.gov/index.php/how-we-work/objectivity> (last visited Apr. 29, 2024).

II. Some of the signatories of the Hunter Biden statement were on active CIA contracts at the time of the statement.

Internal CIA documents show that several signatories of the Hunter Biden statement—including Michael Morell—were on active CIA contract at the time the statement was published. This evidence shows that these signatories were likely earning an income supported by American taxpayer dollars while politicizing intelligence in order to boost the Biden campaign’s race for the presidency.

A. The signatories of the Hunter Biden statement claimed to not access classified information in the course of drafting the statement.

The former intelligence officials interviewed by the Committees have repeatedly asserted that they were merely a group of private citizens exercising their First Amendment rights and speaking on a matter of public interest.⁴⁷ None had access to classified information—they claimed—and were therefore just providing an opinion on a matter of public significance based upon the experience of their careers. During his transcribed interview with the Committees, for example, Morell testified that he had no access to classified material or any other investigative material prior to writing the Hunter Biden statement.⁴⁸ Morell stated:

Q. Had you had any conversations with officials at the FBI?

A. No.

Q. Had you been privy to any classified briefings . . . about this?

A. No.⁴⁹

* * *

Q. . . . Mr. Morell, as part of the research that you did in between the contact with Mr. Blinken and the contact with Marc [Polymeropoulos], did you contact any individuals as a part of that research?

A. I did not.

Q. So the full sum of that research involved your internet searches?

A. Yes.⁵⁰

⁴⁷ See, e.g., Morell Interview at 77.

⁴⁸ Morell Interview at 17, 20.

⁴⁹ Morell Interview at 16-17.

⁵⁰ Morell Interview at 20.

The other primary drafter of the public statement, Marc Polymeropoulos, similarly testified that he had no access “to classified information regarding the contents of Hunter Biden’s laptop.”⁵¹ Former CIA Director John Brennan likewise asserted that he did not have access to classified information.⁵² In his transcribed interview with the Committees, former Director of National Intelligence, James Clapper, stated that he did not seek to access any classified information when he signed the public statement.⁵³ Director Clapper stated:

Q. Well, you’re the former Director of National Intelligence, who’s about to make a very public statement about a very specific thing that you were claiming is likely Russian disinformation, you had the clearance.

You could have requested a briefing on it. Why did you not even consider doing that?

A. I didn’t do it because I didn’t think it was appropriate.

Q. Why?

A. Because I didn’t want to be tainted by . . . access to classified information.

Q. But why would it be tainted to try to find the truth before you signed—

A. Bad choice of words. . . . I wanted only to go on what I had seen publicly. That’s all. I didn’t want any connection with classified information . . . in any way.

Q. Well, it confuses me why you would be willing to sign a letter like this, and you had access to agencies who could have clarified it, and you didn’t consider even nor make an effort to find out if what you were about to say was true or not.

A. I thought it was proper and appropriate to sound a warning that the Russians could be involved. That’s all.⁵⁴

⁵¹ Transcribed Interview of Marc Polymeropoulos at 35 (Apr. 17, 2023).

⁵² Transcribed Interview of Mr. John Brennan at 78 (May 11, 2023).

⁵³ Transcribed Interview of Mr. James Clapper at 42 (May 17, 2023).

⁵⁴ *Id.*

Each signatory interviewed sought to assure the Committees that they had no access to classified information about the *New York Post* story or the contents of Hunter Biden’s laptop.⁵⁵ Even still, the use of their official titles and security credentials could be read to suggest access to classified information unavailable to everyday Americans. In his interview before the Committees, Makridis testified that the Hunter Biden statement’s claims could appear more legitimate to the average American because the signatories used their former intelligence titles.⁵⁶ Makridis testified:

Q. And at the end of this statement, the 51 former intelligence officials all used their former titles in their signature blocks and . . . many of these titles include . . . former Director of National Intelligence, former [D]irector of the Central Intelligence Agency. If you were an average citizen reading this statement, do you think that the titles of their former office could have boosted the legitimacy of their claim that the Russians were trying to influence how Americans vote in this election? Do you think that that would appear more legitimate because of their former titles that they have attached to the statement?

A. I think it’s possible.⁵⁷

Makridis confirmed that in applying their former intelligence titles to the Hunter Biden statement, the signatories could have leveraged their power and access to persuade Americans to believe, wrongly, that the Hunter Biden laptop was somehow the product of Russian disinformation. That alone is concerning. Further investigation has revealed, however, that these former intelligence officials actually could have had access to this type of specialized material.

B. Several signatories of the Hunter Biden statement had active contracts with the CIA on the statement’s publication date.

Despite repeated assertions that the Hunter Biden statement’s signatories were former intelligence officials with no access to classified information related to the *New York Post* story about Hunter Biden’s laptop, internal CIA staff emails reveal that at least some of the signatories were on active contract with the CIA at the time of its drafting, review, and publication.⁵⁸ In particular, in an internal email from October 20, 2020, a CIA employee wrote to a colleague: “I

⁵⁵ See, e.g., Transcribed Interview of Mr. Nicholas Rasmussen at 11-12 (May 15, 2023) (“[T]he most important thing from my perspective was to focus on the caveating language, because I knew – at least based on what I knew, that there was not certainty about the provenance of the laptop issue. And so I focused in on the paragraph in particular that stated quite clearly that we did not know if the emails are genuine or not and that we did not have evidence of Russian Government involvement, just that this confluence events makes us deeply suspicious.”).

⁵⁶ Makridis Interview at 70.

⁵⁷ *Id.*

⁵⁸ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 11:05 AM) (Bates CIA000157) (on file with the Committees).

also love that at least a few of the random signatories belong to individuals currently working here on contracts.”⁵⁹

I also love that at least a few of the random signatures belong to individuals currently working here on contracts...

From: [REDACTED]
To: [REDACTED]
Subject: RE: letter from former IC officers
Date: Tuesday, October 20, 2020 11:05:02 AM

Classification: UNCLASSIFIED

I also love that at least a few of the random signatures belong to individuals currently working here on contracts...

-----Original Message-----

From: [REDACTED]
Sent: Tuesday, October 20, 2020 10:13 AM
To: [REDACTED]
Subject: FW: letter from former IC officers

Classification: UNCLASSIFIED

This frustrates me. I don't think it is helpful to the Agency in the long run. Sigh.

<https://www.politico.com/f/?id=00000175-4393-d7aa-af77-579f9b330000>

This frustrates me. I don't think it is helpful to the Agency in the long run. Sigh.

Following the Committees' review of this document, the Committees requested the identities of CIA contractors who signed the Hunter Biden statement. While the CIA has not declassified the complete list of individuals who were on contract with the Agency at that time due to purported operational security, it has disclosed that at least two signatories—Michael Morell and former CIA Inspector General David Buckley—were on active contract on the day of the Hunter Biden statement was published.⁶⁰ This disclosure means, in essence, that Morell and Buckley were likely earning taxpayer dollars from their work with the intelligence community—

⁵⁹ *Id.*

⁶⁰ See Letter from Robert F. Dugas, Deputy General Counsel for Litigation and Investigations, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence (Apr. 25, 2024) (Bates CIA-000236) (on file with Committees); see also Email from [Redacted] to [Redacted] (Oct. 20, 2020, 11:05 AM) (Bates CIA000157) (on file with the Committees).

headed, ultimately, by President Donald Trump—while simultaneously working with the presidential campaign of Vice President Joe Biden to influence the outcome of the 2020 American presidential election.⁶¹

UNCLASSIFIED

Name	Contract with CIA (directly or through a company) on October 19, 2020?
John Brennan	No
Michael Morell	Yes
Marc Polymeropoulos	No
David Buckley	Yes
Nick Rasmussen	No

Beyond the potential access to classified information or the use of their positions to influence the approval of the statement, it is concerning that those on contract at the CIA would even be involved in the crafting and promotion of what amounted to a campaign press release. Even Morell, the architect of the Hunter Biden statement and an individual on active contract with the CIA, acknowledged in his transcribed interview—before the Committees learned about his contract—that it is “inappropriate for a currently serving staff officer or contractor to be involved in the political process.”⁶²

Makridis agreed with Morell’s statement that is inappropriate for a CIA contractor to be engaged in the political process. In his transcribed interview with the Committees, he testified:

Q. Mr. Morell testified before Congress on April 4th, 2023, that it would be inappropriate for a currently serving staff officer or a contractor to be involved in the political process. Do you agree with Mr. Morell’s statement?

A. I think that’s generally understood.⁶³

It appears that CIA leadership never expressed any concern about the fact that individuals on active contract with the CIA signed the Hunter Biden statement. According to Makridis, if individuals were on active contract with the CIA, “[t]he PCRB review process would have looked at—at that. So they would have handled that issue if it were a problem.”⁶⁴ Yet there is no indication in any of the evidence or documents produced to the Committees showing that the PCRB stopped or slowed the review of the statement to “look[] at” the participation of

⁶¹ *Id.*

⁶² Morell Interview at 31.

⁶³ Makridis Interview at 92.

⁶⁴ *Id.* at 91.

signatories on contract. Instead, the documents show that the PCRB approved the release of the statement within six hours of it being submitted.

Although Hatch Act political restrictions do not apply to federal contractors in the same way they do to CIA employees,⁶⁵ Makridis stated that he would have examined the relevant ethical circumstances in more detail before signing off on the Hunter Biden statement. He explained that if he were CIA director at the time, he “would [have made] a call to the office of general counsel and [had] that person come in, and we would have [had] that discussion.”⁶⁶ Those who were in charge at the time, however, apparently did not have such discussions, and the PCRB greenlit the statement submitted by a former official with an active CIA contract.

The CIA also produced documents shedding light on the conflicts of interest this contractor status created. Internal CIA documents that were recently produced to the Committees indicate that former CIA Inspector General David Buckley, like Morell, was on active contract with the CIA.⁶⁷ Buckley, however, also held a green badge—which gives cardholders access to secure CIA facilities—at the time of the Hunter Biden statement’s publication.⁶⁸ According to the CIA, Buckley remained either on active contract or with green badge access to all CIA facilities until April 2022.⁶⁹ Historically, green badge access has been given to individuals regularly employed by or permanently assigned to the Agency, allowing them access to all of its facilities.⁷⁰ In Buckley’s case, this would mean he retained unfettered access to all CIA facilities through April 2022. Morell was also hired back as a contractor in May 2021, after the publication of the statement.⁷¹

⁶⁵ JUSTICE MANAGEMENT DIVISION, U.S. DEP’T OF JUSTICE, POLITICAL ACTIVITIES, <https://www.justice.gov/jmd/political-activities> (last visited Apr. 24, 2024).

⁶⁶ Makridis Interview at 92.

⁶⁷ See Letter from Robert F. Dugas, Deputy General Counsel for Litigation and Investigations, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence (Apr. 25, 2024) (Bates CIA-000236) (on file with Committees)

⁶⁸ See Letter from Robert F. Dugas, Deputy General Counsel for Litigation and Investigations, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence (May 20, 2024) (Bates CIA-000237).

⁶⁹ See Letter from Robert F. Dugas, Deputy Gen. Counsel for Litigation and Investigations, Office of Gen. Counsel, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence. (Feb. 14, 2024) (Bates CIA-000235) (on file with Committees).

⁷⁰ Security Regulations for the Central Intelligence Group (Aug. 15, 1947) (approved for release Mar. 2, 2001).

⁷¹ See Letter from Robert F. Dugas, Deputy Gen. Counsel for Litigation and Investigations, Office of Gen. Counsel, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence. (Feb. 14, 2024) (Bates CIA-000235) (on file with Committees).

MICHAEL MORELL	Independent contractor, no fee senior advisory services	Independent Contractor	5/1/21-10/8/21	YES	TS/SCI
-----------------------	---	------------------------	----------------	-----	--------

NAME	NATURE OF CONTRACT	CONTRACTOR COMPANY	DATE(S) IDENTIFIED AS A CONTRACTOR/GREEN BADGE	INDIVIDUAL HELD AGENCY CLEARANCE ON 10/19/2020	HIGHEST LEVEL OF CLEARANCE CARRIED AT TIME STMT WAS ISSUED
JEREMY BASH	Independent contractor, no fee senior advisory services	Independent Contractor	4/2/19-4/1/22 and 8/22/22-Present Expires 8/21/24	YES	TS/SCI
RODNEY SNYDER	Industrial contractor	Guidehouse Inc.	7/26/16-9/30/20 and 7/20/21-7/14/23	YES	TS/SCI
DAVID BUCKLEY	Industrial contractor	KPMG LLP	5/3/17-4/25/22	YES	TS/SCI
RICHARD H. LEDGETT JR.	Independent contractor, no fee senior advisory services	Independent Contractor	4/22/19-4/21/21	YES	TS/SCI
MICHAEL MORELL	Independent contractor, no fee senior advisory services	Independent Contractor	5/1/21-10/8/21	YES	TS/SCI
DOUG WISE	Independent contractor, no fee senior advisory services	Independent Contractor	1/17/24-Present Expires 1/16/25	NO	N/A

DAVID BUCKLEY	Industrial contractor	KPMG LLP	5/3/17-4/25/22	YES	TS/SCI
----------------------	------------------------------	-----------------	-----------------------	------------	---------------

It is extremely concerning that signatories of the Hunter Biden statement were on contract with the CIA at the time of the statement’s drafting, review, and publication. This revelation shows that Morell, Buckley, and likely other signatories were receiving U.S. taxpayer funds while engaged in a politicized project to mislead American voters on behalf of the Biden campaign. Such an overtly political action would be illegal under the Hatch Act for a permanent CIA employee. Congress ought to consider whether to extend this important prohibition to CIA contractors as well.

III. Officials inside the CIA recognized that the Hunter Biden statement was political.

Morell and Polymeropoulos drafted the Hunter Biden statement with the explicit goal of assisting then-candidate Biden in his race to become president. As Morell testified to the Committees: “There were two intents. One intent was to share our concern with the American people that the Russians were playing on this issue; and two, it was to help Vice President Biden.”⁷² Moreover, Morell and Polymeropoulos informed prospective signatories of the intent of the statement prior to its publication, writing that the statement was meant to insulate Vice President Biden from serious electoral vulnerabilities created by his family’s influence peddling activities. Given the fact that some of the signatories were on active contract with the CIA—an organization that is explicitly prohibited from operating domestically⁷³—their effort to score political points for then Vice President Biden undermined the integrity of the Agency.

⁷² Morell Interview at 11.

⁷³ Makridis Interview at 89.

From: Michael M <Michael Morell >
Sent: Sunday, October 18, 2020 7:47 PM
To: James Clapper < >
Subject: Re: Request to Sign On to Statement

Jim,

Thanks.

And, your editorial suggestion has been made. It was a good one.

Michael

On Sun, Oct 18, 2020 at 6:10 PM James Clapper < > wrote:

Michael:

I'll gladly sign on; I said as much on CNN Friday evening.

I have one editorial suggestion for the letter: I think it would strengthen the verbiage if you say this has all the classic earmarks of a Soviet/Russian information operation rather than the "feel" of a Russian operation.

Jim

On Oct 18, 2020, at 5:25 PM, Michael <Michael Morell > wrote:

Sir,

Please see attached. Would love to have you sign. Trying to get Dan Coats to join us.

Thanks.

Begin forwarded message:

From: Michael M <Michael Morell >
Date: October 18, 2020 at 4:48:43 PM EDT
To: Michael M <Michael Morell >
Cc: Marc Polymeropoulos < >
Subject: Request to Sign On to Statement

Marc and I drafted the attached because we believe the Russians were involved in some way in the Hunter Biden email issue and because **we think Trump will attack Biden on the issue at this week's debate and we want to give the VP a talking point to use in response.**

We would be honored if each of you would be willing to join us in signing the letter.

If you do agree to sign, please let me know how you would like your affiliation to read. For those CIA officers on the bcc line, I would like to find a way to highlight your Russia work, if appropriate. For example, Marc's citation will read:

Marc P...
Former Senior CIA Operations Officer
Former Acting Chief of Operations for Europe and Eurasia

If you want to agree to sign but make that "conditional" on seeing who else is willing to sign, I'm happy to send you the final list, probably tomorrow, before obtaining your final approval.

I will clear the statement with the Publication Review Board at CIA tomorrow.

Let us know. Thanks.

Michael and Marc

<Hunter Biden Statement.docx>

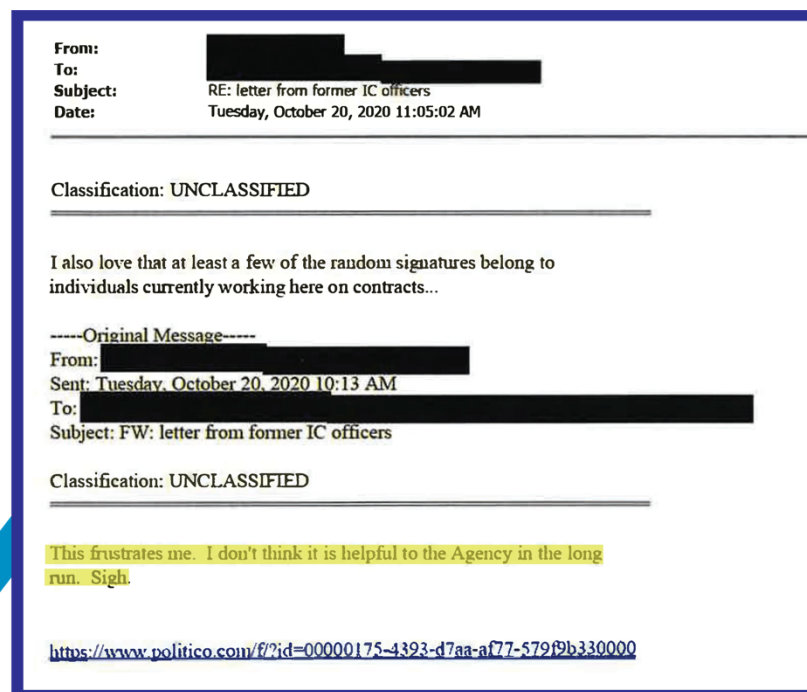
we think Trump will attack Biden on the issue at this week's debate and we want to give the VP a talking point to use in response.

On October 18, 2020, Morell—the key orchestrator behind the Hunter Biden statement, who was receiving taxpayer dollars through his CIA contract at the same time—and Polymeropoulos drafted an email that they sent to a group of former intelligence officials, asking them to sign the statement.⁷⁴ The message outlined the politicized motivations behind the statement. Morell and Polymeropoulos wrote:

Marc and I drafted the attached because we believe the Russians were involved in some way in the Hunter Biden email issue and because we think Trump will attack Biden on the issue at this week's debate and we want to give the VP a talking point to use in response.

We would be honored if each of you would be willing to join us in signing the letter.⁷⁵

Shortly after the Hunter Biden statement's publication, individuals inside the CIA noted their concerns with the statement. In one internal CIA email sent on October 20, 2020, staff lamented that the statement would hurt the CIA, "[t]his frustrates me. I don't think it is helpful to the Agency in the long run."⁷⁶



This frustrates me. I don't think it is helpful to the Agency in the long run. Sigh.

⁷⁴ Email from Michael Morell to Michael Morell, Marc Polymeropoulos, and Bcc'd Recipients (Oct. 18, 2020, 4:48 PM) (on file with the Committees).

⁷⁵ Email from Michael Morell to Michael Morell, Marc Polymeropoulos, and Bcc'd Recipients (Oct. 18, 2020, 4:48 PM) (on file with the Committees).

⁷⁶ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 10:13 AM) (Bates CIA000157) (on file with the Committees).

In his transcribed interview with the Committees, Makridis testified that he agreed that the Hunter Biden statement damaged the integrity of the CIA and garnered unhelpful attention for the CIA. During his testimony before the Committees, he stated that it is best for the CIA to not be splashed on the news and that the Agency had an important duty best done without publicity.⁷⁷ Makridis testified:

Q. . . . [C]ould you please read the contents of that bottom email to me?

A. “This frustrates me. I don’t think it is helpful to the Agency in the long run. Sigh.”

Q. And it includes a URL link to the Politico article, which does link to the October 19th statement on the Hunter Biden email story signed by 51 former intelligence officials. Why do you think this individual was frustrated by the publication of the statement?

* * *

A. I don’t recall this email. But why was the person frustrated? I don’t know. I guess it’s an interesting question to ask the person. Again, I don’t recall this email.

Q. Do you have any personal frustrations with the October 19th statement?

A. You know, I think the Agency’s work is best done when it . . . doesn’t sort of splash across the press in any way, but that’s a general statement, and I think most CIA officers would sort of say the same.⁷⁸

Makridis testified that he viewed the Hunter Biden statement as a political document that influenced the presidential race between President Trump and Vice President Biden.⁷⁹ Makridis testified:

Q. So I think you were asked at the last hour in minority questioning, did you—is it your opinion this statement of the 51 former intelligence officials was a political statement . . . because of the congressional investigation that followed? Was that your testimony? Or was it inherently political?

⁷⁷ Makridis Interview at 29-30.

⁷⁸ *Id.*

⁷⁹ *Id.* at 97.

- A. Well, I said I wouldn't be involved in politics, right? So that's what you're, sort of, getting at. . . . I mean, it's talking about President Trump, Vice President Biden. I mean . . . you can't read that and say there isn't politics involved of some nature.⁸⁰

Unlike other intelligence officers, Makridis said that he took issue with the nature of the Hunter Biden statement. Makridis stated that he would not have signed onto the publication if asked because he isolates his professional life from political matters. Makridis confirmed:

- Q. . . . [W]ould you have signed this statement?
- A. As I said earlier, I've stayed out of politics and things that could be politicized, so . . . for that reason, I would not have signed the statement.⁸¹

On October 20, 2020, Polymeropoulos sent to the PCRB for review a set of talking points that he had drafted related to the Hunter Biden statement. These talking points—which the PCRB ultimately approved for publication—raised concerns for Agency employees, according to documents produced to the Committees.⁸²

⁸⁰ *Id.*

⁸¹ *Id.* at 44.

⁸² CIA produced versions of the relevant documents with differing redactions. The Committees were able to confirm the documents concerned the same matter based on a comparison of the documents. The below graphic includes two email chains in which the subject lines and time stamps for the first three emails in each chain are identical. The bodies of these initial three emails in each chain appear identical, but the unredacted version references a manuscript submitted by Polymeropoulos regarding the Hunter Biden laptop story. The highlighted and connected portions of the graphic demonstrate that these two email chains were identical until they verged into separate conversations. Based on a side-by-side comparison, the Committees were able to confirm that these chains both reference Polymeropoulos's talking points. During his transcribed interview, Mr. Makridis confirmed the Committees' comparison. *See* Makridis Interview at 85 (“Q: [B]ut we can at least establish that they are both in response to an email chain referencing Marc Polymeropoulos' manuscript talking points. A: It appears that way.”).

One CIA employee wrote an internal email noting that it was “interesting” that the PCRB approved the talking points for publication in the first place.⁸³

From: [REDACTED]
To: CIMC_RAD_NITB
Subject: FW: PCRB Item of Interest 20 October (Two of two)
Date: Tuesday, October 20, 2020 10:11:54 AM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.jpg](#)
[REDACTED]

Classification: UNCLASSIFIED//FOUO
=====

Interesting to see what was submitted and approved by PCRB. Please do not forward.

[REDACTED]
Branch Chief, Nontraditional Intelligence Threats Branch (NITB)
Counterintelligence Mission Center/Research & Analysis Department (CIMC/R&AD)
[REDACTED] | [REDACTED]
[REDACTED]

[REDACTED]

⁸³ See Email from the Branch Chief of Nontraditional Intelligence Threats, CIA to CIMC_RAD_NITB, CIA (Oct. 20, 2020, 10:11 AM) (Bates CIA-000232) (on file with the Committees).

In another email on the same topic, a CIA staff member described Polymeropoulos as engaging in a “pro-Biden campaign and may be disclosing classified information in his efforts.”⁸⁴

From: [Redacted]
To: [Redacted]
Subject: FW: PCRB Item of Interest 20 October (Two of two)
Date: Tuesday, October 20, 2020 10:45:50 AM
Attachments: [image001.jpg](#)
[image002.png](#)
[Redacted]

Classification: UNCLASSIFIED//~~FOUO~~
=====

Good Morning, [Redacted] and [Redacted]

It appears [Redacted] is actively involved in a pro-Biden campaign and may be disclosing classified information in his efforts. It is difficult to believe that the timing of the attached [Redacted] and the [Redacted] are coincidental. [Redacted]
[Redacted]

Thanks,
[Redacted]

Included in his talking points submitted to the PCRB and aimed at discrediting the Hunter Biden laptop as a Russian plant, Polymeropoulos made broad and unsupported—and, as it turns out, wrong—political assertions about so-called Russian disinformation. He wrote:

From Fox News—the lead dissemination mechanism inside the US, to Senator Johnson of Wisconsin, there is no shortage of individuals in the GOP orbit who will lap up anything that the Russians throw their way.⁸⁵

⁸⁴ See Email from [Redacted] to [Redacted] (Oct. 20, 2020, 10:45 AM) (Bates CIA000178 - CIA000180) (on file with the Committees).

⁸⁵ See Letter from Robert F. Dugas, Deputy General Counsel for Litigation and Investigations, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence (May 20, 2024) (Bates CIA-000239) (on file with Committees).

It is concerning enough that Polymeropoulos's talking points sought to discredit the Hunter Biden laptop in an effort to boost then-candidate Biden in the 2020 presidential election. Polymeropoulos had decades of experience in the CIA and should have known the proper protocols surrounding the use of classified information. In his testimony before the Committees, Makridis outlined the broad mandate every CIA staff member operates under, stating:

- Q. Okay. Now, someone trying to assist a presidential campaign using classified information—potentially using classified information from the CIA, fair to say even bigger no-no, if I may?
- A. Use of classified information, regardless of the purpose, is a no-no.
- Q. Right.
- A. Whether that's for personal gain, political gain, or just a mistake. That's a no-no.⁸⁶

Makridis stated what every individual entrusted with a government clearance understands, that the unauthorized exposure of classified information is unacceptable under any circumstances. Despite this, Polymeropoulos—either knowingly or negligently—leveraged classified information to help the Biden campaign. Ultimately, the PCRB prevented Polymeropoulos from disseminating classified information in his talking points, but CIA staff still expressed concerns that his talking points were approved at all.⁸⁷ However, the CIA lacked any safeguards to prevent this classified information from being shared publicly before the PCRB stepped in.

⁸⁶ Makridis Interview at 88.

⁸⁷ Email from [Redacted], Branch Chief of Nontraditional Intelligence Threats, CIA to CIMC_RAD_NITB, CIA (Oct. 20, 2020, 10:11 AM) (Bates CIA-000232).

Conclusion

The October 19, 2020, statement on Hunter Biden’s laptop signed by 51 former senior intelligence community officials served to interfere in the American electoral system in the final weeks before the 2020 presidential election. The highest officials within the CIA were aware of the statement prior to its publication. Signatories of the statement—including lead architect, former Acting CIA Director Michael Morell, and former CIA Inspector General David Buckley—were on active contract with the CIA at the time the statement was drafted, reviewed, and ultimately published. This revelation raises the concern that these officials abused the access of their positions to curate, promote, and receive expedited approval of the statement. Indeed, the PCRB continuously requested quick decisions from officials within the CIA and partners at ODNI about the status of publication of the statement. This occurred after Morell specifically requested an expedited review process and during a time when he had contracting status and was under consideration to be named President Biden’s CIA Director.

The signatories’ choice to leverage the authority of their former intelligence community titles to peddle a narrative about foreign election interference inappropriately embroiled the Agency in the domestic political process. The poor judgment displayed by the signatories and the CIA’s executive suite—those who could have prevented the Agency from being entangled in a false and domestically politicized narrative of Russian interference—is as relevant today as it was four years ago. To date, there are no clear or transparent rules to prevent intelligence contractors from leveraging their access to the CIA for political purposes.

Seasoned CIA officials like Morell and Polymeropoulos were able to subvert the process to spread disinformation in the weeks leading up to the 2020 presidential election because the CIA lacked meaningful safeguards to prevent this from happening. Unless and until the CIA makes substantial reforms to its own oversight processes surrounding public statements and contractor behavior, these problems could persist.

Without rigorous oversight of the intelligence community—and without proper safeguards to prevent the weaponization of privileged access within the intelligence community—rogue actors like Morell and Polymeropoulos are likely to continue engaging in political work under the guise of responsible action. As a result, the Committees will continue oversight to prevent individuals from using the authority of the federal government for their own partisan desires.

Addendum

On July 11, 2024, over two weeks after the release of the Committees' second interim report, the CIA notified the Committees that it identified an error in the CIA's productions regarding Mr. Morell's and Mr. Buckley's contracting status.¹ Specifically, the CIA now states that, contrary to its earlier representations to the Committees, Mr. Morell was not on contract with the CIA on October 19, 2020.² Although the CIA claims that Mr. Morell was not on contract as of October 19, 2020, the CIA reports that he was on contract both before and after that date, but it has provided few additional details to the Committees. The CIA believes "[t]his mistake was based on a misreading of the contract documentation" and it "regret[s] and apologize[s] for these errors."³ It further claims that all other information provided to the Committees "accurately reflect[s] available information contained in CIA records."⁴

Although the Committees appreciate the CIA's effort to correct the record, it has raised more questions and concerns about the accuracy of information the CIA provides to Congress. The CIA confirmed multiple times for the Committees that Mr. Morrell was on contract as of October 19, 2020, prior to the release of the second interim report.⁵ The CIA notified the Committees of its mistake after issuance of the report and following complaints from Mr. Morell.⁶ The Committees will continue to conduct oversight into this matter, including how the CIA came to provide misleading information to the Committees.

¹ Letter from Robert F. Dugas, Deputy General Counsel for Litigation and Investigations, CIA to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, and Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence (Jul. 11, 2024).

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ *See, e.g.*, Letter from Robert F. Dugas, Deputy General Counsel for Litigation and Investigations, Central Intelligence Agency, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary & Rep. Michael Turner, Chairman, H. Permanent Select Comm. on Intelligence (Apr. 25, 2024) (Bates CIA-000236) (on file with Committees).

⁶ *See* Steven Nelson, 'Spies Who Lie' were CIA contractors when they falsely implied Hunter Biden laptop was Russian fake, NEW YORK POST (Jun. 25, 2024).