



**ELECTION INTERFERENCE: HOW THE FBI “PREBUNKED” A TRUE STORY
ABOUT THE BIDEN FAMILY’S CORRUPTION IN ADVANCE OF THE 2020
PRESIDENTIAL ELECTION**

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 30, 2024

EXECUTIVE SUMMARY

“But, when we get hauled up to [Capitol] hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG [U.S. Government] to plan for it.”

—July 15, 2020, 3:17 p.m. ET, internal Facebook message during Facebook’s meeting with the FBI and other agencies.¹

At 5:00 a.m. ET, on Wednesday, October 14, 2020, less than three weeks before the 2020 presidential election, the *New York Post* published a potentially election-altering news story about a years-long influence peddling scheme carried out by the family of the Democratic nominee for president, former Vice President Joe Biden.² The *Post* article detailed how Hunter Biden leveraged his famous last name to provide foreign officials with access to his father in exchange for the Biden family’s significant financial gain.³ This information was recovered from the hard drive of a laptop attributed to Hunter Biden, and the article included pictures of a signed federal subpoena, demonstrating that the Federal Bureau of Investigation (FBI) had seized that hard drive.⁴ Neither Hunter Biden nor the Biden presidential campaign denied the allegations or the provenance of the laptop; indeed, the Biden Department of Justice (DOJ) has since authenticated the laptop as evidence in federal court.⁵

Soon after the *Post* article was published, however, something strange happened. Almost immediately, major social media platforms, including Twitter and Facebook—the modern-day digital town square—censored the true story about Biden family influence peddling. As a consequence, millions of Americans cast their presidential vote unaware of serious, credible allegations of misconduct levied against one of the two candidates. This censorship served to benefit one candidate over the other and wrongfully affected the 2020 election.⁶ Today, these companies and their executives belatedly admit that their censorship was wrong.⁷

Why were the social media companies so ready to censor a true story about Hunter Biden featured in a prominent American newspaper? Because the FBI had primed them for it. For nearly a year, the FBI had been conditioning social media companies to expect a “hack-and-leak” operation from Russia involving Hunter Biden. In more than thirty meetings across eight

¹ Internal messages among Facebook personnel (July 15, 2020, 3:17 p.m.), *see* Ex. 10.

² *See* Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020).

³ *Id.*

⁴ *Id.*

⁵ James Lynch, *Prosecution Introduces Hunter Biden’s Infamous Laptop at Trial, Uses Data as Evidence of Crack Addiction*, NAT. REVIEW (June 4, 2024).

⁶ *See, e.g.*, Rich Noyes, *SPECIAL REPORT: The Stealing of the Presidency, 2020*, MEDIA RSCH. CTR. (Nov. 24, 2020) (“Even more Biden voters (45.1%) said they were unaware of the financial scandal enveloping Biden and his son, Hunter . . . According to our poll, full awareness of the Hunter Biden scandal would have led 9.4% of Biden voters to abandon the Democratic candidate[.]”).

⁷ Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[W]e shouldn’t have demoted the [*New York Post*] story.”); Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.); Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.).

months, the FBI led Big Tech to believe that the allegations in the *Post* story were Russian disinformation, even though the FBI had authenticated Hunter Biden’s laptop nearly a year prior.⁸

Beginning in early 2020, the FBI embarked on a concerted campaign to preemptively debunk—or “prebunk”—allegations about the Biden family’s influence peddling. Federal agencies repeatedly warned social media platforms about a pre-election Russian influence operation relating to Hunter Biden and the Ukrainian company Burisma.⁹ In many of these meetings between federal agencies and Big Tech, the FBI raised the topic of potential “hack-and-leak” operations amid conversations about “election security” and potential foreign influence operations.¹⁰ In response, some platforms even adopted new content moderation policies specifically designed to address hacked materials.¹¹

Then, when the *Post* reported on Biden family influence peddling the morning of October 14, 2020, Big Tech did exactly what it had been primed to do. The social media companies obediently treated the article as a potential Russian hack-and-leak operation and applied their content moderation policies to censor it, prevent it from spreading, and hide it from the American people.¹²

Of course, as was obvious then and as is widely acknowledged now,¹³ the laptop was real and its contents were authentic. It was not Russian disinformation. The FBI knew this, too—it had been in possession of Hunter Biden’s laptop since late 2019 and used it in one or more ongoing investigations in 2020.¹⁴ Indeed, in June 2024, the Justice Department used content from the laptop as evidence against Hunter Biden in his trial for felony gun crimes.¹⁵ And yet, the FBI not only primed the social media companies to distrust allegations about Biden family influence peddling in advance, it misled social media companies about the authenticity of Hunter Biden’s laptop after the *Post* story broke.¹⁶

The FBI’s duplicity notwithstanding, Big Tech companies bear blame as well. Contemporaneous documents from the relevant period show that social media companies

⁸ See *infra* Section II.B; Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12.

⁹ See *infra* Section II.C.

¹⁰ *Id.*

¹¹ See *infra* Section II.D.

¹² See *infra* Section III.

¹³ See, e.g., Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he reporting was not Russian disinformation[.]”); Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024); Ingrid Jacques, *Trump right about Hunter’s ‘laptop from hell,’ though Biden claimed Russian disinformation*, USA TODAY (June 6, 2024).

¹⁴ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12.

¹⁵ Ryan King et al., *Hunter Biden gun trial jurors shown infamous laptop first exposed by The Post in dramatic courtroom reveal*, N.Y. POST (June 4, 2024); see also Josh Christenson, *Video of Dems, media rejecting Post’s Hunter Biden laptop story as ‘Russian disinfo’ goes viral after FBI confirms authenticity in court*, N.Y. POST (June 6, 2024).

¹⁶ See *infra* Section III.

recognized and received information that the Biden family influence peddling allegations were likely not Russian disinformation;¹⁷ nonetheless senior leadership at these companies decided to take steps to hide this true content highly relevant to the upcoming presidential election because they knew a failure to censor the story could affect how a potential incoming Biden-Harris Administration would treat them.¹⁸

Nick Clegg <[REDACTED]@s.whatsapp.net>
Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...

“Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...”

—Oct. 14, 2020, internal messages between Facebook’s then-Vice President of Global Affairs Nick Clegg to Vice President of Global Public Policy Joel Kaplan about Facebook’s censorship of the *New York Post* article

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been conducting oversight of how and to what extent the Executive Branch has coerced or colluded with companies and other intermediaries to censor lawful speech.¹⁹ Through a series of reports, the Committee and Select Subcommittee have revealed how the Executive Branch worked with social media companies, “disinformation” pseudoscientists, and others to censor Americans’ online speech.²⁰

This interim report focuses on the coordination between the FBI and Big Tech to suppress allegations about Biden family influence peddling in advance of the 2020 election. Testimony from key FBI and Big Tech personnel and subpoenaed nonpublic internal documents and communications obtained by the Committee and Select Subcommittee show that in the months before the election, the FBI provided social media companies with specific warnings:

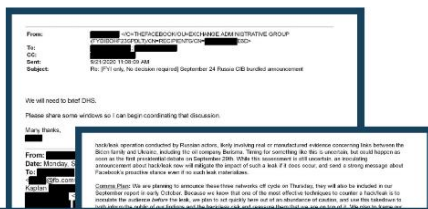
¹⁷ See, e.g., *infra* Section III.B.3.

¹⁸ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), see Ex. 101.

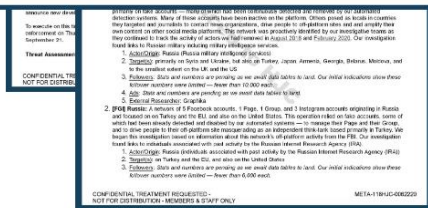
¹⁹ See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

²⁰ See, e.g., 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 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); 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 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); 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 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 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 FBI’S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH (Comm. Print July 10, 2023); 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 WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

- **WHO: *Russia*.** The FBI repeatedly warned Big Tech of a potential influence operation by Russian actors targeting the 2020 election.²¹
- **WHAT: *A hack-and-leak operation*.** The FBI repeatedly warned Big Tech that the Russian influence operation would likely take the form of a hack and leak, similar to the leak of Democratic National Committee emails in 2016.²²
- **WHEN: *Late September or October 2020*.** The FBI repeatedly warned Big Tech that this hack-and-leak operation would come right before the election, either as “an October surprise”²³ or “as soon as the first Presidential debate on September 29th.”²⁴
- **WHY: *To reveal “evidence” regarding “links between the Biden family and Ukraine,” including “Burisma.”*** The FBI warned Big Tech that the Russian hack-and-leak operation would likely involve “real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma.”²⁵ Internal Microsoft notes state that a “week” before the *New York Post* story broke on October 14, the “FBI tipped [Big Tech] off” that “this Burisma story was likely to emerge.”²⁶



Threat Assessment: We have recently received indications from USG partners that they believe there is a risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma. Timing for something like this is uncertain, but could happen as soon as the first presidential debate on September 29th. While this assessment is still uncertain, an inoculating announcement about hack/leak now will mitigate the impact of such a leak if it does occur, and send a strong message about Facebook's proactive stance even if no such leak materializes.



“USG partners . . . believe there is a risk of a hack/leak operation . . . likely involving . . . evidence concerning links between the Biden family and Ukraine, including the oil company Burisma.”

—Sept. 21, 2020 internal Facebook email to senior Facebook executives

²¹ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), see Ex. 1; Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 21-25.

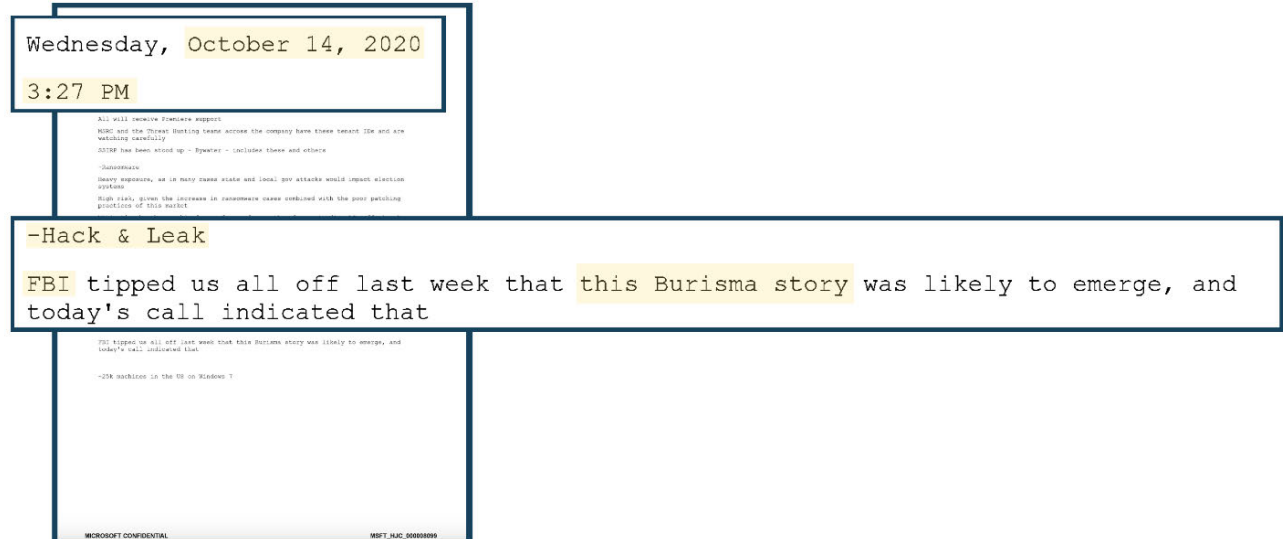
²² *Id.*

²³ Internal message from Facebook personnel to Nick Clegg (Oct. 15, 2020, 9:29 a.m.), see Ex. 2.

²⁴ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), see Ex. 1.

²⁵ *Id.*

²⁶ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), see Ex. 3.



“FBI tipped us all off last week that this Burisma story was likely to emerge”
 —Oct. 14, 2020, internal Microsoft notes on meeting between U.S. government and Big Tech

As documents produced to the Committee and the Select Subcommittee show, the U.S. government—particularly the FBI, while in possession of Hunter Biden’s laptop—provided detailed warnings of an anticipated future Russian influence operation that directly mirrored the contents of the laptop.²⁷ Documents and testimony also reveal that FBI personnel who were part of the FBI task force providing these warnings knew that the laptop was real prior to the release of the *New York Post* story.²⁸ Armed with evidence of Biden family corruption, the FBI worked for months to ensure that when this evidence emerged in the public sphere, Big Tech would be ready to downplay and censor it.

Big Tech’s immediate reactions to the October 14 *Post* story confirm how the companies were primed by the FBI’s months-long prebunking efforts. For example, internal Facebook communications show that the company almost immediately deemed the story to be a “hack/leak” of the sort Facebook was “expect[ing].”²⁹ On the morning of October 14, Facebook employees exchanged candid communications about the story, including:

- 8:37 AM ET: “About what we expected in the hack/leak department [...] it’s pretty much exactly what we pregamed.”³⁰
- 8:42 AM ET: “It looks like exactly the hack/leak scenario we’d expected.”³¹
- 9:06 AM ET: “Can we check with FBI Delaware if they have anything [on] this [...] Article claims that FBI has had the HDD [hard drive] since December.”³²

²⁷ See *infra* Section II.C.

²⁸ See *infra* Section II.A.

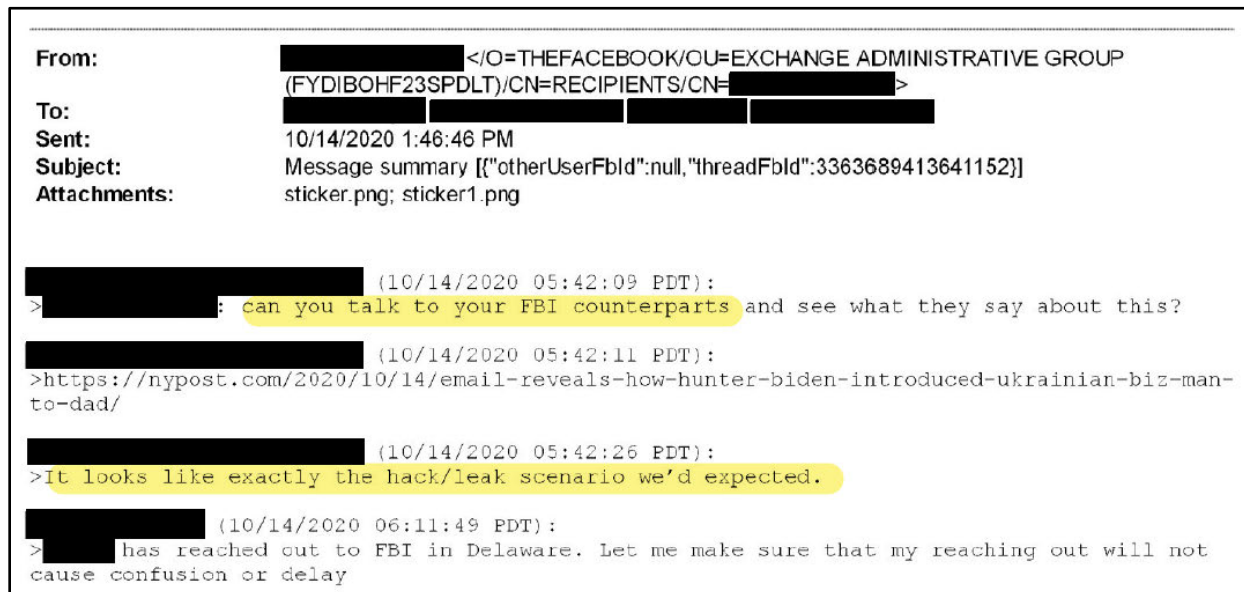
²⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:37 a.m.), see Ex. 4.

³⁰ *Id.*

³¹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:42 a.m.), see Ex. 5.

³² Internal messages among Facebook personnel (Oct. 14, 2020, 9:06 a.m.), see Ex. 6.

- 9:09 AM ET: “Exact content expected for hack and leak.”³³
- 9:10 AM ET: “Right on schedule.”³⁴
- 9:14 AM ET: “[Facebook employee] is not in touch with the FBI on this. I’ll connect with Maryland and [Facebook employee] will raise at the [FBI’s Foreign Influence Task Force] meeting today.”³⁵
- 9:33 AM ET: “FYI. Our legal team is reaching out to FBI on this.”³⁶
- 10:40 AM ET: “We’re enqueueing the content with demotion and doing outreach to 3PFCs [third-party factcheckers]. No updated info from FBI, no outreach from the Biden campaign.”³⁷
- 10:55 AM ET: “is this the Oct surprise everyone was waiting for?”³⁸



“It looks like exactly the hack/leak scenario we’d expected”
 —Oct. 14, 2020, internal messages among Facebook personnel

Other documents suggest that key employees within the social media companies understood how their censorship would influence the election. Before the story broke, Facebook personnel understood that their response to an alleged hack and leak could sway the presidential election: in a July 2020 internal exchange, a member of Facebook’s Trust and Safety team said that “when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with [the U.S. Government] to plan for it.”³⁹ Nothing had

³³ Internal messages among Facebook personnel (Oct. 14, 2020, 9:09 a.m.), *see* Ex. 7.

³⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 9:10 a.m.), *see* Ex. 7.

³⁵ Internal messages among Facebook personnel (Oct. 14, 2020, 9:14 a.m.), *see* Ex. 6.

³⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 9:33 a.m.), *see* Ex. 8.

³⁷ Internal messages among Facebook personnel (Oct. 14, 2020, 10:40 a.m.), *see* Ex. 7.

³⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 10:55 a.m.), *see* Ex. 107.

³⁹ Internal messages among Facebook personnel (July 15, 2020, 3:17 p.m.), *see* Ex. 10.

changed by the time the story broke on October 14: the Head of Electoral and Emerging Risk for Facebook’s Trust and Safety reacted by noting that it was only “482 hours to first polls close.”⁴⁰



(7/15/2020 12:17:05 PDT):
 >But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG to plan for it.



“But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG [the U.S. Government] to plan for it.”
 —July 15, 2020, internal messages among Facebook personnel

The FBI has defended its actions as information exchange with private-sector partners to prevent amorphous “foreign malign influence” operations.⁴¹ But if the FBI’s intent was truly to help social media companies combat actual foreign influence operations, the FBI should have shared the single most important fact: the influence-peddling allegations in the *Post* story were based off of real, credible information, including information in the FBI’s possession. The FBI failed to do so. While the FBI eventually conceded that it had no indication that the allegations in the *Post* story were Russian disinformation—only after an FBI agent mistakenly revealed to Twitter that the laptop was “real”—the FBI still withheld the fact that it had seized and authenticated Hunter Biden’s laptop months prior.⁴²

As a result, Twitter and Facebook continued to censor the most significant news story of the election cycle, limiting the reach of allegations of Biden family corruption and ultimately benefitting the Biden-Harris campaign.⁴³ Twitter suppressed the *Post* story by removing links to

⁴⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 11:11 a.m.), *see* Ex. 9.

⁴¹ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, No. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024) at 7.

⁴² Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.), at 83–85.

⁴³ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

it, applying “safety” warnings, and blocking the ability to send it via direct message.⁴⁴ Although Twitter lifted the ban on the story the next day, it continued to suspend the *Post*’s account until October 30.⁴⁵ For a week, Facebook manually demoted the content by 50 percent, substantially reducing the likelihood that users would see it in their feed.⁴⁶ During this week, over 30 million Americans cast their votes in the 2020 election—nearly one-fifth of the final vote total, and far more than the final reported margin of forty-five thousand votes that determined the outcome of the election.⁴⁷

* * *

The roots of the FBI’s 2020 prebunking scheme date back to the 2016 presidential election, after which emerged sensationalized accounts that foreign “disinformation” had affected the integrity of the election. Fueled by left-wing election denialism, a cottage industry of pseudoscientists, think tanks, and university centers sprung up to combat the alleged rise in misinformation and disinformation, which they held responsible for President Trump’s victory. The FBI formed the Foreign Influence Task Force to coordinate with social media companies and prevent alleged foreign disinformation from reaching American voters. These entities worked together and with social media companies to censor speech—disproportionately conservative speech—all in the name of stopping disinformation and, ironically enough, promoting democracy.

The FBI’s prebunking of allegations of Biden family influence peddling in the closing weeks of the 2020 presidential election was merely a continuation of its earlier efforts to stop President Trump. This is the same FBI that abused its foreign surveillance authorities to spy on President Trump’s campaign in 2016.⁴⁸ This is the same FBI that fabricated evidence to support warrantless surveillance on a Trump campaign associate.⁴⁹ This is the same FBI where senior officials bragged about an “insurance plan” to prevent Donald Trump from becoming president and promised each other they would “stop” him.⁵⁰ This is the same FBI that has purged conservative agents from its ranks and asked employees whether their colleagues are supporters

⁴⁴ Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/1598822959866683394>.

⁴⁵ Bruce Golding, *How tweet it is: Twitter backs down, unlocks Post’s account*, N.Y. POST (Oct. 30, 2020).

⁴⁶ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 117; Internal messages among Facebook personnel (Oct. 14, 2020, 11:05 a.m.), *see* Ex. 7; *see also* Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), Ex. 101.

⁴⁷ *See* Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020); James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELS. (Dec. 15, 2020); Paul Waldman, *We came much closer to an election catastrophe than many realize*, WASH. POST (Nov. 18, 2020).

⁴⁸ *See* Bill Rivers, *FBI abuses in domestic surveillance of the Trump campaign eerily echo Red Scare raids*, NBC NEWS (Jan. 10, 2020); *Trump Really Was Spied On*, WALL ST. J. (Feb. 14, 2022).

⁴⁹ Press Release, U.S. Attorney’s Office, Dist. of Conn., FBI Attorney Admits Altering Email Used for FISA Application During “Crossfire Hurricane” Investigation (Aug. 19, 2020), <https://www.justice.gov/usao-ct/pr/fbi-attorney-admits-altering-email-used-fisa-application-during-crossfire-hurricane>.

⁵⁰ John Bowden, *FBI agent in texts: ‘We’ll stop’ Trump from becoming president*, THE HILL (June 14, 2018); Jim Geraghty, *Why Did Two FBI Officials Discuss an ‘Insurance Policy’ In Case of Trump’s Election?*, NAT. REVIEW (Dec. 14, 2017).

of President Trump.⁵¹ The FBI's protestations that it is not biased against conservatives ring hollow when it actively suppressed true and explosive allegations concerning the family of the Democrat nominee for president in 2020.

It is impossible to know what would have happened if the FBI had not prebunked the allegations about Biden family influence peddling. But it is unquestionable that the FBI's actions influenced the 2020 presidential election. And it cannot happen again.

⁵¹ See Josh Christenson, *FBI abuses security clearance to 'purge' conservatives, views them as 'unworthy' of employment: whistleblower*, N.Y. POST (July 2, 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, FBI WHISTLEBLOWER TESTIMONY HIGHLIGHTS GOVERNMENT ABUSE, MISALLOCATION OF RESOURCES, AND RETALIATION (Comm. Print May 18, 2023).

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS	10
I. Background.....	11
II. After the FBI obtained the laptop with information on Biden family corruption in late 2019, the FBI began to condition Big Tech to incorrectly treat it as Russian disinformation.....	13
A. The FBI case team that possessed and authenticated Hunter Biden’s laptop in late 2019 briefed the FITF about the laptop months before the <i>Post</i> story.	15
B. The FBI and Big Tech met 30-plus times in 2020 to discuss a potential “hack and leak” while Big Tech privately laughed about “influenc[ing] the 2020 elections.”.....	17
1. FITF Bilateral Meetings.....	18
2. USG-Industry Meetings.....	19
C. The FBI specifically warned Big Tech about a Russian hack-and-leak operation in fall 2020 involving “Burisma” and the Biden family.	24
D. Social media companies changed their policies on hacked materials and started “inoculating” the public for a “hack and leak.”	32
1. Facebook.....	32
2. Google.....	36
3. Twitter.....	37
E. The Aspen Institute hosted a tabletop exercise for Big Tech companies about a potential Russian hack-and-leak scenario involving the Bidens and Burisma.	38
III. Big Tech censored the true story, and the FBI hid key information, while millions voted.....	40
A. Big Tech quickly censored the true <i>New York Post</i> story, believing it was “exactly” what the FBI had warned about for months.....	41
B. Big Tech reached out to the FBI and the FBI hid key information.	46
1. The Twitter-FITF Bilateral Meeting.....	46
2. The FBI’s Internal Deliberations	48
3. The Facebook-FITF Bilateral Meeting	50
4. The USG-Industry Meeting	52
5. The FITF’s Follow-Up Discussions	53
C. Despite a lack of evidence, Big Tech continued to censor the story because of concerns about a potential Biden-Harris Administration.....	55
1. Facebook.....	55
2. Twitter.....	62
3. Other companies	65
D. FBI continued to withhold information as Big Tech continued to reach out.....	67
IV. Epilogue: The fight against FBI election interference continues.....	71
V. Appendix.....	76

I. Background

“Hack & Leak[.] FBI tipped us all off last week that this Burisma story was likely to emerge, and today’s call indicated that.”

—Oct. 14, 2020, 3:27 p.m. ET, internal notes from Microsoft summarizing a “USG-Industry” meeting on the day the *New York Post* published the story on the Biden family’s influence peddling.⁵²

As the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have revealed, following the 2016 election, offices within the Executive Branch launched efforts to covertly censor Americans’ free expression. The FBI formed the Foreign Influence Task Force (FITF) in the fall of 2017.⁵³ The Global Engagement Center (GEC), a multi-agency entity housed within the State Department established by President Obama in early 2016 to counter terrorism,⁵⁴ expanded its mandate in 2017 to include countering foreign disinformation.⁵⁵ Not to be outdone, the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) formed the Countering Foreign Influence Task Force (CFITF) in 2018, which evolved into the “Mis, Dis, and Malinformation (MDM) Team” in 2021 to counter foreign *and American* speech.⁵⁶

Once the Biden-Harris Administration took power, these censorship efforts only further expanded. Senior members of the Biden-Harris White House immediately began a months-long pressure campaign on Facebook, YouTube, Amazon, and other companies to censor views disfavored by the Biden-Harris Administration.⁵⁷ The Office of the Director of National Intelligence (ODNI) launched ODNI’s Foreign Malign Influence Center in 2021.⁵⁸ DHS created the Orwellian Disinformation Governance Board in May 2022.⁵⁹ And CISA built out and met

⁵² Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

⁵³ *Combatting Foreign Influence*, FEDERAL BUREAU OF INVESTIGATION, <https://www.fbi.gov/investigate/counterintelligence/foreign-influence> (last visited Oct. 18, 2024).

⁵⁴ Exec. Order No. 13,721, 81 C.F.R. 14943 (2016).

⁵⁵ *The Global Engagement Center: Leading the United States Government’s Fight Against Global Disinformation Threat: Hearing Before the Subcomm. on State Dep’t and USAID Management, Int’l Operations, and Bilateral Int’l Development of the S. Comm. on Foreign Rels.*, 116th Cong. (Mar. 5, 2020).

⁵⁶ 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); *see also* 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).

⁵⁷ STAFF OF H. COMM. ON THE JUDICIARY & SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, *THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITIC OF THE BIDEN ADMINISTRATION*, (Comm. Print May 1, 2024).

⁵⁸ *Organization*, NAT’L COUNTERTERRORISM CENTER, <https://www.dni.gov/index.php/nctc-who-we-are/organization/340-about/organization/foreign-malign-influence-center> (last visited Oct. 18, 2024).

⁵⁹ Amanda Seitz, *Disinformation board to tackle Russia, migrant smugglers*, ASSOCIATED PRESS (Apr. 28, 2022).

with its MDM Advisory Subcommittee—featuring Big Tech executives and disinformation pseudo-scientists—throughout 2022.⁶⁰

The Executive Branch also began colluding with private and academic institutions on censorship during this period. The Committee and Select Subcommittee’s oversight of the censorship-industrial complex has revealed how a consortium of “disinformation” academics led by Stanford University’s Stanford Internet Observatory (SIO), called the Election Integrity Partnership (EIP), worked directly with CISA and the GEC to monitor and censor Americans’ online speech in advance of the 2020 presidential election.⁶¹ Created in the summer of 2020 “at the request of DHS/CISA,”⁶² the EIP enabled the federal government to launder its censorship activities through a university in hopes of bypassing both the First Amendment and public scrutiny.⁶³

This constellation of censorship organizations, alongside Big Tech, worked overtime to nominally “secure” the 2020 election from foreign interference.⁶⁴ In reality, this meant censoring election-related speech, including questions about the validity of unrestricted mail-in voting.⁶⁵ And it also meant “inoculating” the public against damaging stories about Biden family influence peddling.⁶⁶

⁶⁰ 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).

⁶¹ 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).

⁶² Email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 p.m.); *see* Ex. 123.

⁶³ *See* STAFF OF H. COMM. ON THE JUDICIARY & SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV’T OF THE H. COMM. ON THE JUDICIARY, THE WEAPONIZATION OF ‘DISINFORMATION’ PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ FREE SPEECH (Comm. Print Nov. 6, 2023).

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

II. After the FBI obtained the laptop with information on Biden family corruption in late 2019, the FBI began to condition Big Tech to incorrectly treat it as Russian disinformation

“We have recently received indications from USG partners that they believe there is a risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma. Timing for something like this is uncertain, but could happen as soon as the first presidential debate on September 29th.”

—Sept. 21, 2020, 2:04 p.m. ET, internal Facebook email about a potential Russian hack-and-leak threat.⁶⁷

In 2019, the FBI obtained a hard drive from a laptop attributed to Hunter Biden.⁶⁸ Gary Shapley, an IRS whistleblower who spent years overseeing a tax evasion case against Hunter Biden, testified that by November 2019, the FBI had “verified [the laptop’s] authenticity” by “matching the device number against Hunter Biden’s Apple iCloud ID.”⁶⁹

As the *New York Post* later detailed, the laptop contained evidence of a variety of crimes, including extensive evidence of broad influence peddling schemes committed by the Biden family and Biden family business associates.⁷⁰ The laptop also included evidence of Hunter Biden’s use of illegal drugs while engaging in other illicit activities.⁷¹ The laptop has since been used as evidence in Hunter Biden’s recent felony conviction on federal gun charges.⁷²

In 2020, just a few months after the FBI authenticated Hunter Biden’s laptop, it began a months-long campaign to “prebunk” a potential news story about the laptop’s contents, conditioning Big Tech platforms to falsely believe that Hunter Biden and his shady business dealings with the Ukrainian oil company Burisma would be the subject of the next Russian hack-and-leak operation.⁷³ A hack-and-leak operation is when an actor obtains information from a hacking campaign, then releases, or “leaks,” that information via social media or other means for public consumption.

⁶⁷ *Id.*

⁶⁸ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12; see also Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024); Ingrid Jacques, *Trump right about Hunter’s ‘laptop from hell,’ though Biden claimed Russian disinformation*, USA TODAY (June 6, 2024); Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020).

⁶⁹ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12.

⁷⁰ See Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. POST (Oct. 14, 2020).

⁷¹ *Id.*

⁷² Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024).

⁷³ See, e.g., Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), Ex. 1.

The FBI raised warnings about a potential hack-and-leak operation in meetings between the FBI’s Foreign Influence Task Force (FITF) and Big Tech companies. The FBI first began meeting with Big Tech companies during the 2018 election cycle to share information about potential foreign influence operations for which platforms should be on the lookout.⁷⁴ In 2020, the FBI began raising specific warnings about a potential Russian hack and leak of information related to the Biden family—namely Hunter Biden—and Burisma, which would appear through authentic news sources.⁷⁵

By September 2020, many platforms had actively prepared to address this specific potential hack-and-leak scenario. On September 1, 2020, Google began enforcing a new policy specifically designed to curtail the distribution of hacked political materials.⁷⁶ Later in the month, Facebook made an “inoculating announcement” to “mitigate the impact of such a leak if it does occur,”⁷⁷ and then changed its hack-and-leak policies in October “to ensure we are prepared for foreign-backed leak operations that may develop in the weeks to come.”⁷⁸ Also in September 2020, representatives from the country’s largest platforms, including many who were regularly attending FITF meetings, participated in a tabletop exercise—a meeting where participants engage with a hypothetical scenario and offer potential responses and solutions to the hypothetical problems—set up by the Aspen Institute to wargame a response to a potential scenario involving leaked documents concerning Hunter Biden’s work with Burisma.⁷⁹

By the time the *Post* published its story on Biden family influence peddling on October 14, 2020, Big Tech platforms had (1) been thoroughly primed to view the story as a Russian hack-and-leak influence operation; (2) developed and implemented new protocols for handling content relating to a potential hack and leak; and (3) brainstormed and practiced their new responses in tabletop exercises with other platforms and news outlets in the months prior.

Although the FBI conditioned Big Tech to believe any allegations about Hunter Biden were Russian disinformation, the social media companies are far from blameless. Internal messages obtained by the Committee and Select Subcommittee show that personnel at the social media platforms knew the dangerous consequences of their censorship decisions. In one message thread from July 2020, a member of Facebook’s Trust and Safety team said that when Facebook employees inevitably “get hauled up to the hill to testify on why we influenced the 2020 elections,” they would be able to say that they had “been meeting for YEARS with USG to plan for it.”⁸⁰

⁷⁴ Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

⁷⁵ Internal messages among Facebook personnel (Sept. 20, 2020, 6:26 p.m.), *see* Ex. 13; Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

⁷⁶ *Hacked political materials policy global roll-out (November 2020)*, GOOGLE (Sept. 1, 2020), <https://support.google.com/adspolicy/answer/9991623>.

⁷⁷ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

⁷⁸ Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), *see* Ex. 75.

⁷⁹ *See infra* Section II.E; Email from Aspen Digital staff to Roundtable participants (Sept. 1, 2020, 7:44 p.m.), Ex. 99; *see also* Aspen Digital Hack-and-Dump Scenario Outline (Sept. 2020), Ex. 100.

⁸⁰ Internal messages among Facebook personnel (July 15, 2020, 3:17 p.m.), *see* Ex. 10.



(7/15/2020 12:17:05 PDT):
 >But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG to plan for it.



“But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG [the U.S. Government] to plan for it.”

—July 15, 2020, internal messages among Facebook personnel

These messages show that, while Big Tech may not have known that the FBI was priming them to censor a true story, they understood that their meetings with the U.S. government regarding online speech could very well influence the 2020 election.

A. The FBI case team that possessed and authenticated Hunter Biden’s laptop in late 2019 briefed the FITF about the laptop months before the *Post* story.

In late 2019, during the course of an ongoing investigation, the FBI seized and authenticated the hard drive of the laptop attributed to Hunter Biden, the subject of the October 14, 2020 *New York Post* article.⁸¹

Evidence obtained by the Committee and Select Subcommittee shows that the FBI case team was in contact with the FITF months prior to the *New York Post* story. The FBI Special Agent who served as the FITF’s Russia Unit Chief from mid-2019 to June 2021 testified that he received “three to five briefings” on the case because the Hunter Biden investigation was linked to Ukraine, which fell under the purview of the Russia Unit.⁸² The FITF Russia Chief further

⁸¹ Transcribed Interview of Gary Shapley, H. Comm. on Ways and Means (May 26, 2023) (on file with Comm.) at 12; see also Marshall Cohen & Holmes Lybrand, *Special counsel plans to use infamous Hunter Biden laptop as evidence at gun trial*, CNN (May 22, 2024); Ingrid Jacques, *Trump right about Hunter’s ‘laptop from hell,’ though Biden claimed Russian disinformation*, USA TODAY (June 6, 2024).

⁸² Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024), (on file with the Comm.) at 28-29.

testified that he first learned that the FBI was in possession of a laptop attributed to Hunter Biden in one of these briefings before the *Post* article was published.⁸³ Similarly, an FBI Criminal Investigative Division analyst detailed to the FITF in 2020 testified that he learned about the existence of the Hunter Biden investigation “a few months before” October 14, when he received an internal FBI document confirming it, though he did not learn about the laptop until the morning the *Post* article broke.⁸⁴

The FITF Russia Unit Chief’s testimony that members of the FITF knew that the FBI was in possession of Hunter Biden’s authenticated laptop prior to the *Post* story is consistent with other testimony received by the Committee and Select Subcommittee.⁸⁵ Laura Dehmlow, then-China Unit Chief of the FITF and now the Section Chief of the FITF, testified that she and others knew that the FBI was in possession of the laptop well before October 14, 2020.⁸⁶ Dehmlow testified to the Committee:

Q. When the information was relayed to you following the Twitter call that the first agent had said the laptop was real, just to clarify, you knew prior to that conversation that the laptop was real. Is that correct?

A. I did, yes.

Q. But you don’t recall when approximately you learned.

A. I don’t, sorry.

Q. Sitting here today, do you know when the FBI first determined that the laptop was real?

A. I don’t. I know that there is some information in the public record regarding when the FBI acquired the laptop, but I don’t, sitting here, remember that date.

Q. Do you know who else at FITF knew that the laptop was real?

A. I don’t actually. I would assume both my – yes, I would certainly say that Brad Benavides [then-Section Chief of the FITF] was aware.⁸⁷

⁸³ *Id.*

⁸⁴ Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 89-90.

⁸⁵ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.); Transcribed Interview of the Assistant Section Chief of the FITF, H. Comm. on the Judiciary (Apr. 24, 2024) (on file with Comm.); Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.).

⁸⁶ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 35-37.

⁸⁷ Even though two of the three FITF unit chiefs and the Assistant Section Chief testified that they knew that the FBI was in possession of the laptop in advance of the *Post* publishing its report, then-Section Chief Brad Benavides testified that he did not know the FBI was in possession of the laptop prior to the story. See Transcribed Interview of Bradley Benavides, H. Comm. on the Judiciary (Sept. 28, 2023) (on file with Comm.) at 146-160.

Q. What about the individuals on the Russia unit?

A. I would assume the unit chief was also aware. I'm pretty certain of that fact.

Q. For the individual --

DOJ Counsel: Just to clarify, do you know to a certainty that they were aware, or are you just making deductions?

A. I'm pretty certain that they were aware.⁸⁸

This testimony confirms that senior personnel of the FITF, the FBI task force providing warnings to Big Tech about a potential Russian hack-and-leak operation involving Hunter Biden and Burisma, knew that the FBI was in possession of the Hunter Biden laptop well before the *Post* article publicly disclosed the existence of the laptop or the evidence of influence peddling contained therein.

B. The FBI and Big Tech met 30-plus times in 2020 to discuss a potential “hack and leak” while Big Tech privately laughed about “influenc[ing] the 2020 elections.”

Throughout 2020, two parallel tracks emerged for information sharing between government agencies and Big Tech. In “FITF Bilateral Meetings,” FBI FITF staff would meet with individual social media platforms to discuss a number of topics, generally relating to ongoing or anticipated foreign influence operations. In “USG-Industry meetings,” the FBI’s FITF, other federal agencies, and social media companies convened as a large group to share information about potential foreign influence campaigns. Several of the FITF personnel who knew that the laptop was authentic prior to the release of the *New York Post* story attended these large group meetings.⁸⁹ Through both sets of meetings, the U.S. government shared specific warnings of a potential Russian hack-and-leak operation relating to Hunter Biden and Burisma, priming social media platforms to censor the *Post* story when it broke on October 14, 2020.⁹⁰

⁸⁸ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023), (on file with the Comm.), at 37.

⁸⁹ See, e.g., USG-Industry meeting invitation (Apr. 20, 2022, 6:00 p.m.), Ex. 45; USG-Industry meeting invitation (May 13, 2020, 4:00 p.m.), Ex. 47; USG-Industry meeting invitation (June 10, 2020, 6:00 p.m.), Ex. 51; USG-Industry meeting invitation (July 8, 2020, 6:00 p.m.), Ex. 71; USG-Industry meeting invitation (July 15, 2020, 6:00 p.m.), Ex. 57; USG-Industry meeting invitation (Aug. 12, 2020, 6:00 p.m.), Ex. 59; USG-Industry meeting invitation (Sept. 9, 2020, 6:00 p.m.), Ex. 72; USG-Industry meeting invitation (Sept. 16, 2020, 6:00 p.m.), Ex. 64; USG-Industry meeting invitation (Oct. 7, 2020, 6:00 p.m.), Ex. 68; USG-Industry meeting invitation (Oct. 14, 2020, 6:00 p.m.), Ex. 27; USG-Industry meeting invitation (Oct. 21, 2020, 6:00 p.m.), Ex. 73; USG-Industry meeting invitation (Oct. 28, 2020, 6:00 p.m.), Ex. 74.

⁹⁰ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), see Ex. 1; see also Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

1. FITF Bilateral Meetings

From February 10, 2020 to October 14, 2020, the FBI’s FITF met over two dozen times with Google, Twitter, Facebook, Microsoft, and other companies in one-on-one “FITF Bilateral Meetings”—including individual meetings with Facebook and Twitter on October 14, 2020, the day that the *Post* story published.⁹¹ These bilateral meetings have restarted in 2024.⁹²

FBI agents—typically Elvis Chan, Assistant Special Agent in Charge of the FBI’s San Francisco Field Office—scheduled FITF bilateral meetings with social media companies quarterly, with additional calls or meetings on an ad hoc basis.⁹³ Because the FBI would share technical threat intelligence and analysis, the social media platforms’ threat intelligence teams would generally be responsible for attending and participating in the FITF bilateral meetings.⁹⁴

While the FITF primarily shared technical, actor-focused information with Big Tech companies in these meetings, it also discussed high-level strategies and themes employed by foreign actors.⁹⁵ The Russia Unit Chief of the FITF testified that he was “certain” there was discussion of a potential “hack-and-leak” threat from Russia during these meetings.⁹⁶ He explained that in the FITF bilateral meetings, “we often talked about tactics that had happened in the past.”⁹⁷ Because “larger cyber actors” like Russia had shown a propensity for this kind of

⁹¹ See, e.g., Email from Elvis Chan to Yahoo personnel (Jan. 3, 2020, 3:46 p.m.), Ex. 19; Email from Elvis Chan to LinkedIn personnel (Jan. 3, 2020, 3:48 p.m.), Ex. 18; Email from Elvis Chan to Google personnel (Jan. 6, 2020, 8:25 p.m.), Ex. 15; Email from Elvis Chan to Yahoo personnel (Apr. 13, 2020, 4:15 p.m.), Ex. 20; Email from Elvis Chan to LinkedIn personnel (Apr. 13, 2020, 11:21 p.m.), Ex. 24; Email from Elvis Chan to Google personnel (Apr. 14, 2020, 9:51 p.m.), Ex. 21; Email from Elvis Chan to Facebook personnel (May 12, 2020, 5:29 p.m.), Ex. 22; Email from Elvis Chan to Google personnel (July 14, 2020, 10:59 a.m.), Ex. 26; Email from Elvis Chan to LinkedIn personnel (July 14, 2020, 11:02 a.m.), Ex. 31; Email from Elvis Chan to Yahoo personnel (July 14, 2020, 1:58 p.m.), Ex. 28; Email from Elvis Chan to Facebook personnel (July 16, 2020, 10:10 p.m.), Ex. 29; Email from Elvis Chan to Google personnel (Sept. 10, 2020, 2:13 p.m.), Ex. 33; Email from Elvis Chan to LinkedIn personnel (Sept. 10, 2020, 2:13 p.m.), Ex. 37; Email from Elvis Chan to Facebook personnel (Sept. 10, 2020, 5:12 p.m.), Ex. 36; Email from Elvis Chan to Yahoo personnel (Sept. 14, 2020, 5:21 p.m.), Ex. 34; Email from Elvis Chan to Google personnel (Sept. 29, 2020, 11:04 a.m.), Ex. 39; Email from Elvis Chan to Google personnel (Sept. 29, 2020, 11:04 a.m.), Ex. 40; Email from Elvis Chan to Yahoo personnel (Sept. 29, 2020, 11:09 a.m.), Ex. 70; Email from Elvis Chan to Reddit personnel (Sept. 29, 2020, 11:10 a.m.), Ex. 69; Email from Elvis Chan to LinkedIn personnel (Sept. 29, 2020, 2:08 p.m.), Ex. 41; Email from Elvis Chan to Facebook personnel (Oct. 4, 2020, 2:31 p.m.), Ex. 16; see also Ex. 42 (Emails from FBI to Big Tech participants scheduling FITF Bilateral meetings).

⁹² Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

⁹³ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with the Comm.) at 22-23; Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 25.

⁹⁴ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 143.

⁹⁵ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, NO. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024) at 17-18.

⁹⁶ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 21.

⁹⁷ *Id.*

campaign in the past via other hack-and-leak operations, “that’s certainly one of the tactics [the FITF] discussed” with social media companies.⁹⁸

Occasionally, Big Tech’s policy staff attended these bilateral meetings for awareness of the matters under discussion.⁹⁹ For example, the Russia Unit Chief specifically remembered that the Facebook employee who developed an updated hack-and-leak policy for the platform (and subsequently briefed CEO Mark Zuckerberg on these changes) sometimes attended FITF-Facebook bilateral meetings.¹⁰⁰ In Elvis Chan’s *Murthy v. Missouri* deposition, he confirmed that in bilateral meetings, the FBI discussed platforms’ policies regarding hacked materials and how the policies might apply to potential foreign influence operations.¹⁰¹

2. USG-Industry Meetings

A second set of standing meetings occurred among several government stakeholders (including the FBI, DOJ, CISA, DHS’s Office of Intelligence & Analysis, and ODNI) and a group of industry participants from many different companies (including Facebook, Google, Twitter, and Microsoft, among others). Based on the documents the Committee and Select Subcommittee have obtained, the first USG-Industry meeting for the 2020 election occurred no later than April of 2020.¹⁰² These meetings continued on a monthly—and then, as the election drew nearer, weekly—basis in the lead-up to the 2020 election, including on October 14, 2020—the day the *Post* story broke.¹⁰³ In 2024, CISA and the FBI resumed meetings with Big Tech.¹⁰⁴

The USG-Industry meetings were a regular forum for federal agencies and social media companies to exchange high-level information about foreign threats. Meeting agendas and other

⁹⁸ *Id.*

⁹⁹ *Id.* at 143-145.

¹⁰⁰ *Id.* at 145; *see e.g.*, Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), Ex. 75.

¹⁰¹ *Murthy v. Missouri*, No. 3:22-cv-01213, 2023 WL 43352270 (WD La. July 4, 2023) (Deposition of Elvis Chan), at 203-206.

¹⁰² USG-Industry meeting invitation (Apr. 20, 2020, 6:00 p.m.), *see* Ex. 45.

¹⁰³ *See, e.g.*, Email from CISA personnel to industry participants (May 12, 2020, 9:12 a.m.), Ex. 46; USG-Industry meeting invitation (May 13, 2020, 4:00 p.m.), Ex. 47; Internal Facebook readout of USG-Industry meeting (May 14, 2020, 11:31 a.m.), Ex. 48; Agenda emails between industry participants (June 9, 2020, 1:45 p.m.), Ex. 49; Scheduling email from Facebook personnel to industry group (June 9, 2020, 8:45 p.m.), Ex. 50; Internal Facebook readout of the USG-Industry meeting (June 10, 2020, 8:35 a.m.), Ex. 53; USG-Industry Meeting invitation (June 10, 2020, 6:00 p.m.), Ex. 51; Internal messages among Facebook personnel (June 30, 2020, 6:31 p.m.), Ex. 52; Internal messages among Facebook personnel (July 1, 2020, 4:14 p.m.), Ex. 54; Internal messages among Facebook personnel (July 10, 2020, 5:12 a.m.), Ex. 55; Scheduling email from Google personnel to industry group (July 14, 2020, 10:13 p.m.), Ex. 27; USG-Industry Meeting invitation (July 15, 2020, 6:00 p.m.), Ex. 57; Internal Facebook readout of the USG-Industry meeting (July 17, 2020, 7:17 a.m.), Ex. 58; USG-Industry Meeting invitation (Aug. 12, 2020, 6:00 p.m.), Ex. 59; Internal Facebook readout of the USG-Industry meeting (Aug. 13, 2020, 5:58 a.m.), Ex. 60; Agenda emails between CISA and Facebook personnel (Sept. 9, 2020, 11:41 a.m.), Ex. 66; Agenda emails between industry participants (Sept. 11, 2020, 12:40 p.m.), Ex. 61; Scheduling email from Facebook personnel to industry group (Sept. 11, 2020, 1:00 p.m.), Ex. 62; Agenda emails between CISA and Facebook personnel (Sept. 15, 2020, 8:06 a.m.), Ex. 63; USG-Industry Meeting invitation (Sept. 16, 2020, 6:00 p.m.), Ex. 64; Internal Facebook notes about USG-Industry meeting (Sept. 16, 2020), Ex. 65; Agenda emails between CISA and Facebook personnel (Oct. 5, 2020, 6:41 a.m.), Ex. 67; USG-Industry Meeting invitation (Oct. 7, 2020, 6:00 p.m.), Ex. 68.

¹⁰⁴ David DiMolfetta, *CISA, FBI resuming talks with social media firms over disinformation removal, Senate Intel chair says*, NEXTGOV/FCW (May 7, 2024).

documents obtained by the Committee and Select Subcommittee show that the federal agencies and Big Tech repeatedly discussed “Hack/Leak” in the meetings leading up to the 2020 election.

For example, a meeting on July 15, 2020, included “Hack/Leak and USG Attribution Speed/Process” as an agenda item listed under the heading “Deep Dive Topics.”¹⁰⁵

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]69D>

To: [REDACTED]@google.com; [REDACTED]@google.com; [REDACTED]@twitter.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@linkedin.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com; [REDACTED]@google.com; [REDACTED]@reddit.com; [REDACTED]@pinterest.com; [REDACTED]@pinterest.com; [REDACTED]@medium.com; [REDACTED]; [REDACTED]; [REDACTED]@microsoft.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]; [REDACTED]@twitter.com; [REDACTED]@wikimedia.org; [REDACTED]@reddit.com; [REDACTED]@medium.com; [REDACTED]@twitter.com; [REDACTED]@linkedin.com; [REDACTED]@linkedin.com; [REDACTED]; [REDACTED]@verizonmedia.com

CC: [REDACTED]; [REDACTED]

Sent: 7/14/2020 3:11:43 PM

Subject: Dial In Information: 7/15 Monthly USG | Industry Call

Hello Everyone,

Three quick updates before tomorrow:

- Below please find the WebEx dial-in information for the Wednesday, 7/15 USG/Industry call.
- Starting in August onwards, we will migrate to using a BJT for our calls, and that information will be forthcoming.
- Here is the planned agenda (as discussed at our bi-weekly last Friday):
 - 10 minutes: Dial In/Opening
 - 30 minutes: Threat Updates
 - Threat update from USG (FBI, I&A)
 - Threat update from industry (FB, TW, GOOG)
 - 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 - Election process update from USG
 - Hack/Leak and USG Attribution Speed/Process
 - Vote-by-mail: How do we deal with the gap between Nov 3 and results?
 - 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

Thank you for your engagement and commitment here, and look forward to seeing you tomorrow.
USG/Industry Webex meeting.

“Hack/Leak and USG Attribution Speed/Process”
 —July 15, 2020, USG-Industry meeting agenda

¹⁰⁵ USG-Industry meeting agenda (July 14, 2020, 3:11 p.m.), Ex. 76.

In a September 16, 2020, USG-Industry meeting, Big Tech and federal agencies discussed “hack and leak operations” again.¹⁰⁷ Facebook’s internal readout of the meeting explained that the discussion focused on “preparing for ‘hack and leak’ operations attempting to use platforms and traditional media to amplify unauthorized information drops,” among other topics.¹⁰⁸

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 9/17/2020 12:55:58 PM
To: lobbyists [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]
Subject: HPM USG-Industry Monthly Election Integrity Meeting (September)

Team,

Sharing our HPM from this week’s USG-Industry meeting on election integrity and the link to our successfully-landed Joint Industry Statement. Great XFN collaboration on this continues (many thanks to [REDACTED], [REDACTED], [REDACTED] & [REDACTED]).

Let us know if you have any questions.
[REDACTED]

United States: USG-Industry Monthly Election Integrity Meeting (September)

- **What happened:** On Wednesday, September 16, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our i3 Threat Team participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. We again successfully landed a Joint Industry Statement regarding our long-standing and ongoing efforts to secure US2020 in collaboration with the USG entities charged with securing the election, available here: <https://twitter.com/fbnewsroom/status/1306314722082349056?s=20>. Co-signatories included Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia. USG attendees included senior officials from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ’s National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the seventh such convening to prepare for US2020, the fifth call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- **Why relevant:** The discussion focused on timely sharing accurate voting and election information, countering targeted attempts to undermine the election conversation, preparing for “hack and leak” operations attempting to use platforms and traditional media to amplify unauthorized information drops, and mitigation efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.
- **Next Steps:** We will continue to participate in these calls with our tech peers & USG partners through the end of 2020. The next monthly convening will occur on October 7th. We will then transition to weekly calls to check-in & share information through the December 14th Electoral College meeting.

“[P]reparing for ‘hack and leak’ operations”
—Sept. 17, 2020 internal Facebook notes about USG-Industry meeting

¹⁰⁷ USG-Industry Meeting invitation (Sept. 16, 2020, 6:00 p.m.), see Ex. 64.

¹⁰⁸ Internal Facebook readout of USG-Industry meeting (Sept. 17, 2020, 12:55 p.m.), see Ex. 78.

Finally, on October 7, 2020, just one week before the *Post* article on Biden family influence peddling was published, the USG-Industry meeting agenda again included “Hack/Leak concerns” as a topic of discussion.¹⁰⁹

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Monday, October 5, 2020 7:21 AM
To: [REDACTED] <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: October 2020 USG/Industry Meeting (Draft Agenda)

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.

Good morning!

Wanted to follow-up to see if you were ok with the schedule as noted below. If so, we will circulate —as final—with industry today.

Thanks!

Sent from my iPhone

On Sep 29, 2020, at 2:41 PM, [REDACTED] <[REDACTED]@fb.com> wrote:

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!

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

META-118HJC-0000960

[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
 - Election Official Reporting
- **10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)**

“Deep Dive Topics . . . Hack/Leak Concerns”
 —Sept. 29, 2020, USG-Industry meeting draft agenda

¹⁰⁹ USG-Industry meeting draft agenda (Sept. 29, 2020, 2:41 p.m.), *see* Ex. 67.

According to Facebook’s readout, “[t]he discussion focused on efforts to identify and mitigate delegitimization claims against US2020 electoral outcomes, including potential hack/leak scenarios.”¹¹⁰

Message

From: ██████████@fb.com]
Sent: 10/8/2020 10:24:28 AM
To: lobbyists ██████████@fb.com]
CC: ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]
Subject: USG-Industry Monthly Election Integrity Meeting (October)

Team,

Sharing our HPM from this week’s USG-Industry meeting on election integrity. Great XFN collaboration on this continues (many thanks to ██████████, ██████████, ██████████ & ██████████).

Let us know if you have any questions.
██████████

United States: USG-Industry Monthly Election Integrity Meeting (October)

- **What happened:** On Wednesday, October 7, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our i3 Threat Team participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. Participants included Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia. USG attendees included senior officials from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ’s National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the eighth such convening to prepare for US2020, the sixth call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- **Why relevant:** The discussion focused on efforts to identify and mitigate delegitimization claims against US2020 electoral outcomes, including potential hack/leak scenarios, operational readiness of states and localities for administering the vote, and timely election-related information sharing via elections operations.
- **Next Steps:** We will continue to participate in these calls with our tech peers & USG partners through the end of 2020. The meetings will now shift to a weekly 30 minute cadence where we will share information through the December 14th Electoral College meeting.

“The discussion focused on efforts to identify and mitigate...potential hack/leak scenarios”
—Oct. 8, 2020, internal Facebook notes on Oct. 7 USG-Industry meeting

C. The FBI specifically warned Big Tech about a Russian hack-and-leak operation in fall 2020 involving “Burisma” and the Biden family.

According to emails, meeting invitations, and internal readouts of meetings between U.S. government officials and Big Tech employees, foreign influence operations—and hack-and-leak threats specifically—were a recurring topic of discussion among the FBI and social media








¹¹⁰ Internal Facebook readout of USG-Industry meeting (Oct. 8, 2020, 10:24 a.m.), *see* Ex. 80.

companies.¹¹¹ In September 2020, the Big Tech companies participating in these meetings confirmed in a joint press statement that these discussions focused on “[w]ays to counter targeted attempts to undermine the election conversation before, during, and after the election,” including “preparing for possible so-called ‘hack and leak’ operations attempting to use platforms and traditional media to amplify unauthorized information drops.”¹¹²

“For several years, tech companies have worked together, and with U.S. government agencies tasked with protecting the integrity of elections, to counter election threats across our respective platforms. As we approach the November election, we continue to prepare, meet regularly, and share updates on the threats we see. At today’s meeting, we specifically discussed:

1. Ways to help provide real-time, clear information about the voting process and election results given expected logistical disruptions posed by COVID-19.
2. Ways to counter targeted attempts to undermine the election conversation before, during, and after the election. This includes preparing for possible so-called “hack and leak” operations attempting to use platforms and traditional media to amplify unauthorized information drops.
3. Detection efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.

As the global pandemic poses unprecedented challenges for the 2020 U.S. election, we will continue this ongoing communication and close work between industry and U.S. institutions tasked with election security to share key findings and operational insights in the weeks to come.”

FACEBOOK Google   reddit  Microsoft  verizon media  Pinterest  LinkedIn  WIKIMEDIA FOUNDATION

“[W]e specifically discussed...preparing for possible so-called ‘hack and leak’ operations”
—Sept. 2020 statement from tech industry participants in USG-Industry meetings

While Big Tech issued public statements about how it was generally discussing potential hack-and-leak operations with the U.S. government, the discussions themselves were more specific. Indeed, according to internal Big Tech documents obtained by the Committee and Select Subcommittee, the FBI told Big Tech to expect a “hack/leak operation” that almost exactly matched the details of the *New York Post* reporting on Biden family influence peddling.¹¹³ The FBI got the date and the contents right: it repeatedly warned that the supposed hack-and-leak operation would come right before the election, likely as “an October surprise,”¹¹⁴ and that it would reveal “evidence” regarding “links between the Biden family and Ukraine,”

¹¹¹ See, e.g., USG-Industry meeting agenda (July 14, 2020, 3:11 p.m.), Ex. 76; Internal Facebook readout of USG-Industry meeting (Sept. 17, 2020, 12:55 p.m.), Ex. 78; USG-Industry meeting draft agenda (Sept. 29, 2020, 2:41 p.m.), Ex. 67; Internal Facebook readout of USG-Industry meeting (Oct. 8, 2020, 10:24 a.m.), Ex. 80.

¹¹² Statement from tech industry participants, see Ex. 11; see also Internal messages among Facebook personnel (Aug. 5, 2020), Ex. 12; Emails among tech industry participants (Sept. 15, 2020), Ex. 124.

¹¹³ See, e.g., Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), Ex. 1; Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), Ex. 3; see also Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

¹¹⁴ Internal message from Facebook personnel to Nick Clegg (Oct. 15, 2020, 9:29 a.m.), see Ex. 2.

including the oil company “Burisma.”¹¹⁵ In fact, the week before the *Post* story broke on October 14, the “FBI tipped [Big Tech] off” that “this Burisma story was likely to emerge.”¹¹⁶

Documents obtained by the Committee and Select Subcommittee show that Big Tech got the message loud and clear. One Facebook employee predicted that “in the next few weeks” there would be “leaks about Biden’s supposed link to Burisma.”¹¹⁷ This employee wrote that while Facebook would not “be able to prove” that these were hacks, the company would “have responsible USG players publicly saying this is part of a foreign influence operation,” and that their “secret squirrel partners”—apparently referring to U.S. government officials—would also say it was a Russian operation.¹¹⁸ He conceded that there would not be a “public smoking gun to prove” that the leaks were Russian operations, but that “the circumstantial public evidence will be quite strong.”¹¹⁹ Facebook employees even discussed how the company’s policies might apply to different scenarios that “provide precedent for how [Facebook] would analyze the dissemination of materials that may result from a hack of Burisma” and how to brief leadership on their options.¹²⁰

The statement proved prescient. Once the *Post* story was published just a few weeks later, Facebook’s “secret squirrel partners” did exactly what the platform expected.¹²¹ Fifty-one former intelligence community officials organized by Antony Blinken and the Biden campaign falsely claimed that the story bore “all the classic earmarks of a Russian information operation.”¹²² All the while, Big Tech censored the story even though it did not (and, of course, could not) prove that the story was Russian disinformation.

¹¹⁵ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

¹¹⁶ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

¹¹⁷ Internal messages among Facebook personnel (Sept. 9, 2020, 2:28 p.m.), *see* Ex. 81.

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ Internal messages among Facebook personnel (Sept. 9, 2020, 2:37 p.m.), *see* Ex. 81.

¹²¹ Internal messages among Facebook personnel (Sept. 9, 2020, 2:28 p.m.), *see* Ex. 81.

¹²² 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 (Comm. Print June 25, 2024); 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 HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS (Comm. Print May 10, 2023); *see also* Brooke Singman, *Biden campaign, Blinken orchestrated intel letter to discredit Hunter Biden laptop story, ex-CIA official says*, FOX NEWS (Apr. 20, 2023).

[REDACTED] (9/19/2020 11:18:55 PDT):
 >In the upcoming cycle, we're actually likely to be reasonably confident, but unable to prove publicly.

[REDACTED] (9/19/2020 11:19:03 PDT):
 >So there is a question of our confidence tolerance.

[REDACTED] (9/19/2020 11:19:15 PDT):
 >But if Russian actors drop a Burisma leak in the next two weeks

[REDACTED] (9/19/2020 11:19:25 PDT):
 >(which is likely & we are actively prepping for it)

[REDACTED] (9/19/2020 11:19:32 PDT):
 >I doubt we'll be able to prove it is hacked.

[REDACTED] (9/19/2020 11:20:34 PDT):
 >It's Snowden versus Podesta, right? Snowden had lawful access to the materials. He unlawfully took them and shared with an unintended audience. Podesta never intentionally shared anything.

[REDACTED] (9/19/2020 11:22:23 PDT):
 >So today we'd leave Snowden materials up but take Podesta materials down. Is that right?

[REDACTED] (9/19/2020 11:22:50 PDT):
 >Or does Snowden's illegality play into our assessment?

[REDACTED] (9/19/2020 11:23:36 PDT):
 >(Setting aside entirely the idea that we're going to know anything about any of this at the moment the materials appear on FB.)

[REDACTED] (9/19/2020 11:24:03 PDT):
 >yeah fair question.

[REDACTED] (9/19/2020 11:24:41 PDT):
 >1) I am not sure that Snowden had valid access to what he put out, or at least not all of it, so there would be that question

[REDACTED] (9/19/2020 11:25:09 PDT):
 >2) obviously if there were confidential information, classified or PII would be removed

[REDACTED] (9/19/2020 11:25:49 PDT):
 >3) but yes, there is a delicate balance of whether content leaked (by a whistleblower or otherwise) is allowed...

[REDACTED] (9/19/2020 11:26:45 PDT):
 >Actually, it's Snowden + conclusive evidence that Snowden was in fact controlled by the Russians.

[REDACTED] (9/19/2020 11:26:54 PDT):
 >And the Q is whether those two factors combined are sufficient for us to act.

[REDACTED] (9/19/2020 11:28:05 PDT):
 >We are likely to have in the next few weeks a leak or series of leaks about Biden's supposed link to Burisma, where we won't be able to prove they were "hacked", but where we will have responsible USG players publicly saying this is part of a foreign influence operation, our own assessment will align that this is a Russian op, and we will hear from our trusted secret squirrel partners that this is a Russian op.

[REDACTED] (9/19/2020 11:28:24 PDT):
 >I doubt we'll have a public smoking gun to prove that, but the circumstantial public evidence will be quite strong.

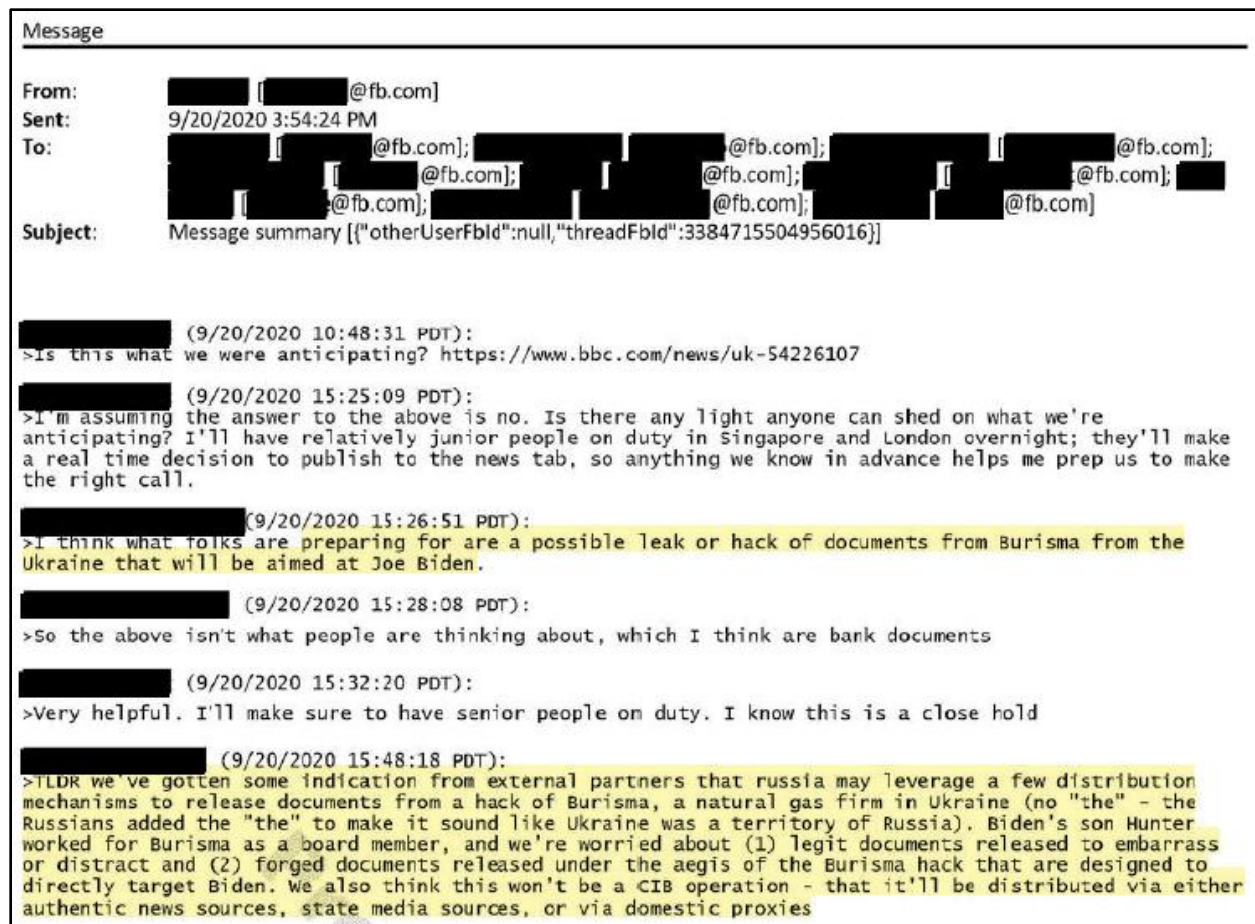
[REDACTED] (9/19/2020 11:29:04 PDT):
 >The Q is whether in that case, we want to be empowered to take stronger action. I could see either (a) removal; or (b) position ourselves to put a label on the content.

“[W]e won't be able to prove they were 'hacked', but . . . we will hear from our trusted secret squirrel partners that this is a Russian op.”

—Sept. 19, 2020, internal messages among Facebook personnel

In a separate exchange of messages between Facebook employees on September 20, 2020, an employee shared a BBC article about a “documents leak” revealing “how Russian

oligarchs have used banks to avoid sanctions,” and asked, “Is this what we were anticipating?”¹²³ Another Facebook employee replied that the BBC article was not the story the company was on the lookout for: “I think what folks are preparing for are a possible leak or hack of documents from Burisma from the Ukraine that will be aimed at Joe Biden.”¹²⁴ Later in the same thread, another Facebook employee added that “we’ve gotten some indication from external partners that Russia may leverage a few distribution mechanisms to release the documents from a hack of Burisma,” and given that “Biden’s son Hunter worked for Burisma as a board member,” the Facebook employee was “worried about (1) legit documents released to embarrass or distract and (2) forged documents released under the aegis of the Burisma hack that are designed to directly target Biden.”¹²⁵ The Facebook employee warned that these would “be distributed via either authentic news sources, state media sources, or via domestic proxies.”¹²⁶



“I think what folks are preparing for are a possible leak or hack of documents from Burisma . . . that will be aimed at Joe Biden”

—Sept. 20, 2020, internal messages among Facebook personnel

¹²³ Internal messages among Facebook personnel (Sept. 20, 2020, 1:48 p.m.), *see* Ex. 13; *FinCEN Files: All you need to know about the documents leak*, BBC (Sept. 21, 2020).

¹²⁴ Internal messages among Facebook personnel (Sept. 20, 2020, 6:26 p.m.), *see* Ex. 13.

¹²⁵ Internal messages among Facebook personnel (Sept. 20, 2020, 6:48 p.m.), *see* Ex. 13.

¹²⁶ *Id.*

The discussion continued with one Facebook employee noting that a leak may be “imminent.”¹²⁷ Another Facebook employee responded, “[we] expect this within the next 1-3 weeks.”¹²⁸ The date of the message—September 20, 2020—was just over three weeks before October 14th, the day that the *New York Post* story was published.

[REDACTED] (9/20/2020 15:50:57 PDT):
>this is extremely helpful to have a head's up on. Thank you. Do we have a sense of timing?

[REDACTED] (9/20/2020 15:51:10 PDT):
>Not yet, unfortunately

[REDACTED] (9/20/2020 15:51:31 PDT):
>the intel we're getting is pretty piecemeal, and my sense is the external folks also don't know whether this will happen, and if so, when

[REDACTED] (9/20/2020 15:51:45 PDT):
>our hypothesis would be that the riskiest period would be right before the first presidential debates

[REDACTED] (9/20/2020 15:51:54 PDT):
>and then the risk rises before each subsequent debate

[REDACTED] (9/20/2020 15:52:33 PDT):
>if we track 2016's wikileaks hack/leak, it could also drop if something damaging came out on the President

[REDACTED] (9/20/2020 15:52:48 PDT):
>the Podesta leaks, for example, were released the same day as the Access Hollywood tape

[REDACTED] (9/20/2020 15:54:01 PDT):
>Ah OK. that makes sense. I thought it was imminent. If there's a discussion underway about how to counter it with responsible news -- i.e. what my team works with -- I'm happy to walk through some options, including how we assess it from a news standpoint in real time once it's released

[REDACTED] (9/20/2020 15:54:15 PDT):
>definitely

[REDACTED] (9/20/2020 15:54:24 PDT):
>I think we'd expect this within the next 1-3 weeks

“I think we’d expect [the hack and leak] within the next 1-3 weeks”

—Sept. 20, 2020, internal messages among Facebook personnel, three weeks before the *New York Post* story on the Biden family’s influence peddling

On September 21, 2020, in a separate email to Facebook leadership, including Facebook’s then-Vice President of Global Affairs Nick Clegg and Vice President of Global Public Policy Joel Kaplan, a Facebook employee stated clearly who specifically was warning Facebook about a Russian hack-and-leak threat involving Burisma and the Biden family in advance of the 2020 election: “USG [U.S. Government] partners.”¹²⁹ In her description of communications with “USG partners,” the Facebook employee wrote that “they [the U.S. government partners] believe there is a high risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma.”¹³⁰ According to the Facebook

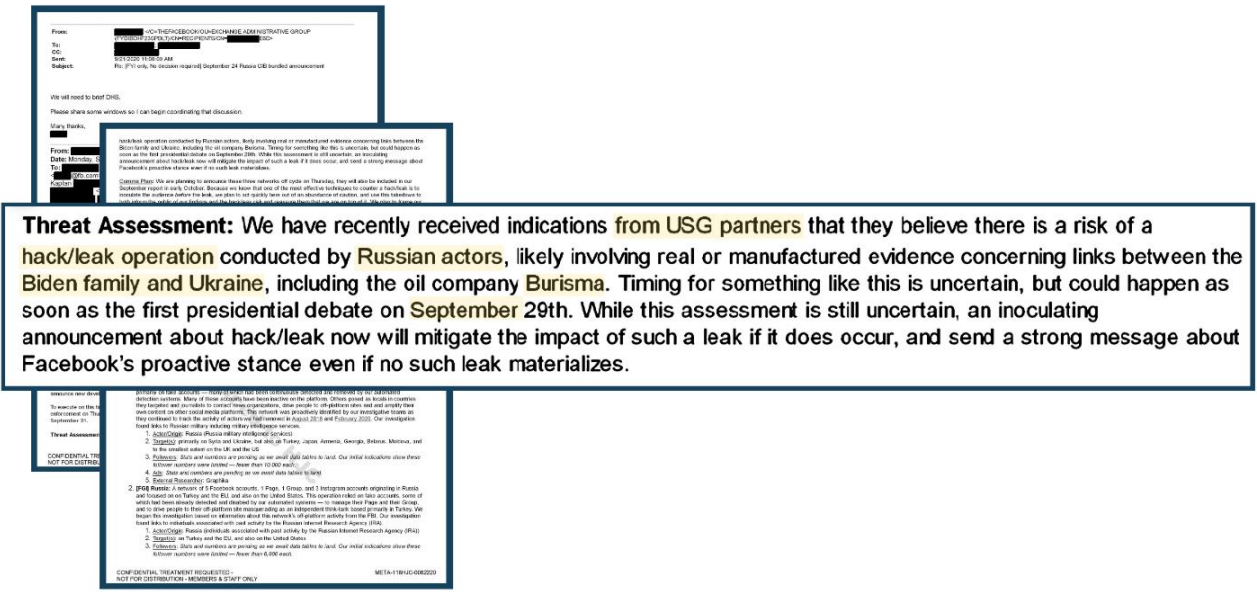
¹²⁷ Internal messages among Facebook personnel (Sept. 20, 2020, 6:54 p.m.), *see* Ex. 13.

¹²⁸ *Id.*

¹²⁹ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

¹³⁰ *Id.*; *see also* Internal messages among Facebook personnel (Sept. 18, 2020, 2:11 p.m.), Ex. 82; Internal messages among Facebook personnel (Sept. 21, 2020, 9:37 a.m.), Ex. 83.

employee, U.S. government “partners” believed that the hack and leak “could happen as soon as the first presidential debate on September 29th.”¹³¹

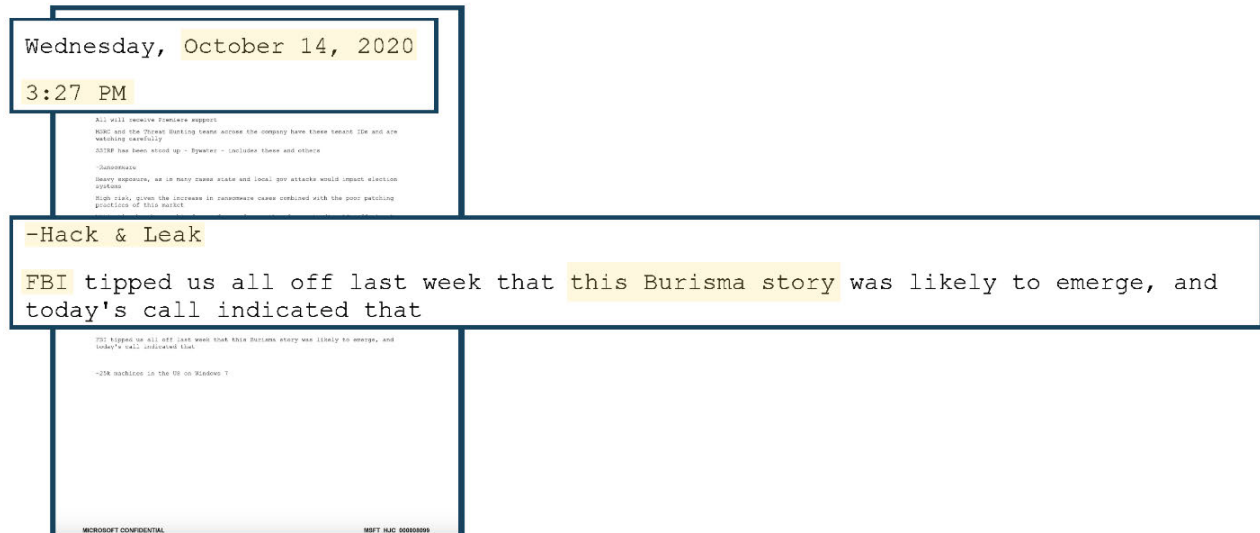


“USG partners . . . believe there is a risk of a hack/leak operation conducted by Russian actors . . . involving . . . evidence concerning links between the Biden family and Ukraine, including the oil company Burisma . . . [that] could happen as soon as the first presidential debate on September 29th”

—Sept. 21, 2020 internal Facebook email to Facebook leadership, including Facebook’s then-Vice President of Global Affairs Nick Clegg and Vice President of Global Public Policy Joel Kaplan

¹³¹ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1; *see also* Internal messages among Facebook personnel (Sept. 18, 2020, 2:11 p.m.), Ex. 82.

Consistent with Facebook’s internal discussions, internal Microsoft notes taken during a USG-Industry meeting on October 14, 2020, confirm that the FBI led the prebunking efforts, stating that the “FBI tipped us all off last week that this Burisma story was likely to emerge, and today’s call indicated that.”¹³²



“FBI tipped us all off last week that this Burisma story was likely to emerge”
 —Oct. 14, 2020, internal Microsoft notes on USG-Industry meeting

These documents confirm that the U.S. government—specifically, the FBI—had not only discussed the possibility of a hack-and-leak operation with Big Tech platforms months before the *Post* story was published, but had also shared specific details, including the type of operation (hack and leak), who the target would be (then-candidate Biden and his family), when it would happen (late September or October 2020), who would orchestrate the leak (Russia), what information would be leaked (the Biden family’s relationship with Burisma), and how the information might be disseminated (via authentic news sources). The FBI shared this information with Big Tech platforms in both bilateral and USG-Industry meetings. As the Committee and Select Subcommittee have learned from witness testimony, multiple FBI personnel assigned to the FITF, the FBI’s task force that provided these “hack-and-leak” warnings, were aware that the FBI had seized and authenticated Hunter Biden’s laptop months prior.¹³³

¹³² Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), see Ex. 3.

¹³³ See Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 28-29; Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 35-37.

D. Social media companies changed their policies on hacked materials and started “inoculating” the public for a “hack and leak.”

In response to the repeated discussions with, and warnings from, the FBI and other federal agencies, platforms began preparing ways to combat an impending hack and leak of information relating to the Bidens and Burisma. Some platforms prepared by attempting to “inoculate the audience *before* the leak,”¹³⁴ while other platforms began to change their content moderation policies to include more strict provisions regarding hacked materials—including changes designed specifically to target hacked political materials.¹³⁵ These efforts by social media platforms to prepare for a potential hack and leak culminated in September 2020, just one month before the *Post* published its story.

1. Facebook

Facebook used public statements to raise awareness about a potential Russian hack-and-leak operation and expanded its hack-and-leak policies to prepare for the potential operation. In September 2020, after receiving “indications from USG partners” that “there is a risk of a hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma,” Facebook determined that the best way to prepare for this potential hack/leak operation was to “inoculate the audience.”¹³⁶

To accomplish this goal of inoculation, Facebook leveraged the announcement of its takedown of three Russian networks perpetrating influence operations around the globe to “both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it.”¹³⁷ Facebook employees described this inoculation—or prebunking—as “one of the most effective techniques to counter a hack/leak.”¹³⁸ Facebook designed the announcement to prime Facebook users to view any pre-election release of damaging information about the Bidens as a Russian hack-and-leak influence operation—much like the FBI was priming social media companies to do.¹³⁹ In September 2020, Facebook believed that “an inoculating announcement about hack/leak now will mitigate the impact of such a leak if it does occur, and send a strong message about Facebook’s proactive stance even if no such leak materializes.”¹⁴⁰

¹³⁴ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1 (emphasis in original).

¹³⁵ Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020, 5:27 p.m.), *see* Ex. 84.

¹³⁶ Internal emails among Facebook personnel (Sept. 21, 2020, 2:04 p.m.), *see* Ex. 1.

¹³⁷ *Id.*; *see also* Email from Facebook personnel to DNI staff (Sept. 24, 2020, 4:16 p.m.), Ex. 85.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

hack/leak operation conducted by Russian actors, likely involving real or simulated evidence concerning links between the White House and Ukraine, including the role of corporate America. Timing for announcing the story is uncertain, but could happen as soon as the first presidential debate in September 2020. While this announcement is off camera, an evening announcement about the hack is now well beyond the point of leak if done now, and sends a strong message about Facebook's position on the hack/leak.

Comms Plan: We are planning to announce these three networks off cycle on Thursday, they will also be included in our September report in early October. Because we know that one of the most effective techniques to counter a hack/leak is to inoculate the audience before the leak, we plan to act quickly here out of an abundance of caution, and use this taken-down to both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it. We plan to frame our public statements carefully to raise awareness, but neither hyperbolize the threat, nor guarantee that such an operation will occur. To land this narrative, we're engaging external researchers and pundits to inform their commentary and raise the importance of responsible coverage of hack/leak operations. We're working to land this story with broadcast and wires to amplify and shape our coverage.

Comms Plan: We are planning to announce these three networks off cycle on Thursday, they will also be included in our September report in early October. Because we know that one of the most effective techniques to counter a hack/leak is to inoculate the audience before the leak, we plan to act quickly here out of an abundance of caution, and use this taken-down to both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it. We plan to frame our public statements carefully to raise awareness, but neither hyperbolize the threat, nor guarantee that such an operation will occur. To land this narrative, we're engaging external researchers and pundits to inform their commentary and raise the importance of responsible coverage of hack/leak operations. We're working to land this story with broadcast and wires to amplify and shape our coverage.

1. [Redacted]

2. [Redacted]

3. [Redacted]

4. [Redacted]

5. [Redacted]

6. [Redacted]

7. [Redacted]

8. [Redacted]

9. [Redacted]

10. [Redacted]

11. [Redacted]

12. [Redacted]

13. [Redacted]

14. [Redacted]

15. [Redacted]

16. [Redacted]

17. [Redacted]

18. [Redacted]

19. [Redacted]

20. [Redacted]

21. [Redacted]

22. [Redacted]

23. [Redacted]

24. [Redacted]

25. [Redacted]

26. [Redacted]

27. [Redacted]

28. [Redacted]

29. [Redacted]

30. [Redacted]

31. [Redacted]

32. [Redacted]

33. [Redacted]

34. [Redacted]

35. [Redacted]

36. [Redacted]

37. [Redacted]

38. [Redacted]

39. [Redacted]

40. [Redacted]

41. [Redacted]

42. [Redacted]

43. [Redacted]

44. [Redacted]

45. [Redacted]

46. [Redacted]

47. [Redacted]

48. [Redacted]

49. [Redacted]

50. [Redacted]

51. [Redacted]

52. [Redacted]

53. [Redacted]

54. [Redacted]

55. [Redacted]

56. [Redacted]

57. [Redacted]

58. [Redacted]

59. [Redacted]

60. [Redacted]

61. [Redacted]

62. [Redacted]

63. [Redacted]

64. [Redacted]

65. [Redacted]

66. [Redacted]

67. [Redacted]

68. [Redacted]

69. [Redacted]

70. [Redacted]

71. [Redacted]

72. [Redacted]

73. [Redacted]

74. [Redacted]

75. [Redacted]

76. [Redacted]

77. [Redacted]

78. [Redacted]

79. [Redacted]

80. [Redacted]

81. [Redacted]

82. [Redacted]

83. [Redacted]

84. [Redacted]

85. [Redacted]

86. [Redacted]

87. [Redacted]

88. [Redacted]

89. [Redacted]

90. [Redacted]

91. [Redacted]

92. [Redacted]

93. [Redacted]

94. [Redacted]

95. [Redacted]

96. [Redacted]

97. [Redacted]

98. [Redacted]

99. [Redacted]

100. [Redacted]

CONFIDENTIAL TREATMENT REQUESTED - NOT FOR DISTRIBUTION - MEMBERS & STAFF ONLY META 1184G-000222

“We know that one of the most effective techniques to counter a hack/leak is to inoculate the audience before the leak”
 —Sept. 21, 2020 internal messages among Facebook personnel

In addition to inoculating its users to anticipate a hack-and-leak operation, Facebook also expanded its hack-and-leak policies. On October 5, 2020, Facebook employees emailed CEO Mark Zuckerberg and COO Sheryl Sandberg to make them “aware of a policy change designed to ensure we are prepared for foreign-backed leak operations that may develop in the weeks to come.”¹⁴¹ The employees explained that the policy change would allow Facebook to “remove any leaked material (whether evidence of a hack exists or not) that is part of a foreign government influence operation.”¹⁴² This was a change from previous policy, which permitted the removal of material resulting from a hack, but allowed leaked content to stay up “because of the significant role of whistleblowers in exposing corruption and empowering accountability throughout history.”¹⁴³ Critically, the Facebook employees told Zuckerberg and Sandberg that the policy had a “narrow focus” and would “only apply to leaks targeting the US 2020 election.”¹⁴⁴

¹⁴¹ Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 5:29 a.m.), see Ex. 75.
¹⁴² *Id.*
¹⁴³ *Id.*
¹⁴⁴ *Id.*

Zuckerberg asked specifically about how the company’s new policy would apply “[i]f a legitimate whistleblower also posts something that a foreign government had leaked.”¹⁴⁸ Other than this one question, he was “supportive” of the policy expansion prior to the *Post* story breaking.¹⁴⁹ A Facebook employee responded that, in that situation, the company “would only remove if the leak was part of a foreign influence operation.”¹⁵⁰

The emails between Zuckerberg and his Facebook team demonstrate how the FBI, specifically the FITF, prompted Facebook to change its content moderation policies. In the months preceding the 2020 presidential election, the FBI’s FITF met with Facebook’s threat intelligence team to warn them of a Russian hack-and-leak operation targeting the 2020 election. Based on these briefings, the threat intelligence team recommended an update to Facebook’s internal policies that would allow the company to remove additional content from the site. Facebook anticipated that the FBI and others would support this change, and Facebook leadership approved the change before its rollout at the beginning of October 2020.

2. Google

Google also developed and implemented new policies prohibiting ads from linking to hacked political materials.¹⁵¹ U.S. enforcement of this new policy began on September 1, 2020—two months before the global policy went into effect.¹⁵² In August 2020, Google staff previewed this shift to employees of the Democratic National Committee (DNC), explaining that “[t]his policy is specifically related to the distribution of hacked political material.”¹⁵³ DNC staff responded approvingly, thanking Google for its “work to reduce the risk and impact of hack-and-dump operations.”¹⁵⁴

¹⁴⁸ Internal email from CEO Mark Zuckerberg to Facebook personnel (Oct. 5, 2020, 1:09 p.m.), *see* Ex. 75.

¹⁴⁹ *Id.*

¹⁵⁰ Internal Facebook email to CEO Mark Zuckerberg and COO Sheryl Sandberg (Oct. 5, 2020, 2:05 p.m.), *see* Ex. 75.

¹⁵¹ *Hacked political materials policy global roll-out (November 2020)*, GOOGLE (Sept. 1, 2020) <https://support.google.com/adspolicy/answer/9991623>.

¹⁵² *Id.*

¹⁵³ Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020, 5:27 p.m.), *see* Ex. 84.

¹⁵⁴ Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020, 9:57 p.m.), *see* Ex. 84.

with the hackers themselves,” and “likely would have restricted the sharing of links related to the hacked materials.”¹⁵⁵ Twitter adopted this policy because it “examined its role in the distribution of [former senior Clinton campaign official] John Podesta’s emails and other hacked materials” that were leaked in 2016.¹⁵⁶ Twitter “reached the conclusion that we [Twitter] needed to have a policy restricting that type of behavior,”¹⁵⁷ and because of concerns raised by the U.S. intelligence community about vulnerabilities that might be exploited in the future.¹⁵⁸ These policies enabled the platform to later censor content based on the FBI’s warnings about a Russian hack and leak in 2020 involving the Bidens and Burisma.¹⁵⁹

E. The Aspen Institute hosted a tabletop exercise for Big Tech companies about a potential Russian hack-and-leak scenario involving the Bidens and Burisma.

Non-governmental third parties, though likely not privy to key information such as the fact that the FBI had Hunter Biden’s laptop, also were part of the prebunking campaign. Most notably, on June 25, 2020, Aspen Digital—a program of the Aspen Institute, a think-tank that has done significant work relating to so-called “information disorder”¹⁶⁰—hosted a “Hack and Leak Roundtable” that included “journalists, ethicists, First Amendment attorneys, and platform executives” for a discussion about “standards and ethics when it comes to publication and coverage in hack and leak scenarios.”¹⁶¹

Documents obtained by the Committee and Select Subcommittee show that Facebook employees who had met with the FITF in 2020 were instrumental in developing and facilitating this roundtable and the subsequent tabletop exercise described below.¹⁶² The roundtable participants discussed how traditional news media and Big Tech platforms would handle materials that they obtained as a result of an alleged hack and leak, how to assess the motivation for hack and leaks, the role government actors could play in confirming whether the materials were authentic or had been manipulated in some way, and whether it was appropriate to apply information labels to related content.¹⁶³ Other attendees included representatives from Twitter, Reddit, Wikimedia Foundation, NBC News, CNN, NPR, the *Washington Post*, and the *New York Times*.¹⁶⁴

¹⁵⁵ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 21.

¹⁵⁶ *Id.* at 20. John Podesta served as Hillary Clinton’s campaign manager in 2016.

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ See *infra* Section III.C.2.

¹⁶⁰ *Commission on Information Disorder*, ASPEN INSTITUTE, <https://www.aspeninstitute.org/programs/commission-on-information-disorder/> (last visited Oct. 18, 2024).

¹⁶¹ Aspen Digital Hack and Leak Roundtable agenda (June 25, 2020), see Ex. 86.

¹⁶² See Emails between Aspen Institute and Facebook personnel (May 19, 2020, 5:48 p.m.), Ex. 91; Emails between Aspen Institute, Facebook, and Stanford personnel (June 25, 2020), Ex. 92; Emails between Aspen Institute and Facebook personnel (July 13, 2020), Ex. 93; Email from Aspen Institute personnel to Facebook personnel (Sept. 28, 2020, 12:01 p.m.), Ex. 94.

¹⁶³ *Id.*; Aspen Digital Hack and Leak Roundtable meeting readout (July 2, 2020, 12:54 p.m.), see Ex. 87; see also Opening remarks from Aspen Institute roundtable, Ex. 88; Emails from Aspen Institute staff to industry participants (July 14, 2020), Ex. 89; Emails from Aspen Institute staff to industry participants (June 22, 2020), Ex. 90.

¹⁶⁴ Aspen Digital Hack and Leak Roundtable participant list (June 25, 2020), see Ex. 95.

A few months later, in September 2020, Aspen Digital hosted a tabletop exercise about a hack-and-leak scenario.¹⁶⁵ In a tabletop exercise, participants simulate their responses to a hypothetical set of facts, reacting to the responses of other participants and new information revealed incrementally throughout the exercise. Unlike the roundtable, which broadly discussed how companies handle materials related to a hack and leak, this exercise revolved around a specific hypothetical scenario involving a leak of Burisma documents tied to Hunter Biden.¹⁶⁶ Once again, Facebook personnel who had met with the FITF in 2020 were the primary drafters of the exercise.¹⁶⁷ According to internal Facebook messages and emails, one Facebook employee even rewrote the scenario as the date of the exercise approached.¹⁶⁸

The final exercise outline laid out a hypothetical day-by-day developing story, beginning on October 5, 2020, in which a news outlet obtained and published leaked documents involving Hunter Biden and Burisma, and various government actors and campaign officials began to respond.¹⁶⁹ The scenario was designed to give social media platforms and news outlets the opportunity to “think through out loud” how they would respond and “game out how various tech platforms and news organizations would respond in real time as the story unfolded.”¹⁷⁰

This exercise gave social media companies the opportunity to stress test the hack-and-leak responses they had proposed—and in some cases finalized—after the FBI’s warnings to expect one in September or October 2020. Even more, the scenario set forth by Aspen Digital closely mirrored the warnings given by the FBI and the details of the actual news story published by the *Post* just one month later.

* * *

By early October 2020, the stage had been set. In individual and group meetings with Big Tech platforms, the FBI’s FITF had repeatedly warned of an impending Russian hack and leak of documents alleging a Biden family influence peddling scheme relating specifically to Hunter Biden and Burisma. The social media platforms had deliberated and implemented new policies designed to limit the visibility of these documents if they did emerge. And in a tabletop exercise, the platforms had simulated how they would spike the exact story that the *Post* would ultimately publish. The prebunking was complete. When October 14 came, the platforms were ready to censor.

¹⁶⁵ Email from Aspen Institute staff to industry participants (Aug. 12, 2020, 12:49 p.m.), *see* Ex. 96.

¹⁶⁶ *Id.*

¹⁶⁷ Internal messages among Facebook personnel (Sept. 20, 2020, 8:03 p.m.), Ex. 97; Email from Aspen Institute personnel to Facebook and Twitter personnel (Aug. 7, 2020, 6:44 a.m.), Ex. 98.

¹⁶⁸ *Id.*

¹⁶⁹ Email from Aspen Digital staff to Roundtable participants (Sept. 1, 2020, 7:44 p.m.), Ex. 99; *see also* Aspen Digital Hack-and-Dump Scenario Outline (Sept. 2020), Ex. 100.

¹⁷⁰ *Id.*

III. Big Tech censored the true story, and the FBI hid key information, while millions voted

“Obviously, our calls on this [*New York Post* story] could colour the way an incoming Biden administration views us more than almost anything else.”

—October 14, 2020, WhatsApp message from Facebook’s then-Vice President of Global Affairs Nick Clegg to Vice President of Global Public Policy Joel Kaplan about Facebook’s censorship of the *New York Post* story.¹⁷¹

Early on October 14, 2020, the *New York Post* published an article, sourced from the contents of Hunter Biden’s abandoned laptop, exposing Biden family influence-peddling in Ukraine and around the world.¹⁷² For months, the FBI had conditioned social media companies to expect a Russian hack-and-leak operation that would target the Bidens and Burisma. The companies had developed responses for this scenario and had war-gamed the best way to apply them. The scenario they had been expecting, it seemed, was finally playing out.

Conditioned to assess that the story was the product of a hack and leak, social media companies’ initial response to the *Post* story was to censor it. Some companies wanted more information, though, and reached out to the FBI to be certain that this was the hack and leak they had been warned of before making final decisions about whether to continue their censorship of the story and the content within. But the FBI refused to acknowledge that it possessed and had authenticated the laptop.

Having not received this critical information from the FBI about the provenance of the laptop, social media platforms continued doing what they had been primed to do since early 2020: censor the *Post*’s true article. Twitter blocked the URL to the story and prohibited it from being shared on the platform, citing violations of its hacked materials policies. Facebook manually demoted the story in its algorithm, making users less likely to see it. Although platforms used different tools to achieve their goal, each invoked the warnings they received from their meetings with the government to explain why they censored the story.¹⁷³

But the FBI’s warnings were not the only thing motivating Big Tech. Platforms were keenly aware that their “calls on this [*New York Post* story] could colour the way an incoming Biden administration views us more than almost anything else.”¹⁷⁴ Platforms knew that if they

¹⁷¹ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), Ex. 101.

¹⁷² Emma-Jo Morris & Gabrielle Fonrouge, *Smoking-gun email reveals how Hunter Biden introduced Ukrainian businessman to VP dad*, N.Y. Post (Oct. 14, 2020).

¹⁷³ See, e.g., Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he FBI warned us about a potential Russian disinformation operation about the Biden family and Burisma in the lead up to the 2020 election. . . . It’s since been made clear that the [*New York Post*] reporting was not Russian disinformation, and in retrospect, we shouldn’t have demoted the story.”); Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

¹⁷⁴ *Id.*

did not act to suppress the story, their failure to censor it would threaten their relationship with a potential Biden-Harris Administration in 2021 and beyond.

This censorship of true election-related material denied millions of voters access to crucial information as they cast their vote for president. When the *Post* article came out nearly three weeks before Election Day, early and mail-in voting had already opened in many states. According to public reporting, between October 14—the day the *Post* published its story—and October 21—the day Facebook’s demotion was finally lifted¹⁷⁵—over 30 million Americans cast their ballots in the election.¹⁷⁶ Roughly one-fifth of all votes in the 2020 presidential election were cast during the week that Facebook censored an article about the Biden family’s involvement in an influence-peddling scheme with foreign powers.¹⁷⁷ This story was particularly relevant to voters making a decision about who to trust in the Oval Office. And, to add to the potential significance of Big Tech’s decision to censor the most important story of the election, the outcome of the 2020 election was fewer than forty-five thousand votes—just 0.1 percent of the votes cast during the time Facebook censored the story.¹⁷⁸

A. Big Tech quickly censored the true *New York Post* story, believing it was “exactly” what the FBI had warned about for months.

The technical and policy teams within the platforms who had been meeting with the FBI immediately recognized the October 14 *Post* story as “exactly” the one the FBI had been warning about in detail.¹⁷⁹ Contemporaneous internal messages among Facebook employees show that the company’s first reaction was to suspect a Russian hack-and-leak operation. For example:

- 8:37 AM ET: “About what we expected in the hack/leak department [...] it’s pretty much exactly what we pregamed.”¹⁸⁰
- 8:42 AM ET: “It looks like exactly the hack/leak scenario we’d expected.”¹⁸¹
- 9:06 AM ET: “Can we check with FBI Delaware if they have anything on this [...] Article claims that FBI has had the HDD [hard drive] since December.”¹⁸²
- 9:09 AM ET: “Exact content expected for hack and leak.”¹⁸³

¹⁷⁵ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 123.

¹⁷⁶ Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020); James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELS. (Dec. 15, 2020).

¹⁷⁷ *Id.*

¹⁷⁷ Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020).

¹⁷⁸ Paul Waldman, *We came much closer to an election catastrophe than many realize*, WASH. POST (Nov. 18, 2020).

¹⁷⁹ *See, e.g.*, Internal messages among Facebook personnel (Oct. 14, 2020, 8:42 a.m.), Ex. 5.

¹⁸⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 8:37 a.m.), *see* Ex. 4.

¹⁸¹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:42 a.m.), *see* Ex. 5.

¹⁸² Internal messages among Facebook personnel (Oct. 14, 2020, 9:06 a.m.), *see* Ex. 6.

¹⁸³ Internal messages among Facebook personnel (Oct. 14, 2020, 9:09 a.m.), *see* Ex. 7.

- 9:10 AM ET: “Right on schedule.”¹⁸⁴
- 9:14 AM ET: “[Facebook employee] is not in touch with the FBI on this. I’ll connect with Maryland and [Facebook employee] will raise at the FITF meeting today.”¹⁸⁵
- 9:33 AM ET: “FYI. Our legal team is reaching out to FBI on this.”¹⁸⁶
- 10:40 AM ET: “We’re enqueueing the content with demotion and doing outreach to 3PFCs. No updated info from FBI, no outreach from the Biden campaign.”¹⁸⁷
- 10:55 AM ET: “is this the Oct surprise everyone was waiting for?”¹⁸⁸
- 11:11 AM ET: “482 hours to first polls close...”¹⁸⁹

[REDACTED] (10/14/2020 05:42:26 PDT):
>It looks like exactly the hack/leak scenario we’d expected.

[REDACTED] (10/14/2020 06:09:51 PDT):
>Exact content expected for hack and leak, but sounds like so far, not much for us to do:
>
>1. No evidence of foreign interference operation
>2. Coming directly from press
>
>Sounds like next steps are to see if FBI contacts have any context for us, and to wait.

[REDACTED] (10/14/2020 06:10:33 PDT):
>Right on schedule.

[REDACTED] (10/14/2020 08:11:58 PDT):
>482 hours to first polls close . . .

“Exact content expected for hack and leak . . . Right on schedule.”
—Oct. 14, 2020 internal messages among Facebook personnel

Documents show that Facebook employees thought the story was “about what we expected in the hack/leak department,” but many also realized that there was “[n]o where [*sic*] near enough evidence to determine this is ‘part of a foreign govt influence op’ . . . other than [*sic*] circumstantial instinct.”¹⁹⁰ Meta’s President of Global Affairs Nick Clegg testified to the Committee and Select Subcommittee that the “team was very anxious to take a rapid decision,” and that the company had been preparing for “the risk of foreign interference” and for “hack-and-leak operations” for some time.¹⁹¹

¹⁸⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 9:10 a.m.), *see* Ex. 7.

¹⁸⁵ Internal messages among Facebook personnel (Oct. 14, 2020, 9:14 a.m.), *see* Ex. 6.

¹⁸⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 9:33 a.m.), *see* Ex. 8.

¹⁸⁷ Internal messages among Facebook personnel (Oct. 14, 2020, 10:40 a.m.), *see* Ex. 7.

¹⁸⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 10:55 a.m.), *see* Ex. 107.

¹⁸⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 11:11 a.m.), *see* Ex. 9.

¹⁹⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 8:37 a.m.), *see* Ex. 4; *see also* Internal Facebook Hack/Leak Policy Assessment (Oct. 20, 2020), Ex. 102.

¹⁹¹ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 123.

As confusion reigned, platforms immediately reached out to the FBI. For example, Facebook’s law enforcement outreach team contacted the FBI’s Baltimore field office, which was leading the Hunter Biden investigation.¹⁹² Critically, many of them had a prescheduled FITF meeting on the calendar for that day.¹⁹³ Internally, Facebook employees said that information from the FITF “would have huge implications on our next steps.”¹⁹⁴

Timestamp	Sender	Recipients	Message text
2020-10-14 06:05:00	[REDACTED] (whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	[REDACTED] -- looking at the calendar today, I see the FITF meeting. I don't recall whether I forwarded the invita to the rest of the group. Did you?
2020-10-14 06:40:20	[REDACTED] (@s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	I did not. I'll be able to dial in on the phone, but balancing a couple things today. Do we have an agenda for today?
2020-10-14 06:40:59	[REDACTED] (whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	The agenda is TBD. They may have OGA at the meeting, but not yet certain.
2020-10-14 06:41:57	[REDACTED] (whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	Think we want to get more info on the email leak in the NY Post from today and also on China based on the DNI's statement that they are much more prolific at ICs now than Russia

“[L]ooking at the calendar today, I see the FITF meeting. . . . Think we want to get more info on the email leak in the NY Post from today.”

—Oct. 14, 2020 internal messages among Facebook personnel

As Big Tech platforms began assessing how to implement their content moderation policies, including their newly updated hacked materials policies, they preemptively censored the story. Lacking evidence of a hack and leak, Facebook did not apply its newly developed hack-and-leak policy, and instead elected to contort its general misinformation policies to apply to the

¹⁹² Internal messages among Facebook personnel (Oct. 14, 2020, 9:14 a.m.), *see* Ex. 104.

¹⁹³ *See, e.g.*, Emails among Elvis Chan and Google personnel (Sept. 29, 2020, 11:04 a.m.), Ex. 40; Emails among Elvis Chan and Facebook personnel (Oct. 4, 2020, 2:31 p.m.), Ex. 16; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 12:32 p.m.), Ex. 103; Internal messages among Facebook personnel (Oct. 14, 2020, 12:35 p.m.), Ex. 103; Internal messages among Facebook personnel (Oct. 14, 2020), Ex. 56; Internal messages among Facebook personnel (Oct. 14, 2020), Ex. 108.

¹⁹⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 1:19 p.m.); *see* Ex. 109.

New York Post story.¹⁹⁵ This meant that Facebook took two steps “in the ensuing hour or two” after the *Post* article was published: (1) it manually flagged the article for review by fact checkers, or enqueued it, and (2) manually buried the story in users’ feeds, or demoted it, by 50 percent for seven days.¹⁹⁶ Notably, Facebook’s automated processes were not triggered—the article was *manually* targeted for demotion and fact-checking by decision-makers on the Trust and Safety team.¹⁹⁷

Joel Kaplan <[REDACTED]@s.whatsapp.net>

We have to decide whether to undo this demotion. None of [REDACTED], [REDACTED], [REDACTED], [REDACTED], or I think this was appropriate/justified. But Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).

Nick Clegg <[REDACTED]@s.whatsapp.net>

Yea I see - unwinding it now will unfortunately create more headaches than it's worth. Calling now

Joel Kaplan <[REDACTED]@s.whatsapp.net>

One thing to clarify—The difficult issue is that the demotion was NOT automatic (we manually demoted it). That’s what makes it hard—if it were automatic, it would be sort of an easy call not to intervene.

“The difficult issue is that the demotion was NOT automatic (we manually demoted it).”
—Oct. 14, 2020 internal messages between Vice President of Global Public Policy Joel Kaplan told then-Vice President of Global Affairs Nick Clegg regarding Facebook’s censorship of the *New York Post* story

Twitter, in contrast, decided to apply the company’s hacked materials policies despite the lack of specific evidence of a hack and leak, and began removing content and blocking the URL.¹⁹⁸ This initial censorship was seen as a stopgap to help the platforms limit the spread of the story by “slowing it down so that the researchers can take time to validate and peel through the layers around the release.”¹⁹⁹ Limiting the spread of the story also allowed platforms to ask for more information from the FBI.²⁰⁰ While companies wanted to wait for any additional information from the FBI to make their ultimate plans about how to handle the story about Biden family influence peddling, they began censoring the content immediately so they did not face backlash for inaction, particularly from “the press/left.”²⁰¹

¹⁹⁵ Transcribed Interview of Meta’s Director of Global Threat Disruption, H. Comm. on the Judiciary (May 16, 2023) (on file with Comm.) at 71-75.

¹⁹⁶ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 117-123; Internal messages among Facebook personnel (Oct. 14, 2020, 11:05 a.m.), Ex. 7.

¹⁹⁷ *Id.*; Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101; Internal messages among Facebook personnel (Oct. 14, 2020, 12:54 p.m.), *see* Ex. 9; Internal messages among Facebook personnel (Oct. 14, 2020, 5:25 p.m.), *see* Ex. 9

¹⁹⁸ Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/1598822959866683394>.

¹⁹⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 11:09 p.m.), *see* Ex. 105.

²⁰⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 1:33 p.m.), *see* Ex. 106.

²⁰¹ Internal messages among Facebook personnel (Oct. 14, 2020, 6:26 p.m.), *see* Ex. 115.

B. Big Tech reached out to the FBI and the FBI hid key information.

While social media companies scrambled internally to analyze the possible foreign influence risks of the *Post* article, they turned to the FBI with questions. After all, the platforms had met with the FITF about foreign interference and potential hack-and-leak operations dozens of times throughout 2020 in anticipation of just such an event. In light of this practice of information sharing, the social media companies thought the FBI would provide details to help the platforms determine which of their content moderation policies to apply.

By happenstance, the FBI had at least three meetings with social media companies already scheduled for October 14, 2020—two bilateral FITF meetings (one with Facebook and one with Twitter) and a USG-Industry meeting—which provided the social media platforms with opportunities to directly confront the FBI for more information.²⁰²

1. The Twitter-FITF Bilateral Meeting

The first meeting occurred between the FITF and Twitter.²⁰³ An FBI analyst present at the meeting testified that Twitter’s Head of Trust and Safety, Yoel Roth, began the meeting by informing the FBI that Twitter had “seen the *New York Post* story about Hunter Biden’s laptop,” assessed it “as a Russian disinformation effort,” and planned to “suppress the story.”²⁰⁴ The analyst then testified that after an “awkward pause,” the FITF’s Russia Unit Chief made a few general comments about Russian disinformation and hack-and-leak threats, after which the analyst jumped in and, referencing the Hunter Biden laptop, said “that’s part of a separate matter.”²⁰⁵ However, according to testimony from two other senior FBI employees with knowledge of the meeting, that FBI analyst actually responded by saying something to the effect of “the laptop is real.”²⁰⁶ The analyst was quickly stopped by an FBI lawyer from the Office of

²⁰² USG-Industry Meeting invitation (Oct. 14, 2020, 6:00 p.m.), *see* Ex. 27; Email from Elvis Chan to Google personnel (Sept. 29, 2020, 11:04 a.m.), *see* Ex. 40; Scheduling emails between FBI and Facebook personnel (Oct. 4, 2020, 2:31 p.m.), *see* Ex. 16; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 12:57 p.m.), Ex. 79. Though there were four meetings scheduled for October 14, 2020, witness testimony and documents containing contemporaneous notes obtained by the Committee have confirmed so far that at least three took place: Twitter-FITF, Facebook-FITF, and the USG-Industry meeting. It is unclear whether the Google-FITF meeting took place and, if so, whether anyone from Google asked whether the laptop was real.

²⁰³ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 65-80; *see also* Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33; Internal FBI meeting notes (Oct. 14, 2020), Ex. 44.

²⁰⁴ Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 32-33, 45.

²⁰⁵ *Id.* at 45; The separate matter referenced was the Hunter Biden investigation. While the analyst who confirmed the existence of the laptop in the Twitter-FITF meeting had known about the Hunter Biden investigation for several months, he learned that the FBI possessed Hunter Biden’s authenticated laptop only on the morning of October 14. Shortly after the *Post* story broke, a colleague at a nearby desk told the analyst and others that he was surprised to see the laptop’s contents in a media report because the laptop was part of the Hunter Biden investigation, which the colleague oversaw as a Program Manager covering the Baltimore Field Office. *Id.* at 28.

²⁰⁶ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 66-67; Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33.

General Counsel, who said “no further comment” and shut down all subsequent conversation on the topic.²⁰⁷ In her interview before the Committee, Laura Dehmlow explained:

Q. Are you familiar with the October 2020 *New York Post* story on Hunter Biden’s laptop?

A. I am.

Q. Do you recall whether any of these social media companies you were meeting with asked you any questions about it?

A. I do.

Q. And what is your recollection? Who –

A. So I remember having a conversation with or being involved in a conversation with Twitter, and I honestly can’t recall if this was repeated to me – I might have been a few minutes late to the meeting – or if – or if I was – I actually overheard it.

But it was – it was relayed to me later that somebody from Twitter – I don’t recall who. I’m not sure who. Somebody from Twitter essentially asked whether the laptop was real. And one of the FBI folks who was on the call did confirm that, yes, it was before another participant jumped in and said no further comment.

Q. Was this individual affiliated with FITF?

A. Again, it was somebody from the Criminal Investigative Division who is embedded with us.

Q. So yes?

A. Yes.

Q. And did this question occur in the context of a bilateral meeting?

A. It did.

Q. Do you recall how soon after the story broke that this meeting occurred?

A. I don’t remember. I believe it was the same week, but I don’t remember the specific day.

²⁰⁷ *Id.*

- Q. On that call with that IA [Intelligence Analyst] who's in the Criminal Investigative Division, that was the individual who said, "yes, the laptop is authentic"? Is that correct?
- A. I don't believe it was that specific. Again, I don't recall hearing the conversation itself. I know it was relayed to me afterwards. But my understanding is that we confirmed that, yes, the laptop was a real laptop.
- Q. And then you said another FBI individual came on and said, "No further comment."
- A. Yes.
- Q. Is that correct?
- A. That's correct.
- Q. Who was that individual?
- A. It was some -- it was one of our lawyers who was on the call.²⁰⁸

The then-Russia Unit Chief of the FITF provided similar testimony to the Committee. He explained:

- Q. During the FITF-Twitter call on the 14th, was there any discussion about the New York Post story or Hunter Biden's laptop?

- A. I recall that when the question came up, an intelligence analyst assigned to the Criminal Investigative Division said something to the effect of, "Yes, the laptop is real." And then I believe it was an OGC attorney assigned to the FITF stepped in and said, "We will not comment further on this topic."²⁰⁹

2. The FBI's Internal Deliberations

FBI personnel testified that after the Twitter bilateral meeting, the FITF had internal discussions about how to respond to future questions about the contents of Hunter Biden's abandoned laptop and the *Post* article.²¹⁰ Various members of the FITF were involved in these

²⁰⁸ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-31.

²⁰⁹ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 66-67.

²¹⁰ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 65-80; *see also* Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33.

conversations, and the FITF Section Chief was made aware.²¹¹ The FITF decided on this course of action because the laptop was a part of an ongoing investigation.²¹² The then-Russia Unit Chief of the FITF testified:

Q. Was there a decision made during these internal deliberations about how the FBI would respond going forward to future questions?

A. The characterization that is – it’s true, we absolutely talked about it, but more to firm up with everyone that it’s a longstanding policy. It wasn’t like this is something that wasn’t known, that we don’t talk about ongoing investigations.

So there was sort of that reiteration of, okay, if they ask about ongoing investigations, we don’t talk about ongoing investigations.

So from that point forward, again, we reiterated that it will be “no comment” when something like that comes up. So as you can imagine, that kind of continued that way.²¹³

For most of the Congress, when the Committee asked for the name of the FBI employee who made the decision that the FBI would have no comment to the social media companies going forward, the Justice Department forbid FBI witnesses from providing it. For example, during FITF Section Chief Dehmlow’s transcribed interview, she testified that she knew the identity of the FBI employee but the Justice Department prohibited her from disclosing the employee’s name:

Q. Who made the decision that the FBI would have no comment to the social media companies going forward?

DOJ Counsel. So I want to be clear. Ms. Dehmlow, obviously, can answer the question as long as it doesn’t get into internal deliberations or advice from a lawyer or anything.

A. Yeah, and, unfortunately I can’t answer that with any further detail on that advice.

Q. So you can’t tell us who made the decision?

²¹¹ *Id.*

²¹² *Id.*

²¹³ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 78-79.

- A. I can say there were internal deliberations with a number of parties, and then -- but I can't get into that further.²¹⁴

3. The Facebook-FITF Bilateral Meeting

Following the FITF's internal deliberations after the FITF-Twitter bilateral meeting, the FITF held a prescheduled bilateral meeting with Facebook and a full USG-Industry meeting, during which the FBI would not officially comment on questions about the laptop or the *Post* article.²¹⁵ The article was brought up in both meetings, but the FBI's "no comment" response ended the discussion and the meetings continued with other matters.²¹⁶ FITF Section Chief Dehmlow testified to the Committee and Select Subcommittee:

Q When the Facebook employee asked the question, do you recall exactly what they asked?

A. I don't.

Q. Do you know if it was about the laptop?

A. Yes. It was essentially whether or not we -- yes, it was something about the laptop. I don't remember -- I know that my answer was "no comment" because -- and the question doesn't stick in my mind because it was something about the laptop. And I said, "No comment."

Again, that was not my decision. It wasn't my final call. There were other agency, other departments, other FBI equities at stake, investigative equities, and so pretty typical for us to come to that conclusion.²¹⁷

Through unofficial FBI channels, Facebook personnel were able to obtain more information than the "no comment" they were offered in the FITF bilateral meeting. According to internal Facebook messages, an FBI official told Facebook that the laptop existed and that it was "part of a criminal matter."²¹⁸

²¹⁴ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 33.

²¹⁵ *Id.* at 65-80; *See also* Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 29-33.

²¹⁶ *Id.*; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 9:05 a.m.), Ex. 56; Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), Ex. 3.

²¹⁷ Transcribed Interview of Laura Dehmlow, H. Comm. on the Judiciary (July 17, 2023) (on file with Comm.) at 36.

²¹⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 3:45 p.m.), *see* Ex. 7; Internal messages among Facebook personnel (Oct. 14, 2020, 8:23 p.m.), *see* Ex. 7; Internal messages among Facebook personnel (Oct. 14, 2020, 1:50 p.m.), *see* Ex. 108. The Russia Unit Chief of the FITF testified to the Committee that he did not know who at the FBI shared with Facebook that the laptop was part of a criminal matter. *See* Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 155.

██████████ (10/14/2020 12:45:15 PDT):
 >For awareness, additional context from ██████████ from the FBI meeting (somewhat sensitive so wasn't shared on the broader IPOC threads):
 >
 >Officially FBI said "The FBI has no information indicating foreign sponsorship, direction, or coordination of the hunter laptop issue" and ██████████ shared that with the US 2020 Esc thread...on the side in the same call however, they did confirm that FBI has the laptop and it's being review "as part of a criminal matter" but didn't give us details.

Timestamp	Sender	Recipients	Message text
2020-10-14 10:50:22	██████████ (s.whatsapp.net)	██████████ @s.whatsapp.net); System Message: ██████████	And I thought he said he could confirm it existed
2020-10-14 10:50:40	██████████ (s.whatsapp.net)	██████████ @s.whatsapp.net); System Message: ██████████ @s.whatsapp.net)	I distinctly remember he said it was a crim matter

"[T]hey did confirm that FBI has the laptop and it's being review [sic] 'as part of a criminal matter'"

—Oct. 14, 2020 internal messages among Facebook personnel

Despite the FBI's limited revelations as well as obvious facts, such as the failure of the Biden campaign to deny the laptop's authenticity, Facebook still chose to censor the *Post* story about Biden family influence peddling.²¹⁹

Joel D. Kaplan (10/14/2020 17:23:48 PDT):
 >I agree that Twitter is in a much more coherent position right now and thus easier to defend. I think either removal or labeling (on newsworthiness grounds) is defensible, if not equally well-received. I think a demotion tied to possible falsity, when none of the parties are actually suggesting the emails/images are false, at least so far—will be increasingly hard to defend. (The fact that the FBI apparently has the laptops may explain why no one in the Biden campaign is denying the authenticity).

"The fact that the FBI apparently has the laptop[] may explain why no one in the Biden campaign is denying the authenticity."

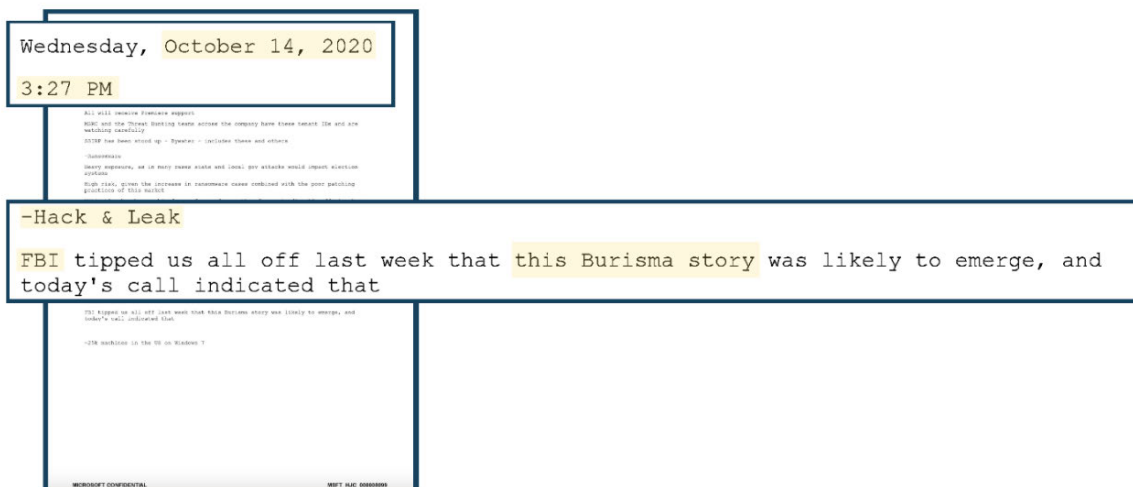
—Oct. 14, 2020 internal message from Facebook's Vice President of Global Public Policy Joel Kaplan to Facebook employees

²¹⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 8:23 p.m.), see Ex. 7.

4. The USG-Industry Meeting

The laptop again came up during the USG-Industry meeting scheduled for the afternoon of October 14.²²⁰ Like he did at the start of the Twitter-FITF meeting earlier that day, Twitter’s Head of Trust and Safety, Yoel Roth, once again shared that Twitter assessed the *Post* story to be Russian disinformation and intended to censor it.²²¹ Afterwards, Elvis Chan “pitched the response over” to the same analyst who had confirmed the laptop’s existence in the Twitter-FITF meeting; that analyst then responded in this USG-Industry meeting “no comment.”²²²

Notably, the analyst’s testimony contradicts Chan’s testimony from his *Murthy v. Missouri* deposition, in which Chan said he “was confident that [he] was not a party to any meeting with social media companies where Hunter Biden was discussed outside of the [Facebook-FITF bilateral meeting].”²²³ Likewise, Chan’s testimony that he had “no internal knowledge of [the Hunter Biden] investigation” was contradicted by the analyst, who testified to the Committee that he messaged Chan and “mentioned that there was an ongoing investigation” on the morning of October 14.²²⁴ The Justice Department continues to prohibit Chan from testifying to the Committee and Select Subcommittee.²²⁵



“FBI tipped us all off last week that this Burisma story was likely to emerge”
—Oct. 14, 2020, internal Microsoft notes on USG-Industry meeting

²²⁰ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), *see* Ex. 3.

²²¹ Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 107-108.

²²² Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 38.

²²³ *Murthy v. Missouri*, No. 3:22-cv-01213, 2023 WL 43352270 (WD La. July 4, 2023) (Deposition of Elvis Chan), at 216.; *see also* Rep. Jim Jordan (@Jim_Jordan), X (Aug. 7, 2023, 10:11 a.m.), https://x.com/Jim_Jordan/status/1688553364211056640 (Facebook Files Part 4) (identifying other contradictions between Elvis Chan’s deposition testimony and documents obtained by the Committee and Select Subcommittee).

²²⁴ *Id.* at 214; Transcribed Interview of an FBI Criminal Investigative Division Analyst, H. Comm. on the Judiciary (Oct. 23, 2024) (on file with Comm.) at 47.

²²⁵ *See* House Judiciary GOP (@JudiciaryGOP), X (Sept. 15, 2023, 4:17 p.m.), <https://x.com/JudiciaryGOP/status/1702778803037057503>.

In minutes from this USG-Industry meeting, describing the discussion of the *New York Post* story with the FBI, Microsoft wrote that the “FBI tipped us all off last week that this Burisma story was likely to emerge, and today’s call indicated that.”²²⁶

5. The FITF’s Follow-Up Discussions

The FITF’s Russia Unit Chief testified that during the course of the FITF’s meetings with social media platforms on October 14, 2020, he felt there was significant confusion around the *Post* article and that it “felt necessary to reach out to some of the more major companies and have a follow-up discussion with them,” particularly in light of the FBI analyst’s apparent confirmation of the laptop’s existence to Twitter.²²⁷ The Russia Unit Chief testified that he had a joint “follow-up discussion” with one representative each from Twitter, Facebook, Google, and Microsoft.²²⁸ In this meeting, he shared a prepared statement that he had “cleared” with superiors while “trying to skirt multiple policies and be within bounds legally.”²²⁹ The statement, he later explained to the Committee and Select Subcommittee, “was something to the effect of: The FBI has nothing in its possession to suggest that the laptop is a hack or a leak.”²³⁰ The Russia Unit Chief also testified that he rebuffed any potential follow-up questions with a response of “I’ve told you everything I can tell you on this matter.”²³¹ He testified that while the FBI “had more information” than just the fact that the laptop was not the product of a hack and leak, he could not share more due to the FBI’s policies.²³² He explained:

Q. After these FITF meetings take place, do you recall any follow-up outreach to you or other members of the FITF with the social media companies asking for more information?

A. Yes. Specifically, I felt that there was some confusion after this meeting or around that time because of that sort of comment that was made outside of policy, and then sort of having to cut it off.

Again, like, when we normally answer “no comment,” we can’t say, “because we have an open investigation,” because that, in and of itself, is revealing that we have an investigation.

So in this case, there was some confusion and I felt necessary to reach out to some of the more major companies and have a follow-up discussion with them.

Q. Which companies did you reach out to?

²²⁶ Microsoft internal meeting notes (Oct. 14, 2020, 3:27 p.m.), Ex. 3.

²²⁷ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 83.

²²⁸ *Id.*

²²⁹ *Id.* at 84.

²³⁰ *Id.*; *see also* Internal messages among Facebook personnel (Oct. 14, 2020, 1:41 p.m.), Ex. 109; Internal messages among Facebook personnel (Oct. 18, 2020, 2:05 p.m.), Ex. 110.

²³¹ *Id.*

²³² *Id.* at 85.

A. I don't remember all of them. I'm pretty sure there was – I usually – I remember that it was, like, one person from each company, and I'm pretty sure Facebook, Google, and Twitter were represented.

Q. Did you do –

A. There may have been one or two other companies, but I don't remember. Maybe Microsoft. But I don't want to speculate, like, exactly which companies were sort of deemed pertinent or that we should give them somewhat of an update.

Chairman Jordan. What did you tell them?

A. So I told them -- I cleared a phrase, trying to skirt multiple policies and be within bounds legally and within policy, of what I could communicate to them, and came up with a phrase that I could share.

And the phrase, I don't have it verbatim, but it was something to the effect of: The FBI has nothing in its possession to suggest that the laptop is a hack or a leak.

And what I intended to communicate with that was that we did not know that the laptop was hacked. And I was very deliberate with my words because there's all sorts of things I could add that would either indicate that it's an ongoing investigation or somehow communicate to them that I know more than I did.

So at that time what I knew was the laptop was not hacked, because we had it in our possession. So I was very deliberate in that statement.

Obviously there was follow-on questions. We expected there would be follow-on questions. So also came up with sort of a follow-on statement. And, again, I don't know this verbatim, but something to the effect of: I've told you everything I can tell you on this matter. Sort of beyond "no comment" but basically no comment otherwise.

So obviously that phrase of we have nothing in FBI holdings to suggest that the laptop is hack-and-leak generally communicates that, as much as I can tell them, to try to clear up at least that element of the situation.²³³

The FITF's Russia Unit Chief testified that he felt an especially strong need to convey this statement to the major social media platforms because of the confusion from the Twitter-

²³³ *Id.* at 83-84 (emphasis added).

FITF meeting, in which an FBI analyst appeared to confirm the existence of the laptop with a statement “made outside of policy” before his superiors intervened.²³⁴ Had the analyst not spoken out of turn, it is unlikely that the FBI ever would have told the platforms anything about the true nature of the Hunter Biden laptop on October 14.²³⁵

Ultimately, in response to questions from Big Tech platforms—who had been primed for months to view this exact story as a Russian operation—about whether the *Post* article was a hack-and-leak operation, the FBI merely responded with “no comment” and “[t]he FBI has nothing in its possession to suggest that the laptop is a hack or a leak.”²³⁶ The FBI gave these answers even though it had possession of the laptop and had authenticated its contents and “knew [that] the laptop was not hacked.”²³⁷

C. Despite a lack of evidence, Big Tech continued to censor the story because of concerns about a potential Biden-Harris Administration.

Even after meeting with the FBI, social media platforms—particularly Facebook—doubled down on their decision to censor the *New York Post* story about Biden family influence peddling. While the FBI clarified that it had no specific evidence of a Russian hack-and-leak operation, it failed to disclose that it possessed and had authenticated the laptop—a key fact that likely would have ended any justification for censorship. Instead, because the FBI’s statements on the laptop failed to clarify the situation, and because the platforms knew that their “calls on this could colour the way an incoming Biden administration views us more than almost anything else,”²³⁸ major platforms, such as Facebook, censored the story.

1. Facebook

After the initial steps to apply Facebook’s misinformation policies by demoting and enqueueing the *Post* story for fact checking, a broader debate emerged on whether to invoke Facebook’s newly developed hacked material policies. This provision required there to be evidence of a hack, but contained an exception allowing materials considered “newsworthy” to remain on the site.²³⁹

Many Facebook employees were initially convinced that the article was the product of a hack and leak, but they had differing degrees of confidence. One employee wrote in an internal message that the story was the “exact content expected for hack-and-leak, but sounds like so far, there is not much for us to do: 1. No evidence of foreign interference operation[,] 2. Coming directly from press[.] Sounds like next steps are to see if FBI contacts have any context for us and to wait.”²⁴⁰

²³⁴ *Id.* at 83.

²³⁵ *Id.* at 83-85.

²³⁶ *Id.* at 83-84

²³⁷ *Id.*

²³⁸ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²³⁹ Internal messages among Facebook personnel (Oct. 14, 2020, 7:03 p.m.), *see* Ex. 7.

²⁴⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 9:09 a.m.), *see* Ex. 7.

From: ██████████ </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS /CN=28E865DE754F42D3ACBCF1C8052D0B8F>
To: ██████████; Nick Clegg; ██████████
 ██████████ Joel Kaplan; ██████████
Sent: 10/14/2020 9:56:34 PM
Subject: Message summary [{"otherUserFbId":null,"threadFbId":3940241416047689}]
Attachments: 121161847_1316086545401657_7329363007398542195_n.png;
 121440254_1251840195175940_3016984524154928067_n.jpg;
 121523296_4486187921454030_1191778544254324768_n.png;
 121570689_337558230646825_1230117776855863053_n.png; sticker.png; sticker1.png

██████████ (10/14/2020 06:03:24 PDT):
 >'Morning, the NY Post published an article on what are allegedly leaked Hunter Biden-Burisma emails. SR (██████████ and team) will send FYI.
 >
 ><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

██████████ (10/14/2020 06:09:51 PDT):
 >Exact content expected for hack and leak, but sounds like so far, not much for us to do:
 >
 >1. No evidence of foreign interference operation
 >2. Coming directly from press
 >
 >Sounds like next steps are to see if FBI contacts have any context for us, and to wait.

██████████ (10/14/2020 06:10:33 PDT):
 >Right on schedule.

██████████ (10/14/2020 07:01:16 PDT):
 >Has it been referred to 3PFC?

Nick Clegg (10/14/2020 07:11:08 PDT):
 >Looks fairly dodgy: <https://mobile.twitter.com/JuddLegum/status/1316376280103825409>

██████████ (10/14/2020 07:15:15 PDT):
 >Has not been referred yet, asked the team to refer now (but ██████████'s assessment FWIW is that this is couched in a way that would be very difficult for 3PFC to rate).

██████████ (10/14/2020 07:40:10 PDT):
 >We're enqueueing the content with demotion and doing outreach to 3PFCs. No updated info from FBI, no outreach from the Biden campaign. Trump is running ads on the claim.

Joel D. Kaplan (10/14/2020 07:42:35 PDT):
 >Do we always apply a demotion when we manually enqueue?

██████████ (10/14/2020 07:43:02 PDT):
 >No. We have standards for doing so and this met the test.

“Exact content expected for hack and leak . . . Right on schedule.”

—Oct. 14, 2020, internal messages among Facebook personnel

Others turned immediately to the hack-and-leak framework as Facebook contemplated a response. In a separate message thread, one Facebook employee wrote “(1) we need to assess whether the content violates our policies against hacked materials (sounds like that is how Twitter is handling) and (2) is the content newsworthy?”²⁴¹ Another Facebook employee

²⁴¹ Internal messages among Facebook personnel (Oct. 14, 2020, 2:06 p.m.), *see* Ex. 9.

responded, after conducting an analysis, that the content “violates hacked policy,” subject to a determination of whether the content met the newsworthiness exception.²⁴²

```
(10/14/2020 11:06:02 PDT):
>Yes, I think (1) we need to assess whether the content violates our policies against
hacked materials (sounds like that is how twitter is handling) and (2) is the content
newsworthy?

(10/14/2020 11:06:25 PDT):
>got it. moving out now.
```

```
(10/14/2020 11:54:54 PDT):
>What's the tldr?

(10/14/2020 11:55:42 PDT):
>Violates hacked policy, we are not in favor of the NW allowance but are providing
arguments on both sides
```

“[W]e need to assess whether the content violates our policies against hacked materials[.]”
—Oct. 14, 2020, internal messages among Facebook personnel

Facebook employees determined what qualified for the newsworthiness exception on a case-by-case basis by “weighing the public interest in seeing content against the risk of harm.”²⁴³ Stories that were uninteresting or harmful “would be removed,” while high-interest or low-harm stories “would either stay up or be labeled, depending on what [Facebook] decide[d].”²⁴⁴ One employee wrote that “it seems like the vast majority of the content obtained from the laptop of a candidate’s child would not be newsworthy,”²⁴⁵ and another concurred, writing that “both [public interest and harm] are pretty low here. It’s not really news that Hunter Biden has done drugs or engaged in other bad behavior.”²⁴⁶

Others in the company disagreed with this assessment. Joel Kaplan, Facebook’s Vice President of Global Public Policy, in particular, pushed back, writing: “Years of stories about the adult family members of Presidents would suggest that that content is newsworthy.”²⁴⁷

```
(10/14/2020 16:17:04 PDT):
>Yes, I would remove these images and link to the images. They are from the same source we
determined is a hack under our rules and they do not have a public interest value.

Joel D. Kaplan (10/14/2020 16:17:44 PDT):
>We are going to remove the content of every publisher who published pictures of the
candidate’s son doing drugs as not newsworthy? Years of stories about the adult family
members of Presidents would suggest that that content is newsworthy.
```

“Years of stories about the adult family members of Presidents would suggest that that content is newsworthy”

—Oct. 14, 2020, internal message from Joel Kaplan to Facebook personnel

²⁴² Internal messages among Facebook personnel (Oct. 14, 2020, 2:55 p.m.), *see* Ex. 9.

²⁴³ Internal messages among Facebook personnel (Oct. 14, 2020, 7:44 p.m.), *see* Ex. 7.

²⁴⁴ Internal messages among Facebook personnel (Oct. 14, 2020, 7:03 p.m.), *see* Ex. 7.

²⁴⁵ Internal messages among Facebook personnel (Oct. 14, 2020, 7:07 p.m.), *see* Ex. 7.

²⁴⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 7:44 p.m.), *see* Ex. 7.

²⁴⁷ Internal messages among Facebook personnel (Oct. 14, 2020, 7:17 p.m.), *see* Ex. 7.

The Facebook employees also debated whether Hunter Biden could be considered a “prominent person in public life”—another consideration in Facebook’s policy on hacked materials.²⁴⁸ Many Facebook employees argued that Hunter Biden did not meet that threshold as the son of a presidential candidate who was not a public figure in his own right.²⁴⁹ Again, Joel Kaplan pushed back, writing: “I don’t really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life.”²⁵⁰

Joel D. Kaplan (10/14/2020 16:48:39 PDT) :
 >I don't really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life. And if Fox concludes that misconduct is newsworthy—pretty consistent with the standards that have applied to adult children of presidents for decades—I don't really buy it's not newsworthy either.

“I don’t really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life.”

—Oct. 14, 2020, internal message from Joel Kaplan to Facebook personnel

Before the newsworthy analysis became determinative, though, Facebook would have had to conclude that the contents of the *Post* article were the result of a hack. The company quickly determined that it did not have evidence to conclude that the *Post* story was the result of a hack.²⁵¹

Because of the lack of evidence of a hack and leak, and because the FBI told Facebook that it also did not have any evidence to suggest such a conclusion, Facebook could not censor the story under its hacked materials policy.²⁵² Instead, the platform contorted its misinformation framework to trigger an automatic seven-day demotion while the story was sent to third-party factcheckers for their review. “Demotion is an appropriate and effective mitigation for what we’re almost certainly observing here,” one Facebook employee wrote in an internal chat.²⁵³ “We’re slowing it down so that the researchers can take time to validate and peel through the layers around the release.”²⁵⁴

Soon after Facebook’s decision to demote and enqueue content concerning Hunter Biden’s laptop and Biden family influence peddling, key decision-makers within the company began to express significant concerns with how the platform handled the situation and the public attention it was receiving. In an internal message thread, Vice President of Global Public Policy Joel Kaplan told then-Vice President of Global Affairs Nick Clegg that the company’s handling

²⁴⁸ Internal messages among Facebook personnel (Oct. 14, 2020, 7:46 p.m.), *see* Ex. 7.

²⁴⁹ *Id.*

²⁵⁰ Internal messages among Facebook personnel (Oct. 14, 2020, 7:48 p.m.), *see* Ex. 7.

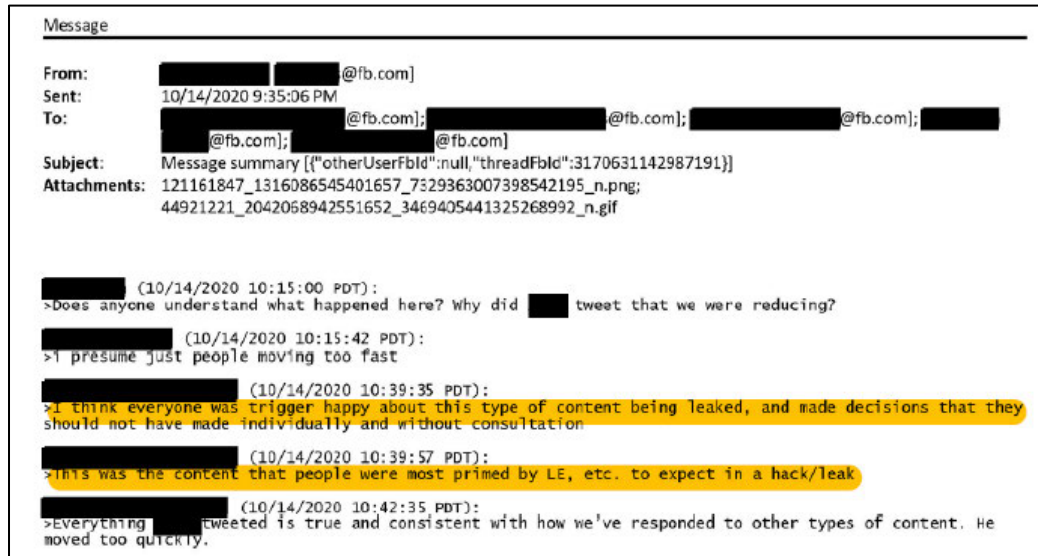
²⁵¹ Transcribed Interview of Meta’s Director of Global Threat Disruption, H. Comm. on the Judiciary (May 16, 2023) (on file with Comm.) at 71-75.

²⁵² *Id.*

²⁵³ Internal messages among Facebook personnel (Oct. 14, 2020, 11:09 p.m.), Ex. 105; *see also* Internal messages among Facebook employees (Oct. 14, 2020, 1:00 p.m.), Ex. 9.

²⁵⁴ *Id.*

of the *Post* article had been “outrageous.”²⁵⁵ These concerns were shared at lower levels of the company: another employee wrote, “I think everyone was trigger happy about this type of content being leaked, and made decisions that should not have been made individually and without consultation.”²⁵⁶ Facebook employees were so “trigger happy” because “this was the content that people were most primed by LE [law enforcement], etc. to expect in a hack/leak.”²⁵⁷ The FBI’s prebunking had worked.



“This was the content that people were most primed by LE, etc. to expect in a hack/leak”
 —Oct. 14, 2020, internal messages among Facebook personnel

The internal conflict over Facebook’s initial demotion of the content spurred discussion of potential alternative courses of action. In his transcribed interview before the Committee and Select Subcommittee, Meta’s President of Global Affairs Nick Clegg testified that there were suggestions to shorten the amount of time the story was demoted for from seven days to five or six, especially “in the absence of any fact checker finding fault with the content.”²⁵⁸ Clegg testified that COO Sheryl Sandberg was in favor of demoting the content for the full seven days, arguing that the company had already taken the action and should not reverse course; meanwhile CEO Mark Zuckerberg “was keen that we sort of cleaved as closely as possible” to the company’s standards, but “deferred very much” to Clegg.²⁵⁹

In an internal message thread, Facebook’s Vice President of Global Public Policy Joel Kaplan and then-Vice President of Global Affairs Nick Clegg discussed other specific concerns with Facebook’s handling of content related to allegations of Biden family influence peddling. Kaplan highlighted a perceived double-standard: Facebook allowed leaked content that was politically damaging to one party, like the *New York Times* story about President Trump’s tax

²⁵⁵ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

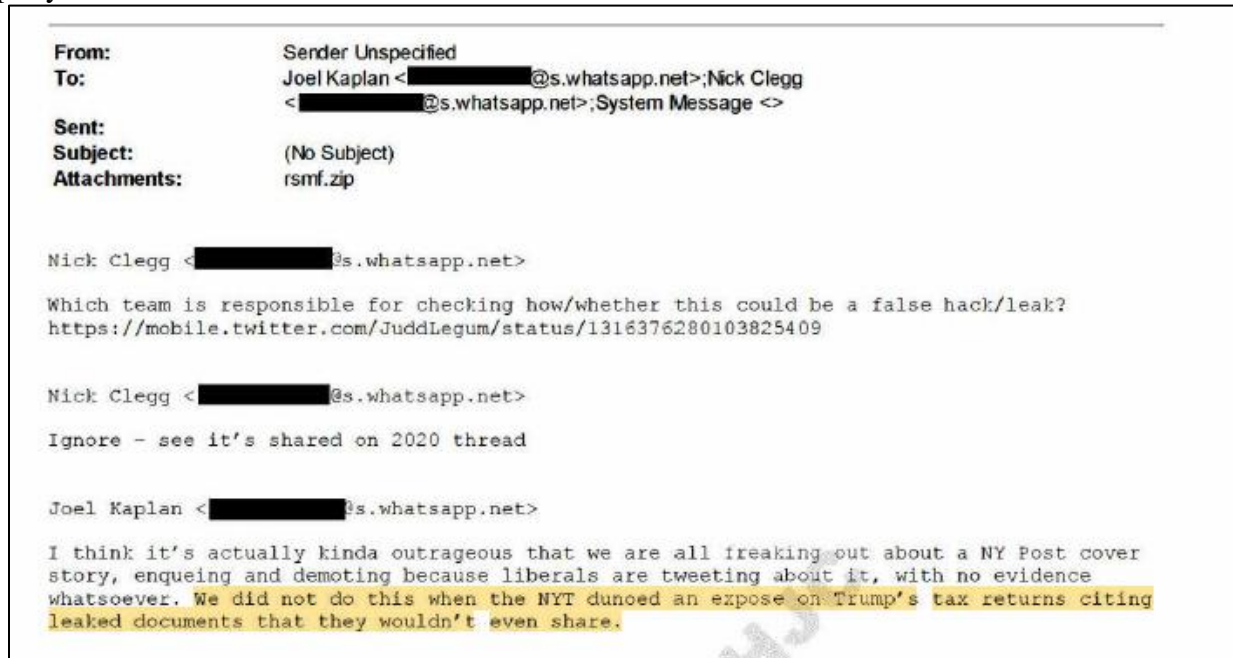
²⁵⁶ Internal messages among Facebook personnel (Oct. 14, 2020, 1:39 p.m.), *see* Ex. 115.

²⁵⁷ *Id.*

²⁵⁸ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 124.

²⁵⁹ *Id.* at 123-126.

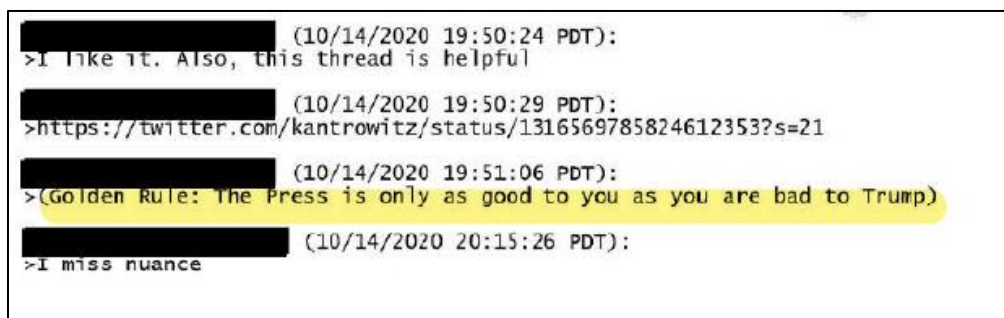
returns, while demoting leaked content like the *Post* story that might be damaging to the other party.²⁶⁰



“We did not do this when the NYT [dumped] [sic] an expose on Trump’s tax returns citing leaked documents that they wouldn’t even share.”

—Oct. 14, 2020, internal messages between Nick Clegg and Joel Kaplan

Similarly, as reflected in internal communications obtained by the Committee and Select Subcommittee, Facebook’s communications team understood that the traditional media employed a double-standard where Big Tech would face criticism *not* based on whether it fairly enforced its policies, but only on whether its enforcement hurt or helped President Trump.²⁶¹ As one Facebook Communications Vice President wrote as the company decided whether and how to censor the *New York Post* story: “Golden Rule: The Press is only as good to you as you are bad to Trump.”²⁶²



“Golden Rule: The Press is only as good to you as you are bad to Trump.”

—Oct. 14, 2020, internal messages from Facebook Communications Vice President

²⁶⁰ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²⁶¹ Internal messages among Facebook personnel (Oct. 14, 2020, 10:51 p.m.), *see* Ex. 115.

²⁶² *Id.*

Internal Facebook messages also suggest that Facebook’s leadership decided to continue to demote the *New York Post* story because of public pressure and concerns about how changing course would affect the company’s relationship with a potential Biden-Harris Administration. In the message thread, Kaplan told Clegg that the platform needed to “decide whether to undo this demotion” but that “Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).”²⁶³ Clegg agreed and responded by saying “unwinding it now will unfortunately create more headaches than it’s worth.”²⁶⁴

Joel Kaplan <[REDACTED]@s.whatsapp.net>
 We have to decide whether to undo this demotion. None of [REDACTED], [REDACTED], [REDACTED], [REDACTED], or I think this was appropriate/justified. But Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).

Nick Clegg <[REDACTED]@s.whatsapp.net>
 Yea I see - unwinding it now will unfortunately create more headaches than it's worth. Calling now

Joel Kaplan <[REDACTED]@s.whatsapp.net>
 One thing to clarify—The difficult issue is that the demotion was NOT automatic (we manually demoted it). That’s what makes it hard—if it were automatic, it would be sort of an easy call not to intervene.

“Unwinding it now will unfortunately create more headaches than it’s worth.”
 —Oct. 14, 2020, internal messages between Nick Clegg and Joel Kaplan

Later in the message thread Clegg recognized that Facebook’s “calls on this could colour the way an incoming Biden administration views us more than anything else.”²⁶⁵

Nick Clegg <[REDACTED]@s.whatsapp.net>
 Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...

“Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else”
 —Oct. 14, 2020, internal messages between Nick Clegg and Joel Kaplan

Facebook seemed to be more concerned about its relationship with a potential Biden-Harris Administration than protecting the free speech of its users on its platform. So, while the FBI had confirmed that there was no evidence that the laptop was a Russian influence operation, Facebook continued with its decision to reduce the story by 50 percent on its platform for seven

²⁶³ Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020), *see* Ex. 101.

²⁶⁴ *Id.*

²⁶⁵ *Id.*

days.²⁶⁶ During these seven days of Facebook censorship, over 30 million Americans voted in the 2020 presidential election—representing nearly one-fifth of the total votes cast.²⁶⁷ After nearly four years, in August 2024, CEO Mark Zuckerberg told the Committee and Select Subcommittee in a letter that Facebook “shouldn’t have demoted the story.”²⁶⁸

2. Twitter

The Twitter Files, a series of reports authored by independent journalists and released shortly after Elon Musk acquired the company, show that Twitter quickly began applying its hacked materials policy to the *Post* article after its release.²⁶⁹ Twitter’s enforcement actions included suppressing the article, removing links, applying safety warnings, and blocking the ability to send it via direct message.²⁷⁰ Twitter even locked then-White House Press Secretary Kayleigh McEnany out of her account for tweeting about the *Post* article and prevented the Committee from tweeting a link to the *Post* article.²⁷¹

Despite the quick and aggressive enforcement of the hacked materials policy, decision-makers at Twitter did have concerns about the platform’s response. Twitter’s Vice President of Global Communications asked whether Twitter could “truthfully claim that this [the *Post* article] is part of the [hacked materials] policy?”²⁷² Twitter’s Deputy General Counsel responded, acknowledging that the company probably needed “more facts to assess whether the materials were hacked,” but that “it is reasonable for us to assume that they may have been and that caution is warranted.”²⁷³ Like Facebook, Twitter censored the story, relying on the warnings it had received from the FBI prior to the story’s publication.

Some decision-makers at Twitter outright disagreed with the decision. Twitter’s former Head of Trust and Safety, Yoel Roth, testified to the Committee and Select Subcommittee that he reviewed the *Post* article and other relevant data, found it to be an ambiguous case, and thus “didn’t believe that the activity in question warranted enforcement under Twitter’s distribution of Hacked Materials Policy,” though he did believe the story should not be promoted.²⁷⁴ Mr. Roth testified to the Committee:

²⁶⁶ Transcribed Interview of Nick Clegg, H. Comm. on the Judiciary (Mar. 1, 2024) (on file with Comm.) at 117-123; Internal messages among Facebook personnel (Oct. 14, 2020, 11:05 a.m.), *see* Ex. 7.

²⁶⁷ Brittany Renee Mayes et al., *The U.S. hit 73% of 2016 voting before Election Day*, WASH. POST (Nov. 3, 2020); Catherine Park, *More than 14M Americans have voted early in 2020 presidential election, data shows*, FOX 10 PHOENIX (Oct. 14, 2020); James M. Lindsay, *The 2020 Election by the Numbers*, COUNCIL ON FOREIGN RELS. (Dec. 15, 2020).

²⁶⁸ Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024).

²⁶⁹ Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/159882295986683394>.

²⁷⁰ *Id.*; *see also* Noah Manskar, *Twitter, Facebook censor Post over Hunter Biden exposé*, N.Y. POST (Oct. 14, 2020).

²⁷¹ Steven Nelson, *WH press secretary locked out of Twitter for sharing Post’s Hunter Biden story*, N.Y. POST (Oct. 14, 2020); House Judiciary GOP (@JudiciaryGOP), X (Oct. 15, 2020, 9:13 a.m.), <https://x.com/JudiciaryGOP/status/1316728942523547653>.

²⁷² Matt Taibbi (@mtaibbi), X (Dec. 2, 2022, 6:34 p.m.), <https://x.com/mtaibbi/status/159882295986683394>.

²⁷³ *Id.*

²⁷⁴ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 29.

- Q. Once you found out about the story, again, to your recollection, walk me through what you did next.
- A. Yeah. My first step was to ask a member of my team to develop what we called a policy assessment of the situation, a brief document that compiled the available evidence about what had happened and to make a recommendation under Twitter's rules for what the company should do.

I recall the situation at that point being pretty ambiguous. There was one article or perhaps a series of articles from the *New York Post* discussing the incident, but there wasn't a lot of available factual evidence at the time.

And so my recollection is that the member of my team working on the policy assessment struggled to identify what the right course of action here would be.

From that point, I discussed the issue with Del Harvey, who was my supervisor, and I represented to her that I didn't believe that the activity in question warranted enforcement under Twitter's Distribution of Hacked Materials Policy.

But, based on the available evidence that seemed to indicate a laptop of unknown provenance, a laptop that potentially had been broken into and the contents of which were being divulged, I made the recommendation to my supervisor that Twitter should take steps to not recommend or amplify the circulation of this content.

That is, I didn't recommend that Twitter delete the story or block its distribution entirely, just that Twitter take steps to not actively recommend it to users, which was a content moderation action we would take in ambiguous cases.

It's my understanding that Ms. Harvey discussed that with Ms. Gadde, and the decision was communicated to me at some point in first half of the day – but I couldn't exactly say when – that Ms. Gadde had decided that the content was a violation of Twitter's policy and that we should enforce against it under the Distribution of Hacked Materials Policy.²⁷⁵

In 2023, Twitter executives testified before Congress and called the company's treatment of the *Post* article a "mistake."²⁷⁶

²⁷⁵ *Id.* at 29-30.

²⁷⁶ Laura Romero, *Former Twitter execs tell House committee that removal of Hunter Biden laptop story was a 'mistake'*, ABC NEWS (Feb. 8, 2023); see also Kelsey Vlamis, *Twitter's former trust and safety chief said it was a mistake to censor the Hunter Biden laptop story: 'We didn't know what to believe'*, BUSINESS INSIDER (Nov. 30, 2022).

In November 2020, in the aftermath of the *Post* debacle, Twitter amended its policy on the distribution of hacked materials.²⁷⁷ First, Twitter changed the scope of the policy “to much more narrowly focus on situations in which there was a clearly confirmed hack that had taken place.”²⁷⁸ Second, the platform changed the kind of enforcement action it would take against hacked materials.²⁷⁹ Instead of removing the content that was the result of a hack, Twitter would merely apply a label to the content with additional information.²⁸⁰ Finally, Twitter added considerations to the policy about what kinds of sources were distributing the content at issue.²⁸¹ Twitter realized that its previous policy failed to account for mainstream media coverage of hacking stories and only focused on stopping the hackers themselves.²⁸² The new policy would “no longer remove hacked content unless it is directly shared by hackers or those acting in concert with them.”²⁸³ In explaining this new hacked material policy, Mr. Roth testified to the Committee:

Q Okay. Did Twitter during your time there have a policy as it related to hacked materials?

A. It did. Twitter had a Distribution of Hacked Materials Policy.

Q. And when was that policy first developed?

A. To the best of my recollection, it was developed and introduced in 2018.

Q. And did it change during your time at Twitter?

A. It did. The policy was substantially changed in 2020.

Q. And how did it change in 2020?

A. Following Twitter’s decision to restrict the *New York Post*’s coverage of Hunter Biden’s laptop, the company made a decision to change the scope of Hacked Materials Policy to much more narrowly focus on situations in which there was a clearly confirmed hack that had taken place and to change the remedy under the policy from being the removal of content to the application of labels that would provide additional information.

Q. And when did this change occur?

A. The updated policy was developed in October and November of 2020. I don’t remember exactly when it was introduced within that window. To the

²⁷⁷ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 19-20.

²⁷⁸ *Id.* at 20.

²⁷⁹ *Id.* at 19-20.

²⁸⁰ *Id.*

²⁸¹ *Id.* at 21.

²⁸² *Id.*

²⁸³ Vijaya Gadde (@vijaya), X (Oct. 15, 2020, 10:06 p.m.), <https://x.com/vijaya/status/1316923557268652033>.

best of my recollection, it would have been in October 2020, but there were public announcements from the company that would have the exact date.

Q. Okay. And who at the company signed off on this change?

A. The policy was developed by me and by members of my team and ultimately was signed off on by Del Harvey and by Vijaya Gadde.

Q. Was there any part of the policy that took into account whether the source being hacked was a public figure?

A. No, that was not a consideration under the policy.

Q. Was there any part of the policy that covered whether the hacking itself was considered newsworthy?

A. That was one of the clarifications that was made in 2020, not whether the hack itself was newsworthy but the sources covering the content.

In the initial drafting of the policy, Twitter had been focused primarily on the activity that we saw in 2016, which were Russian hackers sharing it themselves. The hackers created Twitter accounts in their own personas and were directly laundering the content on social media using aliases like Guccifer 2.0 and DCLeaks.

And so we were focused on restricting that kind of direct distribution. Twitter didn't consider the possibility that the hack would take place or – excuse me – the disclosure of the hack would take place through a mainstream media outlet.²⁸⁴

But this policy update did not change the damage that had occurred: Twitter censored the article detailing the Biden family's influence peddling less than one month before an election, in part because Twitter had been primed by the FBI to expect the story would be part of a Russian hack-and-leak operation.

3. Other companies

The FBI's prebunking efforts notwithstanding, other social media platforms did not follow Facebook and Twitter's lead and came to different conclusions about how to act in response to the *New York Post* article.

In testimony before the Committee and Select Subcommittee, a member of Google's Threat Analysis Group (TAG) explained that shortly after the story was published, he and his

²⁸⁴ Transcribed Interview of Yoel Roth, H. Comm. on the Judiciary (Nov. 1, 2023) (on file with Comm.) at 19-21.

team conducted an analysis of whether the article or laptop were part of a Russian hack-and-leak operation.²⁸⁵ He testified that TAG “did not find any evidence that it was part of a foreign hack-and-leak operation.”²⁸⁶ Accordingly, YouTube “largely did nothing” to censor the *Post* story, per public reporting.²⁸⁷ The TAG member also testified that he consulted with other contacts in the industry, such as Yoel Roth at Twitter and personnel at Apple, to see if they had any evidence that the content was the result of a hack and leak, but found that those platforms had no “direct evidence of specific foreign involvement or hack-and-leak.”²⁸⁸ Google’s TAG staffer testified:

Q. Once [the *New York Post*] story was released, did your team conduct an assessment of whether materials from the story of the laptop were part of an either Russian hack-and-leak or hack-and-dump operation?

A. Yes.

Q. And what were your team’s findings?

A. My team’s findings was that we did not find any evidence that it was part of a foreign hack-and-leak operation.

Q. The story came out on October 14, 2020, early in the morning. . . . [D]o you recall how soon from when the story first broke – at least in the United States, it received a good amount of news coverage – from how soon the story first broke to when your team first began its assessment?

A. Pretty quickly.

Q. Same day?

A. Same day or day after probably.

Q. And then how long did it take your team to reach an initial assessment?

A. I’d say we did an initial assessment based on the information we had access to within a few – within hours.²⁸⁹

After completing its analysis, TAG communicated the finding to Google’s Vice President of Trust and Safety.²⁹⁰ The TAG staffer testified that later the same day, he was asked to join a call with the Vice President of Trust and Safety and “a number of other VPs and some lawyers

²⁸⁵ Transcribed Interview of the Senior Director of Google’s Threat Analysis Group, H. Comm. on the Judiciary (July 19, 2023) (on file with Comm.) at 23-26.

²⁸⁶ *Id.*

²⁸⁷ *A Misinformation Test for Social Media*, N.Y. TIMES (Oct. 21, 2020); *see also* Siva Vaidhyanathan, *The Hunter Biden story was a test for tech platforms. They barely passed*, THE GUARDIAN (Oct. 19, 2020).

²⁸⁸ Transcribed Interview of the Senior Director of Google’s Threat Analysis Group, H. Comm. on the Judiciary (July 19, 2023) (on file with Comm.) at 28.

²⁸⁹ *Id.* at 23-24.

²⁹⁰ *Id.* at 24.

from various products,” including YouTube, to provide a short verbal brief on TAG’s understanding of the article and to answer a few questions.²⁹¹ According to his testimony, questions during this call revolved around whether TAG had found evidence of a foreign hack and leak or heard of any evidence from industry partners.²⁹² The TAG staffer testified that he had not found any direct evidence of a foreign hack-and-leak operation, nor had he received any from industry contacts at other companies.²⁹³ He testified that “the only thing I heard was speculation. I hadn’t heard any evidence” from others in the industry.²⁹⁴

Today, Facebook and Twitter point to the FBI’s warnings when explaining their censorship decisions.²⁹⁵ But other companies’ approach shows that even with the FBI’s prebunking, if Facebook and others had followed their proper protocols, the *New York Post* story should have never been censored.²⁹⁶

Because the FBI primed platforms to look out for a Russian hack and leak targeting the Bidens and Burisma, when the *Post* story was published, some platforms jumped at the chance to censor it and failed to follow all of their applicable policies or the evidence. “[T]rigger happy” companies like Facebook and Twitter “made decisions that should not have been made individually and without consultation.”²⁹⁷

D. FBI continued to withhold information as Big Tech continued to reach out.

In the days following the publication of the *Post* article on Biden family influence peddling, social media platforms continued to seek new information or additional clarity from the FBI. Despite repeated requests, the FBI continually refused to provide more details.

²⁹¹ *Id.* at 26.

²⁹² *Id.* at 28.

²⁹³ *Id.*

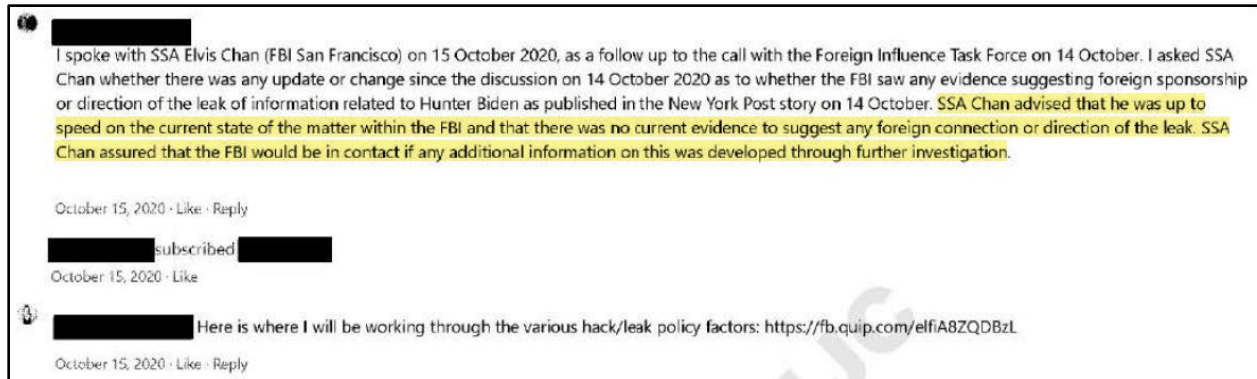
²⁹⁴ *Id.*

²⁹⁵ *See, e.g.*, Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he FBI warned us about a potential Russian disinformation operation about the Biden family and Burisma in the lead up to the 2020 election. . . . It’s since been made clear that the [*New York Post*] reporting was not Russian disinformation, and in retrospect, we shouldn’t have demoted the story.”); Declaration of Yoel Roth, ¶¶ 10–11, Federal Elections Comm’n MUR 7821 (Dec. 17, 2020).

²⁹⁶ *See, e.g.*, Transcribed Interview of Google’s Director of Global Elections Integrity, H. Comm. on the Judiciary (May 22, 2023) (on file with Comm.) at 72. While Alphabet did not censor the *Post* story, they have generally been just as censorious as other platforms. The Committee and Select Subcommittee have demonstrated that in 2021, YouTube altered its content moderation policies at the behest of the Biden-Harris Administration. *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 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). More recently, Google Search’s autocomplete function suppressed information about the July 13, 2024 assassination attempt on President Donald Trump, and YouTube censored a video in which former FBI agent Marcus Allen, a Select Subcommittee witness, described his religious and political beliefs and prayed the rosary. *See* Letter from Rep. Jim Jordan, Chairman, H. Comm on the Judiciary, to Sundar Pichai, CEO, Alphabet (Aug. 5, 2024); Letter from Rep. Jim Jordan, Chairman, H. Comm on the Judiciary, to Sundar Pichai, CEO, Alphabet (Oct. 7, 2024).

²⁹⁷ Internal messages among Facebook personnel (Oct. 14, 2020. 1:39 p.m.), *see* Ex. 115.

On October 15, 2020, a Facebook employee (and former FITF official) called Elvis Chan “as a follow up to the call with the Foreign Influence Task Force on 14 October.”²⁹⁸ The Facebook employee reported back to his colleagues in an internal message thread that he “asked SSA Chan whether there was any update or change since the discussion . . . as to whether the FBI saw any evidence suggesting foreign sponsorship or direction of the leak of information related to Hunter Biden.”²⁹⁹ Chan told the Facebook employee that he (Chan) was “up to speed” on what the FBI knew and “that there was no current evidence to suggest any foreign connection or direction of the leak.”³⁰⁰ Chan assured the Facebook employee that he “would be in contact” if any additional information came to light.³⁰¹



“SSA Chan advised that . . . there was no current evidence to suggest any foreign connection or direction of the leak”
 —Oct. 15, 2020, internal messages among Facebook personnel

The same day, key Facebook decision-makers communicated about hearing “murmurs from the IC [intelligence community] substantiating the Burisma hack” and “the concern that this would be dumped in an October surprise.”³⁰²

²⁹⁸ Internal messages among Facebook personnel (Oct. 15, 2020), *see* Ex. 117.

²⁹⁹ *Id.*

³⁰⁰ *Id.*

³⁰¹ Internal messages among Facebook personnel (Oct. 15, 2020), *see* Ex. 117; *see also* Emails between Facebook personnel and FBI personnel (Oct. 15, 2020, 10:03 a.m.), Ex. 118; Internal messages among Facebook personnel (Oct. 15, 2020, 5:14 p.m.), Ex. 119.

³⁰² Internal messages among Facebook personnel (Oct. 15, 2020, 8:56 a.m.), *see* Ex. 120.

Message

From: [REDACTED]@fb.com
 Sent: 10/15/2020 12:40:59 PM
 To: [REDACTED]@fb.com; Joel Kaplan [REDACTED]@fb.com; [REDACTED]@fb.com; [REDACTED]@fb.com; [REDACTED]@fb.com; [REDACTED]@fb.com
 Subject: Message summary [{"otherUserFbId":null,"threadFbId":3268602856582649}]

[REDACTED] (10/15/2020 05:56:35 PDT):
 >@silent FYI: starting to get stronger murmurs from the IC substantiating the Burisma hack by the GRU and the concern that this would be dumped in an October surprise. Nothing definite yet (and certainly nothing to share w/Rubio), but multiple sources beginning to strengthen the possible link to Russian actors.

Joel D. Kaplan (10/15/2020 05:57:59 PDT):
 >@silent The NY Post is running stories this am with emails about dealings with China. Are the rumors about the entire database of emails, or just about emails related to Burisma?

[REDACTED] (10/15/2020 06:00:23 PDT):
 >@silent about a specific, substantiated Burisma hack, then those emails behind combined with (a) other stolen Biden files; and (b) manipulated files mixed in among them.

[REDACTED] (10/15/2020 06:07:41 PDT):
 >@silent it's worth noting, though, there has been separate reporting of a hack of a prominent law firm that repped Biden, among others. That's another possible source of some of this info. I'll keep an eye as the community digs into this, and flag if we see analysis develop today.

“FYI: starting to get stronger murmurs from the IC substantiating the Burisma hack”
 —Oct. 15, 2020, internal messages among Facebook personnel

Three days later, on October 18, 2020, a Facebook employee reached out to the Russia Unit Chief of the FITF flagging a story furthering the false Russian hack-and-leak narrative, asking “does that change anything in your posture?”³⁰³ The Russia Unit Chief asked for the Facebook employee to give him a call to discuss, still failing to reveal that the FBI possessed and had authenticated Hunter Biden’s laptop.³⁰⁴

Facebook reached out to the FBI for additional information repeatedly. But rather than telling the companies that it was in possession of the laptop, the FBI repeatedly fed the platform its pre-approved message: “The FBI has nothing in its possession to suggest that the laptop is a hack or a leak.”³⁰⁵ Of course, the FBI did not have information suggesting the laptop was a hack or a leak; to the contrary, the FBI possessed and had authenticated the laptop, so “at that time . . . knew . . . the laptop was not hacked.”³⁰⁶

The FBI was not the only government actor that tried to muddy the waters surrounding the provenance of the laptop—the intelligence community also tried to falsely paint this story as a Russian influence operation. On October 19, 2020, fifty-one former intelligence officials issued

³⁰³ Emails between FBI staff to Facebook employee (Oct. 18, 2020, 1:36 p.m.), *see* Ex. 121; *see also* Allison Quinn, *Rudy’s ‘Russian Agent’ Pal Teases ‘Second Laptop’ With Hunter Biden Kompromat*, THE DAILY BEAST (Oct. 18, 2020).

³⁰⁴ *Id.*

³⁰⁵ Transcribed Interview of the Russia Unit Chief of the FITF, H. Comm. on the Judiciary (May 2, 2024) (on file with Comm.) at 84.

³⁰⁶ *Id.* at 83-84.

a statement falsely claiming that the Biden family influence peddling story bore all the hallmarks of a Russian influence operation.³⁰⁷ As the Committee has detailed in two reports coauthored with the House Permanent Select Committee on Intelligence, the statement was a coordinated influence operation set in motion by a senior Biden campaign official, now-Secretary of State Antony Blinken.³⁰⁸ High-level CIA officials—up to and potentially including then-Director Gina Haspel—were made aware of the statement before its publication.³⁰⁹

Companies asked repeatedly for more information about the laptop in the days following the *Post* article. The intelligence community colluded to falsely dismiss the story about Biden family influence peddling as Russian disinformation. And still, the FBI sat on the one fact that could have ended the confusion and set the record straight: the FBI was in possession of the laptop and had authenticated its contents. The FBI's failure to do so ensured that platforms continued to censor—a potentially election-altering decision.

³⁰⁷ 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 (Comm. Print June 25, 2024); 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 HUNTER BIDEN STATEMENT: HOW SENIOR INTELLIGENCE COMMUNITY OFFICIALS AND THE BIDEN CAMPAIGN WORKED TO MISLEAD AMERICAN VOTERS (Comm. Print May 10, 2023); *see also* Brooke Singman, *Biden campaign, Blinken orchestrated intel letter to discredit Hunter Biden laptop story, ex-CIA official says*, FOX NEWS (Apr. 20, 2023).

³⁰⁸ *Id.*

³⁰⁹ 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 (Comm. Print June 25, 2024) at 2.

IV. Epilogue: The fight against FBI election interference continues

The FBI, through the FITF, engaged in a months-long campaign to influence the 2020 election by prebunking the story about Biden family influence peddling, as supported by material recovered from Hunter Biden’s laptop. In over thirty meetings with social media platforms before October 14, 2020, the FBI primed the Big Tech platforms for exactly what would happen: shortly before the election, an established media outlet would publish an article about documents implicating the Biden family and Burisma in a far-reaching influence peddling scheme. Then, when the *Post* published that very story, Big Tech did what the FBI had been priming them to do for months and censored the story.

Since 2020, independent watchdogs have criticized the lack of protocol that allowed the FBI to successfully prebunk the true *Post* story. In July 2024, the Office of the Inspector General of the Department of Justice (DOJ OIG) found that the FITF operates in a “risky legal space” because social media companies may feel compelled to censor speech at its behest.³¹⁰ In the same report, the DOJ OIG concluded that in 2020, the Justice Department and the FBI did not have adequate guardrails governing the FITF’s interactions with Big Tech: “neither the Department nor the FBI had a specific policy or guidance applicable to information sharing with social media companies.”³¹¹

In January 2024, the FBI issued a Standard Operating Procedure (SOP) to govern its discussions with social media companies about content moderation and to formalize steps for sharing information with social media companies.³¹² This SOP requires FBI personnel to include a lengthy disclaimer telling social media companies that “no adverse action will be taken by the FBI based on your company’s decision about whether or how to respond” to the FBI’s communications.³¹³ FBI personnel also are not permitted to ask social media companies what actions have been taken in response to FBI communications.³¹⁴ The DOJ and FBI have refused to make the SOP publicly available and provide the American public with transparency into how the country’s most powerful law enforcement agency attempts to self-regulate its interactions with the companies hosting the modern town square.³¹⁵

While this SOP marks an improvement over the previous protocol (or lack thereof), it does not allay the Committee’s concern that the FBI may be continuing to coerce platforms to censor content. Platforms undoubtedly remain aware of the FBI’s enforcement powers and retaliation capacity. As Stanford Internet Observatory Director Alex Stamos testified to the

³¹⁰ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, NO. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024), at 18.

³¹¹ *Id.* at 8.

³¹² *Id.*

³¹³ COUNTERINTELLIGENCE DIV., FEDERAL BUREAU OF INVESTIGATION, PROVIDING FOREIGN MALIGN INFLUENCE THREAT INFORMATION TO SOCIAL MEDIA PLATFORMS (STANDARD OPERATING PROCEDURE) (Jan. 2024), *see* Ex. 125.

³¹⁴ *Id.*

³¹⁵ *Id.*

Committee, “you can’t have a casual chat with an FBI agent when you’re an executive at a company. It’s not safe.”³¹⁶

The coordination meetings between the FBI and Big Tech stopped for a brief time after the U.S. District Court for the Western District of Louisiana issued, and a unanimous panel of the U.S. Court of Appeals for the Fifth Circuit largely affirmed, a preliminary injunction against the DOJ and FBI that prohibited them from coercing or significantly encouraging social media companies to censor lawful content.³¹⁷ This injunction prevented the FBI and various other federal agencies from having contact with Big Tech regarding the moderation of lawful content.

Unfortunately, the same meetings that led to the prebunking of the laptop story in 2020 have resumed in 2024.³¹⁸ After the Supreme Court stayed the lower courts’ injunction,³¹⁹ the FITF “resumed outreach” to social media companies sometime in early 2024.³²⁰ According to an FBI spokesperson, the purpose of this outreach is “to facilitate sharing information about foreign malign influence with social media companies”—the same mandate that facilitated the FBI’s prebunking of the *Post* story.³²¹ Given this past misconduct, it is concerning that the FBI is once again engaging in a similar manner with the entities responsible for administering the digital town square.

During the course of its investigation, the Committee has issued subpoenas for documents to agencies and companies involved in the prebunking campaign, including the DOJ, the FBI, and major social media and technology platforms.³²² Because the subpoenas are continuing in nature, they require these entities to turn over documents relating to the current, ongoing meetings on a rolling basis.

As these meetings have occurred in 2024, the Committee and Select Subcommittee have begun to receive documents from many platforms and agencies.³²³ These documents show that,

³¹⁶ Transcribed Interview of Alex Stamos, H. Comm. on the Judiciary (June 23, 2023) (on file with Comm.) at 188.

³¹⁷ Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

³¹⁸ *Id.*

³¹⁹ *See* *Murthy v. Missouri*, No. 23A243 (23-411), 601 U.S. ___, (Oct. 13, 2023) (granting application for stay); *but see* *Murthy v. Missouri* 601 U.S. ___ (Oct. 20, 2023) (Alito, J., dissenting) (“At this time in the history of our country, what the Court has done, I fear, will be seen by some as giving the Government a green light to use heavy-handed tactics to skew the presentation of views on the medium that increasingly dominates the dissemination of news. That is most unfortunate.”).

³²⁰ Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

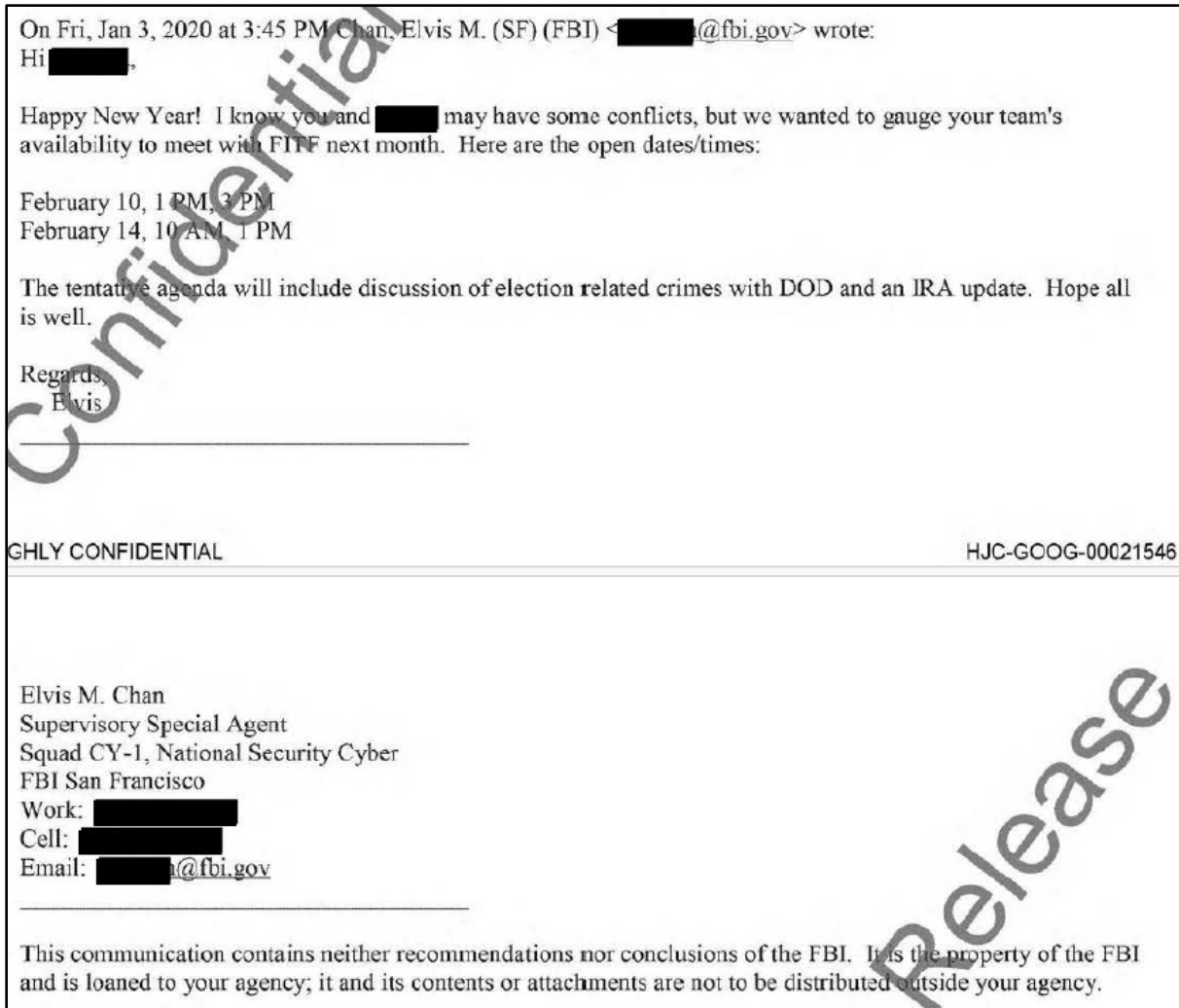
³²¹ *Id.*

³²² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Merrick Garland, Att’y Gen., Dep’t of Justice (Aug. 17, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Jen Easterly, Dir., Cybersecurity and Infrastructure Security Agency (Apr. 28, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mark Zuckerberg, CEO, Meta (Feb. 15, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Sundar Pichai, CEO, Alphabet (Feb. 15, 2023) (attaching subpoena) (on file with Comm.); Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Satya Nadella, CEO, Microsoft (Feb. 15, 2023) (attaching subpoena) (on file with Comm.).

³²³ *See, e.g.*, Email from FBI staff to Facebook personnel (Apr. 24, 2024, 10:26 a.m.), Ex. 122.

as in 2020, Elvis Chan remains the primary point of contact at the FBI for the meetings.³²⁴ They also show that the FBI, consistent with its new SOP, has added a more robust disclaimer at the end of its emails about the ostensibly voluntary nature of social media companies' interactions with the FBI.³²⁵

Previously, the FBI only sometimes included a disclaimer in its communications with Big Tech.³²⁶ When it did so, the disclaimer was only two sentences long and stated that the information provided contained “neither the recommendations nor conclusions of the FBI” and that the contents were the property of the FBI and were not to be distributed.³²⁷



“This communication contains neither the recommendations nor conclusions of the FBI. . . . it and its contents or attachments are not to be distributed outside your agency.”

—Jan. 3, 2020, email from Elvis Chan to Google, showing the FBI’s disclaimer at the time

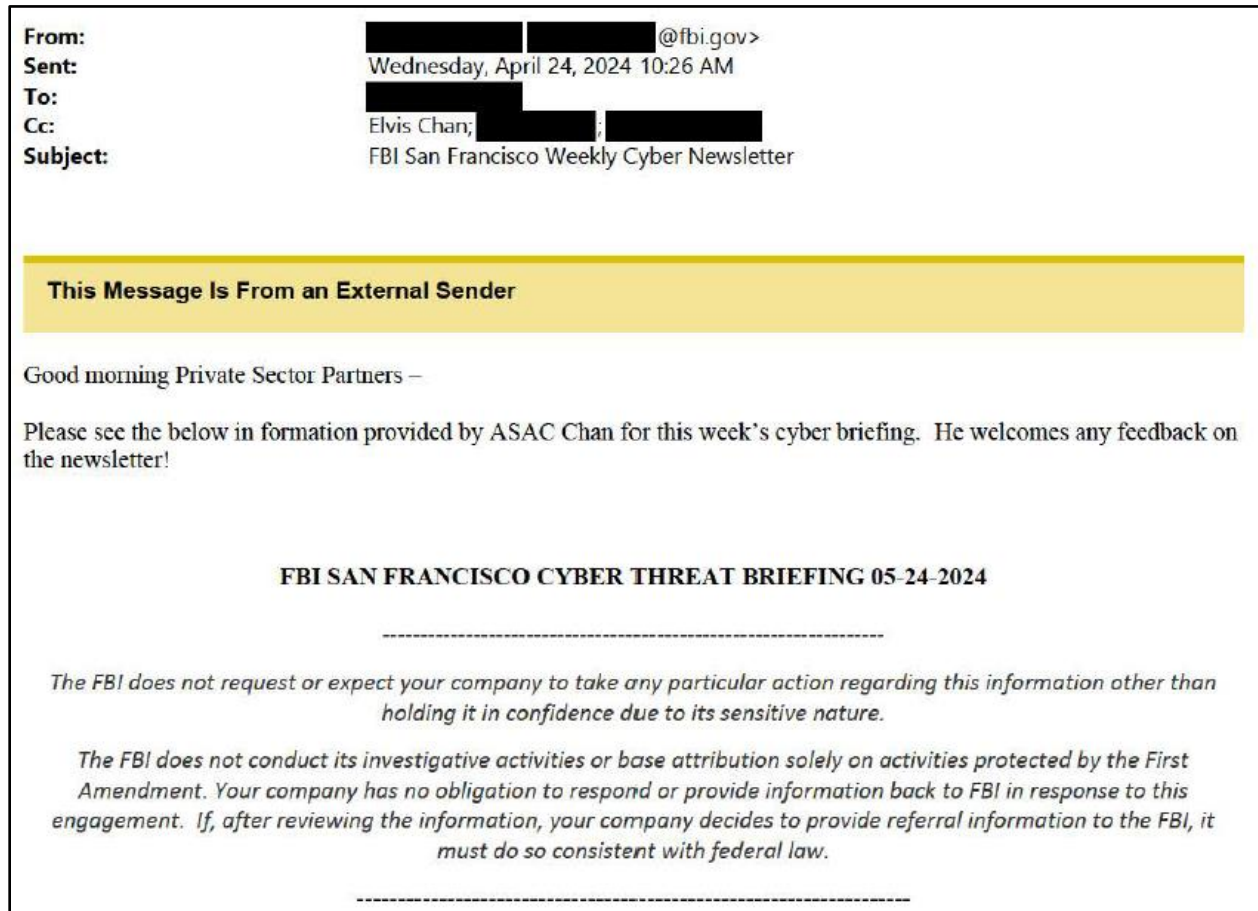
³²⁴ *Id.*

³²⁵ *Id.*

³²⁶ See Email from Elvis Chan to Google personnel (Jan. 6, 2020, 3:45 p.m.); Ex. 15.

³²⁷ *Id.*

In the wake of the Committee’s and Select Subcommittee’s oversight, and increased public attention on the FBI’s censorship activities in 2020, the FBI appended a new disclaimer to its emails with Big Tech. The new disclaimer is twice as long and attempts to assure social media companies that they have “no obligation to respond or provide information back to FBI” in response to its outreach.³²⁸



“The FBI does not request or expect your company to take any particular action regarding this information other than holding it in confidence due to its sensitive nature.”

—Apr. 24, 2024 email from FBI staff to Facebook personnel

The disclaimer, by itself, does not sufficiently resolve the First Amendment implications created by federal law enforcement engaging with Big Tech. Social media platforms, like any company, have a strong incentive to comply with requests from the FBI given its enforcement powers.³²⁹ So long as the FBI continues to engage with the companies that provide and oversee

³²⁸ Email from FBI staff to Facebook personnel (April 24, 2024, 10:26 a.m.); see Ex. 122.

³²⁹ See generally OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, NO. 24-080, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE’S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS (July 2024).

the digital town square, the risk of government infringement on Americans' free expression will remain.³³⁰

* * *

Documents and testimony obtained by the Committee and Select Subcommittee show the FBI's interactions with Big Tech in the months, weeks, days, and hours leading up to and surrounding the publication of the *New York Post*'s explosive October 14, 2020 story about Biden family influence peddling. Internal documents from Big Tech in particular show a months-long FBI campaign priming Big Tech companies to expect a Russian hack and leak about Hunter Biden and Burisma shortly before the election. When the true *Post* story matching the FBI's warnings emerged, the Big Tech companies followed the FBI's specific warnings and censored it, despite internal concerns that the story might not have been the product of a hack and leak. Even when it became clear the story was not Russian disinformation, Facebook and other platforms continued to censor the story out of concerns of how they may be viewed by a future Biden-Harris Administration. For a pivotal week, the most important story of the 2020 presidential election was censored.

The Committee and Select Subcommittee will continue to conduct oversight of the FBI's interactions with social media companies regarding content moderation. The modern town square must be free from direct and indirect government pressure. Government involvement will necessarily distort debate and lead to devastating policy outcomes.³³¹ A prosperous and functioning democracy depends on free expression so that ideas and viewpoints succeed and fail on their merits. The First Amendment demands nothing less.

³³⁰ *Id.*

³³¹ 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 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).

V. Appendix

Table of Contents

Exhibit 1: Internal emails among Facebook personnel (Sept. 21, 2020).....	83
Exhibit 2: Internal message from Facebook personnel to Nick Clegg (Oct. 15, 2020).....	87
Exhibit 3: Microsoft internal meeting notes (Oct. 14, 2020).....	89
Exhibit 4: Internal messages among Facebook personnel (Oct. 14, 2020).....	91
Exhibit 5: Internal messages among Facebook personnel (Oct. 14, 2020).....	99
Exhibit 6: Internal messages among Facebook personnel (Oct. 14, 2020).....	102
Exhibit 7: Internal messages among Facebook personnel (Oct. 14, 2020).....	104
Exhibit 8: Internal messages among Facebook personnel (Oct. 14, 2020).....	117
Exhibit 9: Internal messages among Facebook personnel (Oct. 14, 2020).....	119
Exhibit 10: Internal messages among Facebook personnel (July 15, 2020).....	155
Exhibit 11: Statement from tech industry participants.....	157
Exhibit 12: Internal messages among Facebook personnel (Aug. 5, 2020).....	159
Exhibit 13: Internal messages among Facebook personnel (Sept. 20, 2020).....	166
Exhibit 14: Internal messages among Facebook personnel (Oct. 13, 2020).....	169
Exhibit 15: Emails between Google personnel and FBI staff (Jan. 6, 2020).....	173
Exhibit 16: Internal emails among Facebook personnel (Oct. 14, 2020).....	176
Exhibit 17: Email from FBI Counsel to Google personnel (Jan. 31, 2020).....	180
Exhibit 18: Emails between FBI and Microsoft personnel (Jan. 9, 2020).....	182
Exhibit 19: Email between Elvis Chan and Yahoo personnel (Feb. 12, 2020).....	185
Exhibit 20: Email between Elvis Chan and Yahoo personnel (Apr. 13, 2020).....	188
Exhibit 21: Emails between Elvis Chan and Google personnel (Apr. 14, 2020).....	191

Exhibit 22: Scheduling emails between FBI and Facebook personnel (May 12, 2020).....	193
Exhibit 23: Emails between Elvis Chan and Yahoo personnel (May 18, 2020).....	195
Exhibit 24: Scheduling emails between LinkedIn and FBI personnel (May 20, 2020).....	197
Exhibit 25: Emails between Elvis Chan and Yahoo personnel (July 14, 2020).....	200
Exhibit 26: Emails between Elvis Chan and Google personnel (July 14, 2020).....	204
Exhibit 27: Emails between Elvis Chan and Google personnel (July 14, 2020).....	208
Exhibit 28: Emails between Elvis Chan and Yahoo personnel (July 24, 2020).....	211
Exhibit 29: Scheduling emails between FBI and Facebook personnel (Aug. 10, 2020).....	215
Exhibit 30: Emails between FBI and Facebook personnel about FITF meeting attendees (Aug. 11, 2020).....	219
Exhibit 31: Scheduling emails between LinkedIn and FBI personnel (July 14 – Aug. 12, 2020)	224
Exhibit 32: Emails between Elvis Chan and LinkedIn personnel (Sept. 10, 2020).....	227
Exhibit 33: Emails between Elvis Chan and Google personnel (Sept. 10-11, 2020).....	231
Exhibit 34: Emails between Elvis Chan and Yahoo personnel (Sept. 14, 2020).....	234
Exhibit 35: Emails between Elvis Chan and Google personnel (Sept. 18, 2020).....	238
Exhibit 36: Scheduling emails between FBI and Facebook personnel (Sept. 10-21, 2020).....	240
Exhibit 37: Scheduling emails between Elvis Chan and LinkedIn personnel (Sept. 10-22, 2020)	246
Exhibit 38: Emails between Elvis Chan and Yahoo personnel (Sept. 24, 2020).....	250
Exhibit 39: Emails between Elvis Chan and Google personnel (Sept. 29, 2020).....	254
Exhibit 40: Emails between Elvis Chan and Google personnel (Sept. 29 – Oct. 14, 2020)	257
Exhibit 41: Emails between Elvis Chan and LinkedIn personnel (Sept. 29 – Oct. 13, 2020)	260

Exhibit 42: Emails from FBI to Big Tech participants scheduling FITF Bilateral meetings (Oct. 2020).....	263
Exhibit 43: Internal messages among Facebook personnel (Oct. 14, 2020).....	329
Exhibit 44: Internal FBI meeting summary notes from Twitter-FITF meeting (Oct. 14, 2020)	333
Exhibit 45: Emails between Google personnel and FBI staff (Apr. 20, 2020).....	358
Exhibit 46: Emails between Brian Scully and industry participants (May 11-12, 2020).....	361
Exhibit 47: Scheduling emails from Facebook personnel to industry group (May 13, 2020)	366
Exhibit 48: Internal Facebook readout of USG-Industry meeting (May 14, 2020).....	368
Exhibit 49: Agenda emails between industry participants (June 9, 2020).....	370
Exhibit 50: Scheduling email from Facebook personnel to industry group (June 9, 2020).....	373
Exhibit 51: Scheduling email from Google personnel to industry group (June 10, 2020).....	377
Exhibit 52: Internal messages among Facebook personnel (June 30, 2020).....	379
Exhibit 53: Internal Facebook readout of the USG-Industry meeting (June 10, 2020).....	382
Exhibit 54: Internal messages among Facebook personnel (July 1, 2020).....	384
Exhibit 55: Internal messages among Facebook personnel (July 10, 2020).....	386
Exhibit 56: Internal messages among Facebook personnel (Oct. 14, 2020).....	388
Exhibit 57: Scheduling email from Google personnel to industry group (July 15, 2020).....	394
Exhibit 58: Internal Facebook readout of the USG-Industry meeting (July 17, 2020).....	396
Exhibit 59: Scheduling email from Google personnel to industry group (Aug. 12, 2020).....	398
Exhibit 60: Internal Facebook readout of the USG-Industry meeting (Aug. 13, 2020).....	400
Exhibit 61: Agenda emails between industry participants (Sept. 11, 2020).....	408
Exhibit 62: Scheduling email from Facebook personnel to industry group (Sept. 11, 2020)	411

Exhibit 63: Agenda emails between CISA and Facebook personnel (Sept. 1-15, 2020).....	413
Exhibit 64: Scheduling email from Google personnel to industry group (Sept. 16, 2020)...	418
Exhibit 65: Internal Facebook notes about USG-Industry meeting (Sept. 16, 2020).....	420
Exhibit 66: Agenda email between CISA and Facebook personnel (Sept. 9, 2020).....	424
Exhibit 67: Agenda emails between CISA and Facebook personnel (Sept. 29 – Oct. 5, 2020)	426
Exhibit 68: Scheduling email from Facebook personnel to industry group (Oct. 7, 2020)...	429
Exhibit 69: Emails between Elvis Chan and Reddit personnel (Sept. 29, 2020).....	431
Exhibit 70: Emails between Elvis Chan and Yahoo personnel (Sept. 29, 2020).....	434
Exhibit 71: USG-Industry meeting invitation (July 8, 2020).....	438
Exhibit 72: USG-Industry meeting invitation (Sept. 9, 2020).....	440
Exhibit 73: USG-Industry meeting invitation (Oct. 21, 2020).....	443
Exhibit 74: USG-Industry meeting invitation (Oct. 28, 2020).....	447
Exhibit 75: Internal Facebook emails between Mark Zuckerberg, Sheryl Sandberg, and Facebook personnel (Oct. 5, 2020).....	451
Exhibit 76: USG-Industry meeting agenda (July 14, 2020).....	454
Exhibit 77: USG-Industry meeting invitation (July 14, 2020).....	457
Exhibit 78: Internal Facebook readout of USG-Industry meeting (Sept. 17, 2020).....	461
Exhibit 79: Internal messages among Facebook personnel (Oct. 14, 2020).....	463
Exhibit 80: Internal Facebook readout of USG-Industry meeting (Oct. 8, 2020).....	465
Exhibit 81: Internal messages among Facebook personnel (Sept. 9, 2020).....	467
Exhibit 82: Internal messages among Facebook personnel (Sept. 18, 2020).....	475
Exhibit 83: Internal messages among Facebook personnel (Sept. 21, 2020).....	479
Exhibit 84: Emails between Google personnel and Democratic National Committee staff (Aug. 5, 2020).....	485

Exhibit 85: Emails between Facebook personnel and DNI staff (Sept. 24, 2020).....	488
Exhibit 86: Aspen Digital Hack-and-leak Roundtable agenda (June 25, 2020).....	491
Exhibit 87: Aspen Digital Hack-and-leak Roundtable meeting readout (July 2, 2020).....	493
Exhibit 88: Memo from Aspen Institute roundtable	495
Exhibit 89: Emails from Aspen Institute staff to industry participants (July 14, 2020).....	499
Exhibit 90: Emails from Aspen Institute staff to industry participants (June 22, 2020).....	501
Exhibit 91: Emails between Aspen Institute and Facebook personnel (May 6-19, 2020)....	504
Exhibit 92: Emails between Aspen Institute, Facebook, and Stanford personnel (June 15-25, 2020).....	507
Exhibit 93: Emails between Aspen Institute and Facebook personnel (July 13, 2020).....	513
Exhibit 94: Email from Aspen Institute personnel to Facebook personnel (Sept. 28, 2020)	516
Exhibit 95: Aspen Digital Hack-and-leak Roundtable participant list (June 25, 2020).....	518
Exhibit 96: Email from Aspen Institute staff to industry participants (Aug. 2, 2020).....	521
Exhibit 97: Internal messages among Facebook personnel (Sept. 20, 2020).....	523
Exhibit 98: Email from Aspen Institute personnel to Facebook and Twitter personnel (Aug. 7, 2020).....	528
Exhibit 99: Emails from Aspen Digital staff to Roundtable participants (Aug. 12 – Sept. 1, 2020)	530
Exhibit 100: Aspen Digital Hack-and-Dump Scenario Outline (Sept. 2020).....	533
Exhibit 101: Messages between Nick Clegg and Joel Kaplan (Oct. 14, 2020).....	538
Exhibit 102: Internal Facebook Hack/Leak Policy Assessment (Oct. 20, 2020).....	542
Exhibit 103: Internal messages among Facebook personnel (Oct. 14, 2020).....	553
Exhibit 104: Internal messages among Facebook personnel (Oct. 14, 2020).....	555
Exhibit 105: Internal messages among Facebook personnel (Oct. 14, 2020).....	557

Exhibit 106: Internal messages among Facebook personnel (Oct. 14, 2020).....	560
Exhibit 107: Internal messages among Facebook personnel (Oct. 14, 2020).....	562
Exhibit 108: Internal messages among Facebook personnel (Oct. 14, 2020).....	568
Exhibit 109: Internal messages among Facebook personnel (Oct. 14, 2020).....	578
Exhibit 110: Internal messages among Facebook personnel (Oct. 14, 2020).....	580
Exhibit 111: Internal email between Facebook employees (Oct. 14, 2020).....	583
Exhibit 112: Email from Elvis Chan to Google personnel (Jan. 3, 2020).....	585
Exhibit 113: Internal messages among Facebook personnel (Oct. 14, 2020).....	587
Exhibit 114: Internal messages among Facebook personnel (Oct. 14, 2020).....	594
Exhibit 115: Internal messages among Facebook personnel (Oct. 14, 2020).....	596
Exhibit 116: Internal messages among Facebook personnel (Oct. 14, 2020).....	601
Exhibit 117: Internal messages among Facebook personnel (Oct. 14, 2020).....	606
Exhibit 118: Emails between Facebook personnel and FBI personnel (Oct. 15, 2020).....	610
Exhibit 119: Internal messages among Facebook personnel (Oct. 15, 2020).....	612
Exhibit 120: Internal messages among Facebook personnel (Oct. 15, 2020).....	618
Exhibit 121: Email from FBI staff to Facebook employee (Oct. 18, 2020).....	620
Exhibit 122: Email from FBI staff to Facebook personnel (April 24, 2024).....	622
Exhibit 123: Email between Atlantic Council personnel (July 20-31, 2020).....	625
Exhibit 124: Emails among tech industry participants (Sept. 15, 2020).....	629
Exhibit 125: FBI Standard Operating Procedure: Providing Foreign Malign Influence Threat Information to Social Media Platforms (2024).....	633

Appendix

Exhibit 1

hack/leak operation conducted by Russian actors, likely involving real or manufactured evidence concerning links between the Biden family and Ukraine, including the oil company Burisma. Timing for something like this is uncertain, but could happen as soon as the first presidential debate on September 29th. While this assessment is still uncertain, an inoculating announcement about hack/leak now will mitigate the impact of such a leak if it does occur, and send a strong message about Facebook's proactive stance even if no such leak materializes.

Comms Plan: We are planning to announce these three networks off cycle on Thursday, they will also be included in our September report in early October. Because we know that one of the most effective techniques to counter a hack/leak is to inoculate the audience *before* the leak, we plan to act quickly here out of an abundance of caution, and use this takedown to both inform the public of our findings and the hack/leak risk and reassure them that we are on top of it. We plan to frame our public statements carefully to raise awareness, but neither hyperbolize the threat, nor guarantee that such an operation will occur. To land this narrative, we're engaging external researchers and pundits to inform their commentary and raise the importance of responsible coverage of hack/leak operations. We're working to land this story with broadcast and wires to amplify and shape our coverage.

We are working with the following XFN partners as we prepare to disrupt and announce these networks i3/Threat Intelligence (██████████, ██████████, ██████████, ██████████), Security Policy (██████████, ██████████), Security Comms (██████████), Legal (██████████, ██████████), Product (██████████), GSII (██████████), US Public Policy (██████████), EMEA Comms (██████████, ██████████), (EMEA Public Policy (██████████, ██████████, ██████████)). *Note: Due to the speed here, we are still in the process of getting alignment from all of the local teams.*

The three Russian networks include:

1. A Russia-origin network linked to Russian military intelligence that focused on primarily on Syria and Ukraine, but also on Turkey, Japan, Armenia, Georgia, Belarus, Moldova, and to the smallest extent on the UK and the US;
2. A Russia-origin network linked to individual(s) associated with past activity by the Russian Internet Research Agency (IRA) that focused primarily on Turkey and the EU, and also on the United States;
3. A Russia-origin network that focused broadly on global geopolitical issues, and more specifically on Belarus

DETAIL

Note: The below asset and follower figures are still awaiting the dashboard table to land and may be subject to limited changes.

1. **[FGI] Russia:** A network of 214 Facebook accounts, 35 Pages, 18 Groups, and 34 Instagram accounts originating in Russia and focused primarily on Syria and Ukraine, and also on Turkey, Japan, Armenia, Georgia, Belarus, Moldova, and to the smallest extent on the UK and the US. We identified several clusters of connected activity that relied primarily on fake accounts — many of which had been continuously detected and removed by our automated detection systems. Many of these accounts have been inactive on the platform. Others posed as locals in countries they targeted and journalists to contact news organizations, drive people to off-platform sites and and amplify their own content on other social media platforms. This network was proactively identified by our investigative teams as they continued to track the activity of actors we had removed in August 2018 and February 2020. Our investigation found links to Russian military including military intelligence services.
 1. Actor/Origin: Russia (Russia military intelligence services)
 2. Target(s): primarily on Syria and Ukraine, but also on Turkey, Japan, Armenia, Georgia, Belarus, Moldova, and to the smallest extent on the UK and the US
 3. Followers: *Stats and numbers are pending as we await data tables to land. Our initial indications show these follower numbers were limited — fewer than 10,000 each.*
 4. Ads: *Stats and numbers are pending as we await data tables to land.*
 5. External Researcher: Graphika
2. **[FGI] Russia:** A network of 5 Facebook accounts, 1 Page, 1 Group, and 3 Instagram accounts originating in Russia and focused on on Turkey and the EU, and also on the United States. This operation relied on fake accounts, some of which had been already detected and disabled by our automated systems — to manage their Page and their Group, and to drive people to their off-platform site masquerading as an independent think-tank based primarily in Turkey. We began this investigation based on information about this network's off-platform activity from the FBI. Our investigation found links to individuals associated with past activity by the Russian Internet Research Agency (IRA).
 1. Actor/Origin: Russia (individuals associated with past activity by the Russian Internet Research Agency (IRA))
 2. Target(s): on Turkey and the EU, and also on the United States
 3. Followers: *Stats and numbers are pending as we await data tables to land. Our initial indications show these follower numbers were limited — fewer than 6,000 each.*

4. Ads: Stats and numbers are pending as we await data tables to land.
 5. External Researcher: Stanford
3. **[FG] Russia**: A network of 23 Facebook accounts, 7 Pages, and 8 Instagram accounts originating in Russia and focused broadly on global geopolitical issues, and specifically on Belarus. We identified several clusters of connected activity that used fake accounts to post and comment on content, manage Pages of the Strategic Culture Foundation, and amplify its content. This network posted primarily in Russian and English about news and current events in countries targeted by this activity. Our attribution will be to "individuals in Russia."
1. Actor/Origin: Russia
 2. Target(s): Global, Belarus
 3. Followers: Stats and numbers are pending as we await data tables to land. We do not yet have initial indications around these follower counts.
 4. Ads: Stats and numbers are pending as we await data tables to land.
 5. External Researcher: DFRLab

Industry Partner Actions: We will be sharing information about these networks with our industry partners.

Law Enforcement Outreach: We received several tips for some of this activity from our LE partners and we will be citing those references where it is appropriate. On Tuesday morning, we plan to brief the FBI's Foreign Influence Task Force (FITF) on these cases and our planned announcement. We are planning to push our LE partners to disclose more publicly as well.

External Researchers: We plan to share these networks with researchers at Graphika, and the Atlantic Council's Digital Forensic Research Lab, and Stanford's Internet Observatory as soon as we acquire legal approvals. We expect their reports on those networks to be released concurrently with our announcement or shortly after to help validate our assessment/action.

--

██████████
Policy Manager - Info Ops
██████████@fb.com

FACEBOOK

Produced to HJC

Exhibit 2

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 10/15/2020 6:29:46 AM
To: Nick Clegg [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbId": [REDACTED], "threadFbId": null}]

[REDACTED] (10/15/2020 06:29:46 PDT):
>@[REDACTED] just FYI, I'm hearing increased murmurs from the IC substantiating a hack of Burisma and their concern in recent weeks that the stolen files would be mixed together with other data stolen from the Bidens and manipulated data, and then dropped in an October surprise. The press is just starting to report about it this am. Likely more details like this to come.

Produced to HJC

Exhibit 3

Governance Meeting

Wednesday, October 14, 2020

3:27 PM

-Voter Reg:

1st Party in CA, OH, WV (3)

3rd Party in AZ, NM, SD, ID, WA (~FL) (5)

All customers were contacted months ago and offered our Azure HiPri review and support

All will receive Premiere support

MSRC and the Threat Hunting teams across the company have these tenant IDs and are watching carefully

SSIRP has been stood up - Bywater - includes these and others

-Ransomware

Heavy exposure, as in many cases state and local gov attacks would impact election systems

High risk, given the increase in ransomware cases combined with the poor patching practices of this market

Mitigation has been a big focus of ours for months, from extending AG, offering Azure for Elections, our membership in SCC, M365 Hi Pri, DART partnership - election security advisors - and of course our training series with Brennan and CISA which included a big emphasis on ransomware

Awesome work by DCU this week, greatly appreciated by DHS and the election community, as told to us today on the cross industry / gov call by DHS's elections lead

-Major Microsoft Outage

Would have considered lower likelihood, but recent events have bumped it higher

Strong mitigation - together with the Hi Pri team we achieved a code change advisory across all teams, no major updates will occur within 48 hours of the election w/ out cvp sign off

-Hack & Leak

FBI tipped us all off last week that this Burisma story was likely to emerge, and today's call indicated that

~25k machines in the US on Windows 7

Exhibit 4

>Should [REDACTED] send the "we are aware?" I don't think there's anything here beyond an FYI and a note that we're going to see what (if anything) FBI has to say.

[REDACTED] (10/14/2020 06:03:18 PDT):

>Nothing from FBI yet but LE outreach will let this group know if we get anything from them.

[REDACTED] (10/14/2020 06:04:13 PDT):

I also pinged [REDACTED] - feels like something worth specifically asking the FITF. Unlikely they will say much at this point, but worth the ask.

[REDACTED] (10/14/2020 06:06:31 PDT):

>We can send a short note, though as you say, not much to add at this stage.

[REDACTED] (10/14/2020 06:06:44 PDT):

>We can flag a short note. Though I am very skeptical of rags like the N.Y. post and Daily Mail m, as they a just rumor mills

[REDACTED] (10/14/2020 06:06:56 PDT):

>One step up from the Enquirer

[REDACTED] (10/14/2020 06:08:46 PDT):

>Completely agree. This is the sweet spot for landing something like this. Press so we won't be in a position to act directly, but not discerning enough to validate before publishing. There's nothing radical or surprising here at this point, but feels better for leadership to know we're tracking than get surprised by it on their morning feeds.

[REDACTED] (10/14/2020 06:09:43 PDT):

>We have an already scheduled meeting for later today with the FBI FITF and press them. [REDACTED] is also going to be on that call.

[REDACTED] (10/14/2020 06:11:01 PDT):

>VP group is aware

[REDACTED] (10/14/2020 06:11:32 PDT):

>Ok, we can stand down the we are aware email then i think.

[REDACTED] (10/14/2020 06:11:46 PDT):

>thanks for letting us know [REDACTED]

[REDACTED] (10/14/2020 07:11:56 PDT):

>Have we enqueued? Should we enqueue?

[REDACTED] (10/14/2020 07:12:40 PDT):

>Was just asking something similar on another thread -- I think we should, but I doubt the fact checkers will have much to fact check.

[REDACTED] (10/14/2020 07:12:52 PDT):

>It's pretty carefully calibrated to be anchored in unverifiable assertions/etc.

[REDACTED] (10/14/2020 07:14:01 PDT):

>Okay how do we make that happen. [REDACTED]

[REDACTED] (10/14/2020 07:15:24 PDT):

>I'll work with Misinfo Policy on-call now

[REDACTED] (10/14/2020 07:17:23 PDT):

[REDACTED] - just added you into a chat started w/ misinfo process. URL of the article is not enqueued, they are looking if the post has been.

[REDACTED] (10/14/2020 07:18:47 PDT):

>would be useful to be able to say to reporters that it has been enqueued if we are comfortable with that. There are a lot of indicators of falsity around it.

[REDACTED] (10/14/2020 07:20:18 PDT):

>if you're thinking about this in light of the CNN briefing in 40 mins, prob best to just say that the content is eligible to be fact checked

[REDACTED] (10/14/2020 07:22:41 PDT):

>Misinfo policy is reviewing now to determine if we should proactively enqueue. Predicted virality below:

>URL Next 24H Predicted VPs: Very high (8,196,540)

>Post Next 24H Predicted VPs: Normal (153,722)

[REDACTED] (10/14/2020 07:27:27 PDT):

>FWIW Trump has a video up of his ad attacking Biden on this, I imagine this will be the first of many. <https://www.facebook.com/DonaldTrump/videos/441385026841336/>

[REDACTED] (10/14/2020 07:52:28 PDT):

>Providing an update here

>1. Policy approved the URL for enqueueing + temp demotion and has been done.
 >2. There is another NY Post URL being reviewed by misinfo policy (published around the same time as the URL we enqueued). https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook
 >3. CrowdTangle surfaced a number of FBIDs making the same claims. Open question as to whether we should enqueue all instances.

[REDACTED] (10/14/2020 07:58:33 PDT):

>Ok, we just aligned in policy on the calls here.

>

>We are E&D the three URLs from the NY Post below:

>

><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/> seems to be the one Legum calls out.

>

>https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook

>

><https://nypost.com/2020/10/14/obama-conference-call-leaked-to-burisma-biden-emails/>

>

>We have signal of falsity on 2 claims: laptop and Ukrainian prosecutor was investigating Burisma, so other URLs or posts including these will also be E&D.

[REDACTED] (10/14/2020 09:11:47 PDT):

>update on this – there are a few different stories out there from NyPost at this point, and some do seem to include verifiable / fact checkable claims.

[REDACTED] (10/14/2020 09:11:55 PDT):

>Eg: they cite actual emails and comms w/out any data to validate them, and are careful not to dig into the most uncertain piece here – the source of the laptop and additional context around it.

[REDACTED] (10/14/2020 09:12:24 PDT):

>Glad we've got them enqueued. We're getting credit for moving quickly here, but getting a rating would be useful clarity here if it's going to come!

[REDACTED] (10/14/2020 09:27:41 PDT):

>The "we're moving quickly" apparent on Twitter of all places.

[REDACTED] (10/14/2020 10:01:40 PDT):

>The NY Post articles that were approved for enqueue and demotion have unintentionally stopped being demoted – [REDACTED] (CMOC oncall)/[REDACTED] are engaged with ops to determine a fix.

[REDACTED] (10/14/2020 10:02:00 PDT):

>Is there detail on this?

[REDACTED] (10/14/2020 10:02:36 PDT):

>If we need help from misinfo engg please add [REDACTED] or [REDACTED] to the working chat thread

[REDACTED] (10/14/2020 10:03:47 PDT):

>The URLs are caught in a tool called [REDACTED], a backstop that misinfo product uses because our URL classifiers used to have low precision

[REDACTED] (10/14/2020 10:04:50 PDT):

[REDACTED] and [REDACTED] from misinfo are engaged and investigating. Please add them to working chat thread

[REDACTED] (10/14/2020 10:05:16 PDT):

>Great! They are both on the thread

[REDACTED] (10/14/2020 10:17:21 PDT):

>Demotions are now applied (via Demote on Demand). Current status:

>

>For extreme clarity:

>

>NY Post 1 (3799378103462160): Apply demotion (already enqueued)

>

>NY Post 2 (4556511704421082): Apply demotion (already enqueued)

>

>NY Post 3 (3630832923627559): No action (not enqueued)

>

>Twitchy (3339412429503150): No action (already enqueued)

>

>Daily Mail (3326731784030479): No action (not enqueued)

[REDACTED] (10/14/2020 10:19:19 PDT):

>A

[REDACTED] (10/14/2020 10:40:31 PDT):

>Update from the FBI FITF call: The FBI has no information indicating foreign sponsorship, direction, or coordination of the hunter laptop issue.

[REDACTED] (10/14/2020 10:44:00 PDT):

>fyi: Twitter is "moving toward" treating this information as presumptively hacked material given the suspicious elements around the laptop.

[REDACTED] (10/14/2020 10:44:30 PDT):

>Where are you hearing that and what actions would they take?

[REDACTED] (10/14/2020 10:44:48 PDT):

>Working on getting more context on what they'd do.

[REDACTED] (10/14/2020 10:45:13 PDT):

>That would be very helpful

[REDACTED] (10/14/2020 10:47:15 PDT):

>Coming from my ongoing convos w/my counterparts at Twitter and Google.

[REDACTED] (10/14/2020 10:47:28 PDT):

>Twitter is taking down the NYPOST story.

[REDACTED] (10/14/2020 10:47:42 PDT):

>b/c it includes screenshots and images obtained from the harddrive.

[REDACTED] (10/14/2020 10:47:55 PDT):

>They are acting only based on those screenshots, so coverage/debate is ok.

[REDACTED] (10/14/2020 10:48:01 PDT):

>But the stories include original source material.

[REDACTED] (10/14/2020 10:50:55 PDT):

[REDACTED] flagging for you. [REDACTED] which one?

[REDACTED] (10/14/2020 10:51:38 PDT):

>At minimum this one: <https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 10:51:43 PDT):

>Likely any with original source material

[REDACTED] (10/14/2020 10:56:07 PDT):

>What do we expect timing to be?

[REDACTED] (10/14/2020 10:56:20 PDT):

>In case it's useful as we work through the thread for referencing articles, here is the list of articles based on fbid's from [REDACTED]'s message above, mapped to UserURL. [REDACTED] is referencing article 3:

[REDACTED] (10/14/2020 10:56:22 PDT):

>=====Current Articles=====

>1. NY Post 1 (3799378103462160): Apply demotion (already enqueued)

>UserURL: <https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/>

>

>2. NY Post 2 (4556511704421082): Apply demotion (already enqueued)

>UserURL: <https://nypost.com/2020/10/14/obama-conference-call-leaked-to-burisma-biden-emails>

>

>3. NY Post 3 (3630832923627559): No action (not enqueued)

>UserURL: <https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad>

>

>4. Twitchy (3339412429503150): No action (already enqueued)

>UserURL: <https://twitchy.com/gregp-3534/2020/10/14/smoking-gun-ny-post-publishes-damning-emails-on-ukraine-purportedly-recovered-from-hunter-bidens-laptop>

>

>5. Daily Mail (3326731784030479): No action (not enqueued)

>UserURL: <https://www.dailymail.co.uk/news/article-8838939/Joe-Biden-met-son-Hunters-Ukrainian-energy-contacts.html>

[REDACTED] (10/14/2020 11:09:13 PDT):

>Unrelated BI PO in the IPOC

>Case Number: C#213829

>Case Title: Page Settings Unavailable for Political Agencies

>Summary: Per GPA, a number of partners (including several political ad agencies) are reporting that their Page Settings are missing. The high priority here stems from the fact that partners need these settings to submit/finalize SIEP disclaimers ahead of the restriction period/election.

>Next steps: As an initial step, PSO has been looped in to investigate

[REDACTED] (10/14/2020 11:15:10 PDT):
>Momentarily. Link blocking about to happen, and URLs happening after that.

[REDACTED] (10/14/2020 11:17:44 PDT):
>They'll be removing stories that directly distribute the materials, but not stories that merely comment on them.

[REDACTED] (10/14/2020 11:52:41 PDT):
>are they saying anything publicly on this?

[REDACTED] (10/14/2020 12:43:01 PDT):
>apparently Twitter has locked the NY Post twitter account?
<https://twitter.com/noahmanskar/status/1316459416414302208> - [REDACTED] did you hear anything from them on this?

[REDACTED] (10/14/2020 12:43:40 PDT):
>I think this is standard way Twitter works: if a tweet is violating, you are "locked" until you go in and delete in (as a kind of acknowledgement).

[REDACTED] (10/14/2020 12:43:44 PDT):
>their consistent policy when accounts post violating behavior is to lock the acct

[REDACTED] (10/14/2020 12:43:49 PDT):
>ah jinx.

[REDACTED] (10/14/2020 12:58:07 PDT):
>yep.

[REDACTED] (10/14/2020 13:42:44 PDT):
>Flagging a misinfo PO in the IPOC
>Case Number: T77709287
>Case Title: MISINFO ESC: Urgency: Urgent and Needs Immediate Attention (America First Action Currently in RO)
>Summary: America First Action is currently in misinfo RO
>Next Steps: As a first step we're looking at existing strikes and ensuring they've been accrued/counted correctly. Misinfo Policy has been looped in.

[REDACTED] (10/14/2020 14:15:31 PDT):
>FYI for the misinfo pod: <https://twitter.com/LilaGraceRose/status/1316484968583892993?s=20>

[REDACTED] (10/14/2020 14:15:46 PDT):
>Sorry! Wrong chat

[REDACTED] (10/14/2020 15:29:03 PDT):
><https://techcrunch.com/2020/10/14/suspect-provenance-of-hunter-biden-data-cache-prompts-skepticism-and-social-media-bans/>

[REDACTED] (10/14/2020 15:29:19 PDT):
>Expect more cautious-to-debunking stories like this to come.

[REDACTED] (10/14/2020 16:04:27 PDT):
>Update on the First Action PO in the IPOC, which we can consider mostly resolved
>Case Number: T77709287
>Case Title: MISINFO ESC: Urgency: Urgent and Needs Immediate Attention (America First Action Currently in RO)
>Summary: In line with our existing de-duplication policy, we lifted six of seven misinfo strikes issued yesterday (all around the same claim), which left the page with only one strike and out of RO. For the remaining strike, Misinfo Policy's view is that "missing context" would have been a more appropriate rating under our established guidelines.
>Next Steps: 3PFC partnership will raise the rating with the fact checker at a pre-scheduled meeting tomorrow to see if they want to revisit. If the rating is not adjusted by October 16, we will lift the strike.

[REDACTED] (10/14/2020 16:54:14 PDT):
>Twitter dropped their policy explanation for enforcement:

[REDACTED] (10/14/2020 16:54:16 PDT):
><https://twitter.com/TwitterSafety/status/1316525303930458115?s=20>

[REDACTED] (10/14/2020 17:03:31 PDT):
>Quickly flagging a couple of hi-pri POs that have been resolved:

[REDACTED] (10/14/2020 17:04:50 PDT):
>Resolved PO in the IPOC
>Case Number: C#212542
>Case Title: Flagged IG Accounts by Trump Teams

>Summary: Trump campaign flagged four IG accounts they say are getting reduced visibility (including the official Trump Store account)

>Resolution: IG accounts flagged by the Trump campaign. We confirmed that the reduced visibility on two out of the four accounts was due to the accounts being in misinfo RO. For the account of Kaya Jones (a member of the Trump Campaign Advisory Board), Misinfo Policy established that strikes should be de-duped as the content was part of a single IG carousel. This left the account with only two strikes and out of RO. The conservative meme account was found to correctly be in RO. For the remaining two accounts (Isabel Brown - a Turning Point USA contributor - and the Trump Store), Content Quality Platform confirmed they are recommendable and are not being demoted. We did find that SI automation was reducing the visibility of specific comments by Isabel Brown's account and, since there was no malicious behavior, Policy approved adding a shield to prevent this automation from impacting the account.

[REDACTED] (10/14/2020 17:05:47 PDT):

>Resolved PO in the IPOC

>Case Number: C#211584

>Case Title: Reporter inquiry on Calif fake ballot box posts

>Summary: Confirm if content posted by the CA GOP page is violating per determination made in case 210165 that posts about unofficial ballot boxes in California may violate.

>Resolution: The initial violating posts on FB and IG were removed by the partner earlier this week after we conducted outreach. A second post about the unofficial ballot box issue was not found to be violating because it does not explicitly reference the ballot boxes.

[REDACTED] (10/14/2020 17:17:30 PDT):

><https://twitter.com/breitbartnews/status/1316529688370728960?s=21>

[REDACTED] (10/14/2020 20:32:47 PDT):

>We have closed Day 3 from a NA perspective and have handed over to our APAC colleagues! [REDACTED] is now the Crew Lead until he hands over to [REDACTED] in EMEA. Below are our open high-pri escalations that we're tracking:

>*Open High-Pri Escalations*

>*1. Case Number: C#214306*

>Case Title: [US2020] Avaaz: New Investigation Swing State - Voter Fraud Misinformation

>Summary: Avaaz sent a report on Facebook content pertaining to voter fraud and suppression in four swing states: Michigan, Pennsylvania, Wisconsin, and Florida.

>Next Steps: CO-PREsc is reviewing the content in the Avaaz report

>*2. Task Number: T77656938*

>Task Title: Viral Copy/Paste: Ballots Not Counted

>Summary: We have received several escalations from Secretary of State partners regarding posts circulating on our platforms with a warning that if a ballot has any sort of mark on it from a poll worker, it will not be counted. While we know this information to be false in some states, we do not have confirmation that it's false in all 50 states, which complicates enforcement.

>Next Steps: To date we've deleted a few posts specifying a location (where state officials have confirmed the claim to be false) and added FAVIT to the remaining content that was escalated. We've now also set up a CIRD pipeline to track similar content and are aligning with policy on an enforcement plan.

>*3. Task number: T77688004*

>Task Title: MISINFO ESC: Urgency: High-Priority (Under 24-hour Resolution) (Washington Examiner RO)

>Summary: Washington Examiner is in Misinfo Repeat Offender status

>Next steps: Policy and Ops reviewing strikes and confirming whether enforcement is in line with our policies and guidelines

>You can find more details related to the above and other escalations in the stand-up log:
<https://fb.quip.com/ZSKTALOVN5G7>

[REDACTED] (10/14/2020 20:43:21 PDT):

><https://www.facebook.com/DonaldTrump/videos/713788112569060/?vh=e&extid=0&d=n>

[REDACTED] (10/14/2020 20:43:33 PDT):

>Should keep eye out for this in ads

[REDACTED] (10/14/2020 20:44:09 PDT):

>I see the email in there. Does that mean we enforce against this ad?

[REDACTED] (10/14/2020 20:45:01 PDT):

>I'll flag to our Ads escalation team to help track.

[REDACTED] (10/14/2020 20:46:38 PDT):

>Trying to confirm

[REDACTED] (10/14/2020 20:46:41 PDT):

>This is not an ad

[REDACTED] (10/14/2020 20:46:44 PDT):

>This is organic

[REDACTED] (10/14/2020 20:46:51 PDT):
>Ah -- got it.

[REDACTED] (10/14/2020 20:47:01 PDT):
>Sorry -- misunderstood based on your flag.

[REDACTED] (10/14/2020 20:47:14 PDT):
>I am confirming that we should reject if it appears in an ad

[REDACTED] (10/14/2020 20:56:50 PDT):
>Confirmed - this video is allowed as organic content but would not be allowed in an ad

[REDACTED] (10/14/2020 21:03:16 PDT):
>[REDACTED] we had previously been given guidance not to proactively sweep for potentially violating ads. Do you want Ops to start proactive sweeps in light of this new Trump video or is this still only on escalation?

[REDACTED] (10/14/2020 21:03:43 PDT):
>On escalation

[REDACTED] (10/14/2020 21:03:47 PDT):
shared: sticker.png

[REDACTED] (10/14/2020 21:03:52 PDT):
>Thanks!

[REDACTED] (10/14/2020 21:03:54 PDT):
shared: sticker.png

[REDACTED] (10/14/2020 21:04:22 PDT):
>(Or rather, I didn't intend to vary any previous guidance)

[REDACTED] (10/14/2020 21:04:55 PDT):
>Got it. Just wanted to make sure. Thanks!

[REDACTED] (10/14/2020 21:32:55 PDT):
>Where did that instruction come from?

[REDACTED] (10/14/2020 21:33:15 PDT):
>Guidance that we should not proactively sweep for ads

[REDACTED] (10/14/2020 21:38:03 PDT):
>It was part of the guidance following this afternoons leadership meeting

[REDACTED] (10/14/2020 21:47:17 PDT):
>From [REDACTED]? I don't recall discussing proactive versus reactive but may be missing something.

[REDACTED] (10/14/2020 21:50:24 PDT):
>FWIW - we have a group in SNG looking into what we can do from an enforcement perspective if we choose a different approach.

[REDACTED] (10/14/2020 21:52:06 PDT):
>Yes, we got our read out from [REDACTED] - but I'm not sure where the issue was discussed.

[REDACTED] (10/14/2020 22:55:12 PDT):
>Circling back here on the DJT video above. We are going to seed images of the leaked documents, including the ones from the video, so we can catch & enqueue for review at scale any ads that may include these images. We won't be proactively searching or hunting for the ads but are planing to make sure our scaled systems have some mechanism to catch these at scale.

>
>Recall won't be perfect, and it'll take some time to set up, but it'll help us catch some of these things. Let us know if there are any objections to this approach. We have the team scoping what'll take to seed and enqueue any potentially violating ads.

Exhibit 5

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]>
 To: [REDACTED]
 Sent: 10/14/2020 1:46:46 PM
 Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]
 Attachments: sticker.png; sticker1.png

[REDACTED] (10/14/2020 05:42:09 PDT):

> [REDACTED]: can you talk to your FBI counterparts and see what they say about this?

[REDACTED] (10/14/2020 05:42:11 PDT):

><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 05:42:26 PDT):

>It looks like exactly the hack/leak scenario we'd expected.

[REDACTED] (10/14/2020 06:11:49 PDT):

> [REDACTED] has reached out to FBI in Delaware. Let me make sure that my reaching out will not cause confusion or delay

[REDACTED] (10/14/2020 10:58:42 PDT):

>Just off from a call with FBI. They were unaware that our industry/usg call is on for today.

[REDACTED] (10/14/2020 10:59:29 PDT):

>I told them that the meetings have been set for each Wednesday at the same time. They will have a light presence on the call today, none of the regulars, just someone who was on the last call and is available now

[REDACTED] (10/14/2020 11:00:26 PDT):

>Yikes! Did DHS not share the invite? [REDACTED] is there value in [REDACTED] sharing the invite with FBI and ODNI in addition to DHS in case DHS accidentally forgot to forward or share?

[REDACTED] (10/14/2020 11:02:49 PDT):

> [REDACTED] You're back in DC.

[REDACTED] (10/14/2020 11:03:19 PDT):

> [REDACTED] are you on yet? Know there is another fire burning. . [REDACTED] is just doing roll call now.

[REDACTED] (10/14/2020 11:07:30 PDT):

> [REDACTED] do we have anything we can or would share on the hack/leak calculus for FB like the deamplification point?

[REDACTED] (10/14/2020 11:08:40 PDT):

>We asked FBI about this in our meeting just prior to this. They have this as a criminal case. Could not say much more.

[REDACTED] (10/14/2020 11:09:06 PDT):

>Thank you for that -- also, separately, why has Google been so soft on QAnon?

[REDACTED] (10/14/2020 11:09:41 PDT):

>Also, FBI has no indication that there is any foreign amplification of the content.

[REDACTED] (10/14/2020 11:10:39 PDT):

>Would we want to ask them again that if they see something that they should share something, like we've said before?

[REDACTED] (10/14/2020 11:12:05 PDT):

>Agenda mentioned the civil unrest concerns?

[REDACTED] (10/14/2020 11:12:24 PDT):

> [REDACTED]

[REDACTED] (10/14/2020 11:12:36 PDT):
>thank you!

[REDACTED] (10/14/2020 11:21:05 PDT):
> [REDACTED] you May want to reinforce we will continue to do these weekly synchs every Wednesday at 2:00 pm EST. We will use the same dial in every week. Also, we have them scheduled until December 16th as needed.

[REDACTED] (10/14/2020 11:21:12 PDT):
shared: sticker.png

[REDACTED] (10/14/2020 11:22:01 PDT):
>From [REDACTED]
> URLs which will be denylisted:
><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/> (directly distributes materials, hosted by NYP)
><https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/>
><https://www.scribd.com/document/480001587/Email-from-Robert-Biden-to-Devon-Archer>
><https://www.scribd.com/document/480001185/Email-from-Vadim-Pozharskyi-to-Devon-Archer-and-Hunter-Biden>
>
>URLs which will not be denylisted:
><https://www.foxnews.com/politics/hunter-biden-emails-senate-homeland-security-committee-investigating-hard-drive-laptop> (commentary, not direct distribution)
><https://nypost.com/2020/10/14/senate-committee-investigating-hunter-biden-hard-drive-email/> (commentary, not direct distribution)

[REDACTED] (10/14/2020 11:25:24 PDT):
>Do we ask about any poll-related civil unrest?

[REDACTED] (10/14/2020 11:25:45 PDT):
>I think that's our last item, right?

[REDACTED] (10/14/2020 11:28:02 PDT):
>All set, I think?

[REDACTED] (10/14/2020 11:29:42 PDT):
shared: sticker.png

[REDACTED] (10/14/2020 12:35:40 PDT):
> [REDACTED] and [REDACTED] just as an FYI, at my 1:1 with [REDACTED] after today's USG/Industry meeting, we talked about how it will likely not be needed to have a formal "agenda" before these weekly synchs -- we can just have it be "around the horn" on top of mind issues, and we can ping the internal FB chat thread the day before to see if there are issues folks want to raise. Do you have anything you'd like to add to this updated approach? Thank you again for the engagement with DHS and FBI today.

[REDACTED] (10/14/2020 13:02:08 PDT):
>That sounds reasonable, but if that does not work well next week, we may have to rethink.

[REDACTED] (10/14/2020 13:21:18 PDT):
>Good call -- we can play by ear and see how it rolls.

[REDACTED] (10/14/2020 13:46:46 PDT):
>Agree.

Exhibit 6

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=90EE91676BAF4A1B858AB16C9585BD01-[REDACTED]>
To: [REDACTED]
Sent: 10/14/2020 8:02:54 AM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]

[REDACTED] (10/14/2020 06:06:09 PDT):
> [REDACTED] Can we check with FBI Delaware if they have anything in this:
<https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 06:06:40 PDT):
>Article claims that FBI has had the HDD since December.

[REDACTED] (10/14/2020 06:07:03 PDT):
>This has been escalated in the various election channels

[REDACTED] (10/14/2020 06:07:46 PDT):
>Cyber law [REDACTED] might also know about this and be in contact with FBI on it.

[REDACTED] (10/14/2020 06:07:53 PDT):
>I'll call them this morning. Is the questions just about any relation to FB or IG in terms of any stolen content?

[REDACTED] (10/14/2020 06:08:19 PDT):
>Yep, I think they is the proper scope.

[REDACTED] (10/14/2020 06:08:25 PDT):
>*that

[REDACTED] (10/14/2020 06:08:32 PDT):
>OK

[REDACTED] (10/14/2020 06:09:45 PDT):
> [REDACTED] says he asked [REDACTED] to ping FITF about this as well.

[REDACTED] (10/14/2020 06:14:26 PDT):
> [REDACTED] is not in touch with the FBI on this. I'll connect with Maryland and [REDACTED] will raise at the FITF meeting today.

[REDACTED] (10/14/2020 08:02:54 PDT):
>Thanks all for your work today in the meeting, amazing job. We've got so much going on and we truly packed ten pounds of shit into a 5 pound bag in that meeting. Thanks again so much for your prep and delivery.

Exhibit 7

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=28E865DE754F42D3ACBCF1C8052D0B8F>
To: [REDACTED]; Nick Clegg; [REDACTED]
 [REDACTED] Joel Kaplan;
Sent: 10/14/2020 9:56:34 PM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]
Attachments: 121161847_1316086545401657_7329363007398542195_n.png;
 121440254_1251840195175940_3016984524154928067_n.jpg;
 121523296_4486187921454030_1191778544254324768_n.png;
 121570689_337558230646825_1230117776855863053_n.png; sticker.png; sticker1.png

[REDACTED] (10/14/2020 06:03:24 PDT):
 > Morning, the NY Post published an article on what are allegedly leaked Hunter Biden-Burisma emails. SR ([REDACTED] and team) will send FYI.
 >
 ><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 06:09:51 PDT):
 > Exact content expected for hack and leak, but sounds like so far, not much for us to do:
 >
 >1. No evidence of foreign interference operation
 >2. Coming directly from press
 >
 > Sounds like next steps are to see if FBI contacts have any context for us, and to wait.

[REDACTED] (10/14/2020 06:10:33 PDT):
 > Right on schedule.

[REDACTED] (10/14/2020 07:01:16 PDT):
 > Has it been referred to 3PFC?

Nick Clegg (10/14/2020 07:11:08 PDT):
 > Looks fairly dodgy: <https://mobile.twitter.com/JuddLegum/status/1316376280103825409>

[REDACTED] (10/14/2020 07:15:15 PDT):
 > Has not been referred yet, asked the team to refer now (but [REDACTED]'s assessment FWIW is that this is couched in a way that would be very difficult for 3PFC to rate).

[REDACTED] (10/14/2020 07:40:10 PDT):
 > We're enqueueing the content with demotion and doing outreach to 3PFCs. No updated info from FBI, no outreach from the Biden campaign. Trump is running ads on the claim.

Joel D. Kaplan (10/14/2020 07:42:35 PDT):
 > Do we always apply a demotion when we manually enqueue?

[REDACTED] (10/14/2020 07:43:02 PDT):
 > No. We have standards for doing so and this met the test.

Joel D. Kaplan (10/14/2020 07:49:47 PDT):
 > Can you remind what the standards are?

[REDACTED] (10/14/2020 07:53:23 PDT):
 > <https://docs.google.com/document/d/1V07rKnzAsQK6TRtsot3CnbIeXYNPDdYfuU9XvhIMaTk/edit?usp=sharing>

[REDACTED] (10/14/2020 07:54:15 PDT):
 > The relevant ones here are: (1) A civic debate regarding a matter of country-wide importance or relevant to a given election; OR

[REDACTED] (10/14/2020 07:54:31 PDT):
 > Falsity: Other press reporting, including but not limited to from publishers on the NPI

[REDACTED] (10/14/2020 07:55:29 PDT):

>Demotion: Press article or direct report debunking the key claim from established press outlets, if both Content Policy and the regional team (Public Policy, News Partnerships) deem the report credible

>Social media posts from journalist expressing disbelief regarding - or debunking - the key claim, if both Content Policy and the regional team (Public Policy, News Partnerships) deem the journalist post credible (Ops may but is not expected to search for this content)

[REDACTED] (10/14/2020 07:55:46 PDT):

>Outreach: Content is about a national office holder or candidate for national office, as defined by politicians on our whitelist; OR

Joel D. Kaplan (10/14/2020 07:56:42 PDT):

>Where are we seeing the suggestions of falsity?

[REDACTED] (10/14/2020 07:57:07 PDT):

>We started with the tweet Nick shared above.

[REDACTED] (10/14/2020 07:57:45 PDT):

>We also have tweets from Maggie Habermann (NYT) and a disinformation expert [REDACTED] is familiar with.

[REDACTED] (10/14/2020 07:59:08 PDT):

>This doesn't seem like it meets the standard of "press article or direct report"

[REDACTED] (10/14/2020 07:59:44 PDT):

>The tweets are "Social media posts from journalist expressing disbelief regarding - or debunking - the key claim"

[REDACTED] (10/14/2020 08:01:39 PDT):

shared: 121440254_1251840195175940_3016984524154928067_n.jpg

[REDACTED] (10/14/2020 08:01:56 PDT):

>Judd Legum is an activist (former/current political opposition researcher) and has never worked for a reputable media outlet.

[REDACTED] (10/14/2020 08:02:31 PDT):

>Right, so this seems to turn on whether the Maggie Haberman tweet above meets our standard

[REDACTED] (10/14/2020 08:03:49 PDT):

>I guess the concern is that it seems like there are a lot of things that this standard would potentially apply to (e.g., NYT reporting on taxes)?

[REDACTED] (10/14/2020 08:04:15 PDT):

>How strong is the demotion?

[REDACTED] (10/14/2020 08:04:43 PDT):

[REDACTED] (10/14/2020 08:05:10 PDT):

>Yes, we make a lot of judgment calls. This is one of them.

[REDACTED] (10/14/2020 08:05:10 PDT):

>I believe 50%

[REDACTED] (10/14/2020 08:06:26 PDT):

>It seems like this could blow up, that we are demoting a mainstream press article

[REDACTED] (10/14/2020 08:06:58 PDT):

>However sketchy

[REDACTED] (10/14/2020 08:07:36 PDT):

>Okay. I will route all decision through this group going forward then.

[REDACTED] (10/14/2020 08:07:50 PDT):

>Do you want us to undo the demotion and enqueueing and stop calling fact checkers?

[REDACTED] (10/14/2020 08:08:09 PDT):

>I will advise however, that crisis management by committee is very bad practice.

[REDACTED] (10/14/2020 08:08:23 PDT):

>It seems like we shouldn't call them

[REDACTED] (10/14/2020 08:08:32 PDT):

>They should be well aware

[REDACTED] (10/14/2020 08:12:46 PDT):

>Okay, done.

[REDACTED] (10/14/2020 08:12:53 PDT):

>If we find ourselves talking about this process on this particular piece of content (with a lot more to come, if history is any indicator), having a clear explanation of what we did and why is going to be key - obviously. Were we fair and consistent with other moments during the campaign?

[REDACTED] (10/14/2020 08:12:59 PDT):

>Direction to do outreach has been withdrawn.

[REDACTED] (10/14/2020 08:14:36 PDT):

>Yes, we were following the guidelines and guardrails that we wrote for ourselves over the months (year?) since the Pelosi video. We've worked incredibly hard to be ready for this.

[REDACTED] (10/14/2020 08:51:26 PDT):

>We're seeing multiple other stories making similar claims (alleging email evidence from a laptop and the prosecutor being fired for investigating Burisma). Do you want to enqueue, demote, and badge the stories? Protocols say to do so.

[REDACTED] (10/14/2020 08:57:27 PDT):

>What does badge mean?

[REDACTED] (10/14/2020 08:57:30 PDT):

>3PFCs have asked via a slack chat that we maintain with them if we want them to rate this content. Please let me know how partnerships should reply. I advise we should tell them it's enqueued and we think they should rate it.

[REDACTED] (10/14/2020 08:57:59 PDT):

>We put "badges" on similar content so that 3PFCs can find all the related content in one place instead of having to hunt through the queues for it.

[REDACTED] (10/14/2020 09:01:28 PDT):

>If it's in the queue, it's up to them, right?

[REDACTED] (10/14/2020 09:01:59 PDT):

>Yes

[REDACTED] (10/14/2020 09:02:10 PDT):

>This seems like an odd case for actively encouraging them, given that our own assessment is that they probably don't have the right information/capability

[REDACTED] (10/14/2020 09:02:14 PDT):

>Per [REDACTED]

[REDACTED] (10/14/2020 09:03:01 PDT):

>So my instinct for what it's worth is to leave it to them - but interested in others' views

[REDACTED] (10/14/2020 09:03:24 PDT):

>And I would continue to enqueue all of this content and badging seems fine to assist with collating

[REDACTED] (10/14/2020 09:04:13 PDT):

>It seems like a real edge case to me on demoting on the basis of the press coverage that I've seen, which expresses skepticism but not necessarily outright disbelief (though it's a judgment call, I recognize)

[REDACTED] (10/14/2020 09:12:57 PDT):
><https://twitter.com/TrumpWarRoom/status/1316398578995257344>

[REDACTED] (10/14/2020 09:13:22 PDT):
><https://twitter.com/DonaldJTrumpJr/status/1316403732272295938>

[REDACTED] (10/14/2020 09:13:45 PDT):
>wait - what?

[REDACTED] (10/14/2020 09:14:11 PDT):
>We are clarifying now - with the exception of the lede, this is all correct.

[REDACTED] (10/14/2020 09:14:21 PDT):
[REDACTED] and [REDACTED] are talking.

[REDACTED] (10/14/2020 09:14:37 PDT):
>Lede indicates animus -- which we could have lived without.

[REDACTED] (10/14/2020 09:19:56 PDT):
>We are working to treat this content-event like any other in the campaign. [REDACTED] will clarify - and I think we should proceed as we are now by staying middle of the road in how we're interpreting and applying the rules.

[REDACTED] (10/14/2020 09:20:56 PDT):
>Here is the updated tweet we are recommending [REDACTED] reply to his original tweet. WSJ, NYTimes and CNN tweeting that this is SOP

[REDACTED] (10/14/2020 09:20:58 PDT):
>This is part of our standard process to reduce the spread of misinformation. As we laid out in this newsroom post, "if we have signals that a piece of content is false, we temporarily reduce its distribution pending review by a third-party fact-checker." [link]

[REDACTED] (10/14/2020 09:22:13 PDT):
><https://twitter.com/sheeraf/status/1316399312843141123>

[REDACTED] (10/14/2020 09:25:11 PDT):
shared: 121523296_4486187921454030_1191778544254324768_n.png

[REDACTED] (10/14/2020 09:26:12 PDT):
>Everyone please let us know if we should hold on our update to [REDACTED]'s tweet. We'd like to move swiftly. In the next 10 minutes.

[REDACTED] (10/14/2020 09:26:32 PDT):
>This one:
>
>This is part of our standard process to reduce the spread of misinformation. As we laid out in this newsroom post, "if we have signals that a piece of content is false, we temporarily reduce its distribution pending review by a third-party fact-checker." [link]

Joel D. Kaplan (10/14/2020 09:31:20 PDT):
>I don't think we should double down on "signals that it's false."

[REDACTED] (10/14/2020 09:32:12 PDT):
>This is the language from the policy as it was interpreted.

[REDACTED] (10/14/2020 09:32:30 PDT):
>We should be clinical and defend the policy.

Joel D. Kaplan (10/14/2020 09:32:49 PDT):
>I don't think we should say it.

Joel D. Kaplan (10/14/2020 09:33:37 PDT):
>In this context, it just sounds like we're repeating we think it's false.

[REDACTED] (10/14/2020 09:44:20 PDT):
>We are repeating that there were signals of falsity that led to the content being referred to fact checkers. I believe this is the letter of our policy that we are repeating. Do you

have another suggestion?

Final Report 1028

[REDACTED] (10/14/2020 09:45:39 PDT):

>Two open questions from above - (1) should we enqueue, demote, badge similar content? ([REDACTED] and I both recommend yes). (2) should we respond to 3PFCs' request for guidance on whether we want them to review/rate this content? [REDACTED] recommends no; I recommend yes). [REDACTED] asked for additional views, so I'm holding on acting.

[REDACTED] (10/14/2020 09:45:43 PDT):

>This is standard operating procedure. Speed is of the essence to make that case more forcefully. Can we proceed?

[REDACTED] (10/14/2020 09:46:03 PDT):

>This is standard operating procedure. Speed is of the essence to make that case more forcefully. Can we proceed?

[REDACTED] (10/14/2020 09:49:17 PDT):

>Should we just use the first sentence and link to post without quoting it?

[REDACTED] (10/14/2020 09:51:16 PDT):

>Not sure I entirely agree on doubling down on demotion

[REDACTED] (10/14/2020 09:52:06 PDT):

>2 things:

[REDACTED] (10/14/2020 09:52:10 PDT):

>[REDACTED] is going to propose some language here. I think we have a reasonable path forward.

[REDACTED] (10/14/2020 09:52:40 PDT):

>1.) Talked with [REDACTED] and we are aligned with [REDACTED] not to prompt Fact Checkers beyond our standard operating procedure

[REDACTED] (10/14/2020 09:52:50 PDT):

>2.) Updated tweet here:

[REDACTED] (10/14/2020 09:53:00 PDT):

>Though I recognize that inconsistency creates new issues

[REDACTED] (10/14/2020 09:54:08 PDT):

>Okay, I'm assuming this is the decision unless someone else weighs in in the next 3 minutes.

Joel D. Kaplan (10/14/2020 09:54:59 PDT):

>Sorry-what's the decision?

[REDACTED] (10/14/2020 09:55:56 PDT):

>In response to 3PFCs request for guidance on whether to rate or not, to tell them to do whatever they think is appropriate.

Joel D. Kaplan (10/14/2020 09:56:38 PDT):

>Okay, I also think we should hold on enqueueing, badging, demoting additional content.

Joel D. Kaplan (10/14/2020 09:56:54 PDT):

>And see what factcheckers do here

[REDACTED] (10/14/2020 09:56:58 PDT):

>Great, will also consider that a decision unless someone else objects in next three minutes.

[REDACTED] (10/14/2020 09:57:13 PDT):

>@Joel [REDACTED] Tweet here. Please approve: "This is part of our standard process to reduce the spread of misinformation. We temporarily reduce distribution pending fact-checker review. Previous newsroom post [HERE]"

Joel D. Kaplan (10/14/2020 09:57:22 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 09:57:40 PDT):

Final Report 1029

shared: sticker.png

[REDACTED] (10/14/2020 09:58:52 PDT):

>Talked with [REDACTED] -- we are good to go on Tweet

[REDACTED] (10/14/2020 09:58:55 PDT):

>Moving it out

[REDACTED] (10/14/2020 10:00:11 PDT):

>Per [REDACTED] there is a product issue and the links aren't actually being demoted.

[REDACTED] (10/14/2020 10:00:21 PDT):

>@ [REDACTED] are you tracking on the demotion issue?

[REDACTED] (10/14/2020 10:01:22 PDT):

>Was not aware, checking

[REDACTED] (10/14/2020 10:01:35 PDT):

>Sounds like product is implementing a bypass solution now on the two articles that were enqueued and assigned demotions.

[REDACTED] (10/14/2020 11:19:36 PDT):

>One list of the public falsity claims: <https://fb.quip.com/jakGakBJbFBq>

[REDACTED] (10/14/2020 12:45:15 PDT):

>For awareness, additional context from [REDACTED] from the FBI meeting (somewhat sensitive so wasn't shared on the broader IPOC threads):

>Officially FBI said "The FBI has no information indicating foreign sponsorship, direction, or coordination of the hunter laptop issue" and [REDACTED] shared that with the US 2020 Esc thread...on the side in the same call however, they did confirm that FBI has the laptop and it's being review "as part of a criminal matter" but didn't give us details.

[REDACTED] (10/14/2020 12:52:51 PDT):

>But that would assume the laptop repair guy might be violating the law, yes?

[REDACTED] (10/14/2020 12:52:56 PDT):

>Rather than the IRA.

[REDACTED] (10/14/2020 13:04:38 PDT):

>Here is what the Biden campaign put out in terms of a fact disputed (but I think largely irrelevant to where we are headed):

>"The New York Post never asked the Biden campaign about the critical elements of this story. They certainly never raised that Rudy Giuliani - whose discredited conspiracy theories and alliance with figures connected to Russian intelligence have been widely reported - claimed to have such materials. Moreover, we have reviewed Joe Biden's official schedules from the time and no meeting, as alleged by the New York Post, ever took place."

[REDACTED] (10/14/2020 13:13:48 PDT):

>NYPost Locked out of Twitter: <https://twitter.com/noahmanskar/status/1316459416414302208?s=21>

[REDACTED] (10/14/2020 13:13:48 PDT):

>Twitter statement: "In line with our Hacked Materials Policy, as well as our approach to blocking URLs, we are taking action to block any links to or images of the material in question on Twitter."

Nick Clegg (10/14/2020 13:23:58 PDT):

>How about:

>"This material is allowed for public awareness, even though it may contain material from a hacked source. Learn more x,y,z"

Nick Clegg (10/14/2020 13:28:31 PDT):

>Or: "This material may contain material from a hacked source. It is made available here because it is newsworthy content. Learn more x,y,z."

[REDACTED] (10/14/2020 13:35:07 PDT):

><https://fb.workplace.com/KayleighMcEnany7/photos/a.675511112508409/352117792117563/?type=3>

Nick Clegg (10/14/2020 13:43:18 PDT):

> [REDACTED] on point 1 for comms I'd make it active not passive: "We are applying a label to inform our users that this content may contain material from a hacked source, but is still available for public awareness [under our newsworthiness policy]." Or somesuch. Need to make the label look as muscular as poss.

[REDACTED] (10/14/2020 14:14:48 PDT):

>For our follow up at 3:30:

>

>Some in DC expect the next rounds of this are going to be images of Hunter B smoking crack - followed by video with the commercial sex workers.

>

>I know I was the sole vote for total removal on the hack policy. (And I appreciate that the Hunter B images would still come down with the label being suggested.) But, if we are going to get to taking things down full-stop soon (based on this rumor), I'm highlighting my absolutist position, again. While I'm a moralizing sort - the reason I like it best of all is that you can explain it in one sentence. FWIW...

[REDACTED] (10/14/2020 14:27:24 PDT):

> [REDACTED] has flagged to me that Twitter might be in process of backtracking

[REDACTED] (10/14/2020 14:28:26 PDT):

>Unclear what that means, will update

[REDACTED] (10/14/2020 15:11:07 PDT):

><https://twitter.com/realDonaldTrump/status/1316501350658707456>

[REDACTED] (10/14/2020 15:11:07 PDT):

><https://twitter.com/realDonaldTrump/status/1316501350658707456>

[REDACTED] (10/14/2020 15:26:33 PDT):

shared: 121161847_1316086545401657_7329363007398542195_n.png

[REDACTED] (10/14/2020 15:58:10 PDT):

shared: 121570689_337558230646825_1230117776855863053_n.png

[REDACTED] (10/14/2020 15:58:52 PDT):

>Biden campaign

Joel D. Kaplan (10/14/2020 16:01:08 PDT):

>To [REDACTED]'s point, if there are 40,000 emails or texts on there, we will need to have a position on whether we are labeling them, removing them, or leaving them alone.

[REDACTED] (10/14/2020 16:01:47 PDT):

>yes - and esp as they get to the private things about hunter (any drugs, sex stuff etc) that is going to be particularly sensitive on how we handle....

[REDACTED] (10/14/2020 16:03:10 PDT):

>I think our position is that we are determining whether they qualify for a newsworthy exception on a case-by-case basis. If they don't qualify, they would be removed. If they do qualify, they would either stay up or be labeled, depending on what we decide.

Nick Clegg (10/14/2020 16:04:06 PDT):

>Using which labels, when we label?

[REDACTED] (10/14/2020 16:04:43 PDT):

>Do we feel firm on "newsworthy" definition?

[REDACTED] (10/14/2020 16:06:34 PDT):

>If I understood [REDACTED]'s description from before, we would tend to think that content that went directly to the Vice President's behavior would be newsworthy. Content that just relates to Hunter Biden's character or personal conduct would not.

>
>The label would be the one that the team worked out today. I personally would not label the content. I would leave up newsworthy content without a label and explain ourselves.

[REDACTED] (10/14/2020 16:06:40 PDT):

>It's a balancing test, so there's inherent tension in the definition. Generally speaking, I think things about the personal behavior of the candidate's son that do not involve the candidate do not have a public interest factor.

[REDACTED] (10/14/2020 16:07:51 PDT):

>It seems like the vast majority of the content obtained from the laptop of a candidate's child would not be newsworthy.

[REDACTED] (10/14/2020 16:09:34 PDT):

><https://mol.im/a/8841255>

[REDACTED] (10/14/2020 16:13:06 PDT):

>Should we be removing these images and links to them?

[REDACTED] (10/14/2020 16:13:29 PDT):

>Because they are not newsworthy and were hacked?

[REDACTED] (10/14/2020 16:14:28 PDT):

>Looking now.

[REDACTED] (10/14/2020 16:17:04 PDT):

>Yes, I would remove these images and link to the images. They are from the same source we determined is a hack under our rules and they do not have a public interest value.

Joel D. Kaplan (10/14/2020 16:17:44 PDT):

>We are going to remove the content of every publisher who published pictures of the candidate's son doing drugs as not newsworthy? Years of stories about the adult family members of Presidents would suggest that that content is newsworthy.

[REDACTED] (10/14/2020 16:20:28 PDT):

>On another front:

>

>WaPo is doing a wrap on the story today and what's to know if we were in touch with Biden before our action. We were not. Confirmed by [REDACTED] and [REDACTED].

>

>Can we confirm?

Joel D. Kaplan (10/14/2020 16:20:50 PDT):

>The article also says that the shop owner was tasked with "data recovery." At what point does a "hack" become just a "leak" from a whistleblower?

[REDACTED] (10/14/2020 16:21:20 PDT):

>Our policy is to remove materials that were hacked unless newsworthy. These aren't photos that a friend who was in the room took and posted. Our public interest language is: We assign special value to content that brings to light a serious or imminent threat to public health and safety, relates to the misconduct of a prominent person in public life, or gives voice to a perspective currently being debated as part of a political process. We assign special value to content where the speaker is using the platform for educational purposes, to express the perspective of a vulnerable or a protected group of people, to express national or cultural identity, or to protest or facilitate peaceful assembly.

[REDACTED] (10/14/2020 16:22:25 PDT):

>Our assessment is here: FBI confirmed that they have one or more laptops in their custody

>It was allegedly dropped off at a repair shop in Delaware

>No evidence that this is Hunter Biden's laptop save some stickers

>Shop owner allegedly did not know who dropped it off, but then produced a receipt for Hunter Biden

>The shop owner allegedly alerted the FBI to the existence of the laptop

>The shop owner allegedly made copies of the contents of the computer for Rudy Giuliani's lawyer (this likely violates the shop owner's responsibility to safeguard this private data)

>The grand jury subpoena for the laptop does not connect the laptop to Hunter Biden

>These are private communications that - if authentic - belong to the person who owns the

laptop

>The repair guy disclosed those communications to third parties without approval of the owner (his own claims)

>Those communications were further disseminated by individuals also without approval of the owner (their own claims)

>The disinfo research community is broadly concerned that this pattern of dissemination (seed compromising and possibly forged material with an ideologically aligned cutout, then get that information published in a less-than-reputable press outlet)

>The content from the laptop itself is unverified and exists in image form. Some analysts have alleged there may be evidence of photoshop or manipulation, including image file metadata showing it was processed in photoshop before being turned into an image file.

[REDACTED] (10/14/2020 16:23:20 PDT):

>I did not have any contact with the campaign before making any decisions. While analyzing the information, I asked if we had spoken with the campaign and was told no.

[REDACTED] (10/14/2020 16:30:15 PDT):

>@Nick Clegg, @Joel Kaplan, should we escalate this question about the photos to Sheryl?

[REDACTED] (10/14/2020 16:30:43 PDT):

>My sense is that it's going to be very difficult to chase this stuff

Joel D. Kaplan (10/14/2020 16:34:11 PDT):

>I think we need to develop some options here. For instance, my instinct is that the Presidents adult son engaging in illegal drug use meets the standard of newsworthiness. Illicit photos of him engaged in a sexual act, not so much.

Joel D. Kaplan (10/14/2020 16:34:33 PDT):

>But that's not much to base policy guidance on.

Joel D. Kaplan (10/14/2020 16:36:08 PDT):

>(Or rather, that the Presidential candidate's adult son!)

[REDACTED] (10/14/2020 16:41:23 PDT):

>Options:

>

>1. Go with current definition, in relevant part "relates to the misconduct of a prominent person in public life." Joe Biden is a prominent person in public life, but I assume Hunter Biden is not.

>

>2. Adopt a broader definition given historical/view that the misconduct of a President or aspiring President's close associates and family is relevant to voters. Could simply say that we will treat close associates and family as if they were prominent people in public life. [REDACTED] is someone posted a hacked video of a candidate engaged in consensual sexual behavior, we would remove that, right, because it isn't misconduct?

>

>3. Variant of 2 would be to split the difference somehow - wouldn't allow all of the same content about a candidate's child as we would allow about the candidate, but perhaps "illegal behavior" instead of "misconduct." Not sure

Nick Clegg (10/14/2020 16:42:34 PDT):

>No need to ask Sheryl now - she'll prob say take it down to most of these decisions - but we do need options to guide us on what could be an intense period of whack a mole. My instinct would be to remove this stuff here, especially as will no doubt come under attack for allowing original NY Post to be going viral as we speak. I am comfortable trying to shield Biden jr from intrusion into his privacy.

[REDACTED] (10/14/2020 16:44:16 PDT):

>Confirming that we will tell the Post: no Biden contact prior to referral to 3PFCs

[REDACTED] (10/14/2020 16:44:43 PDT):

>That makes sense to me, Nick. At its core, the newsworthiness test is about weighing the public interest in seeing content against the risk of harm. Both are pretty low here. It's not really news that Hunter Biden has done drugs or engaged in other bad behavior. But the risk of harm to leaving the stuff up is minimal for the same reason. Feels like the right line is probably the one [REDACTED] and [REDACTED] articulated

[REDACTED] (10/14/2020 16:46:02 PDT):

>Right line is the current test, allow hacked materials if they "relate to the misconduct of a prominent person in public life," and treat only the candidates (and spouses?) but not children as prominent people in public life?

Final Report 1033

[REDACTED] (10/14/2020 16:46:53 PDT):

>Yes, that seems about right. How do others feel?

[REDACTED] (10/14/2020 16:47:31 PDT):

>If we do think that risk of harm of leaving stuff up is low, we might also want to consider the operational challenges of trying to stay on top of actioning tens of thousands of pieces of content

Joel D. Kaplan (10/14/2020 16:48:39 PDT):

>I don't really buy how the adult son of a VP who is being accused of influence peddling for a foreign company is not considered a prominent person in public life. And if Fox concludes that misconduct is newsworthy—pretty consistent with the standards that have applied to adult children of presidents for decades—I don't really buy it's not newsworthy either.

Nick Clegg (10/14/2020 16:49:14 PDT):

>You mean tens of thousands of pieces of content re Hunter Biden, or all offspring of prominent politicians? The former is a pretty atypical case right now and I think we should be nimble in dealing with the atypical focus on him and his private woes/life rather than solve for operational simplicity on our part.

[REDACTED] (10/14/2020 16:49:33 PDT):

>I meant content for Hunter Biden

[REDACTED] (10/14/2020 16:50:05 PDT):

>Slightly exaggerating, but I think I saw someone mention that there were 40,000 pieces of content on the laptop?

Nick Clegg (10/14/2020 16:50:41 PDT):

>So where do we draw the line - I don't really understand why sex might be beyond the pale but drug taking is fair game?

[REDACTED] (10/14/2020 16:52:23 PDT):

>Sorry, catching up, was managing something else briefly.

[REDACTED] (10/14/2020 16:56:08 PDT):

>I would draw the line at pictures of him engaging in personal activities that aren't related to his father. Because they are images, we can bank them. And again, this is because the original images are subject to our hack policy. If he'd released the images or whoever was in the room with him released them, we would not take action.

[REDACTED] (10/14/2020 16:56:54 PDT):

>(Unless the image otherwise violated, and sexual activity violates.)

Nick Clegg (10/14/2020 16:58:03 PDT):

>That intuitively makes sense to me - Hunter Biden is a legit object of scrutiny because of his alleged business ties and how/whether he roped in his father to help with them, but private images of sex, drugs released without his permission seem to me to be another matter.

[REDACTED] (10/14/2020 16:59:06 PDT):

>Twitter has released their policy explanation for actions today: <https://twitter.com/TwitterSafety/status/1316525303930458115?s=20>

[REDACTED] (10/14/2020 16:59:18 PDT):

>In addition to the Daily Mail, the NY Post has also published some of these images.

[REDACTED] (10/14/2020 17:01:15 PDT):

><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 17:01:41 PDT):

>And Jack just tweeted on this: <https://twitter.com/jack/status/1316528193621327876>

[REDACTED] (10/14/2020 17:12:53 PDT):

>Sorry - is this line the decision? I want to be sure we have alignment and that folks understand we would be removing content from NY Post, Daily Mail, and potentially others. I can start the teams on looking for the images to see what other high profile users may have posted if that's helpful.

[REDACTED] (10/14/2020 17:13:37 PDT):

>Or are we holding on the images as well until morning?

Nick Clegg (10/14/2020 17:14:42 PDT):

>If we can hold till morning I think we should - so much churn right now. Possible?

[REDACTED] (10/14/2020 17:15:11 PDT):

>Yes. I'll ask the teams to keep doing research overnight so that we have a better sense of scale in the morning.

Nick Clegg (10/14/2020 17:15:41 PDT):

>And does the Dorsey explanation/clarification alter our calculus at all?

[REDACTED] (10/14/2020 17:17:19 PDT):

>Not for me. I thought they explained themselves clearly and, to be frank, that they've put themselves in a more defensible position than we're in right now.

Joel D. Kaplan (10/14/2020 17:23:48 PDT):

>I agree that Twitter is in a much more coherent position right now and thus easier to defend. I think either removal or labeling (on newsworthiness grounds) is defensible, if not equally well-received. I think a demotion tied to possible falsity, when none of the parties are actually suggesting the emails/images are false, at least so far-will be increasingly hard to defend. (The fact that the FBI apparently has the laptops may explain why no one in the Biden campaign is denying the authenticity).

[REDACTED] (10/14/2020 17:30:46 PDT):

>Agree with Joel on all fronts

[REDACTED] (10/14/2020 18:47:11 PDT):

><https://twitter.com/superwuster/status/1316553405498875910?s=21>

Joel D. Kaplan (10/14/2020 18:48:42 PDT):

>Awesome. I bet he wishes he didn't light the fuse that has led to our FTC case now!

Joel D. Kaplan (10/14/2020 18:58:27 PDT):

>I will see your Tim Wu and raise you a Josh Hawley. (Remains to be seen whether he will try and do this before the election):

Joel D. Kaplan (10/14/2020 18:58:32 PDT):

><https://twitter.com/HawleyMO/status/1316535709021491200?s=20>

Joel D. Kaplan (10/14/2020 20:38:15 PDT):

>This video is up on Twitter and FB. I assume we may see it submitted as an ad soon, if it hasn't been already. Shows two emails.

Joel D. Kaplan (10/14/2020 20:38:18 PDT):

><https://www.facebook.com/DonaldTrump/videos/713788112569060/?vh=e&extid=0&d=n>

[REDACTED] (10/14/2020 20:43:52 PDT):

>Flagged to IPOC to keep an eye out for ads

[REDACTED] (10/14/2020 20:44:18 PDT):

>We are agreed that this content in an ad should be rejected, correct?

[REDACTED] (10/14/2020 20:55:45 PDT):

>That would be our agreed-Upon policy application

[REDACTED] (10/14/2020 21:10:22 PDT):

>[REDACTED] team says their guidance is to enforce an ads submission reactively upon escalation - is that your input? I'm trying to figure out if we could flag proactively (before going live); trying to avoid replay of caravan ad (which was auto-approved)...

[REDACTED] (10/14/2020 21:21:11 PDT):
>I actually don't know where that guidance came from

[REDACTED] (10/14/2020 21:21:23 PDT):
>So was just trying not to give contradicting instruction

[REDACTED] (10/14/2020 21:22:08 PDT):
>Enforcing on an ad reactively on escalation seems suboptimal because it means it runs

[REDACTED] (10/14/2020 21:22:39 PDT):
>But I didn't know where that guidance had come from so didn't want to change it without more consultation

[REDACTED] (10/14/2020 21:23:15 PDT):
>Yes i want to avoid it running, exactly. Will ensure team has clear guidance to proactively review/prevent if possible (may take some creative engineering or manual intervention...).

[REDACTED] (10/14/2020 21:23:45 PDT):
>Does anyone disagree? [REDACTED] [REDACTED] suggested this was an instruction from policy.

[REDACTED] (10/14/2020 21:33:11 PDT):
>Just wanting to make sure I understand. the ads would not be rejected for misinformation because it has only been enqueued for fact checking. there has not been any fact check rating to disqualify an ad.

>
>But we would reject ads based on violating our hack policy. though we will say we are allowing same content in organic because it is newsworthy.

[REDACTED] (10/14/2020 21:33:31 PDT):
>Yes, that's my understanding

[REDACTED] (10/14/2020 21:33:47 PDT):
>Newsworthy exception does not apply to ads

[REDACTED] (10/14/2020 21:52:01 PDT):
> [REDACTED] thought this was guidance from this afternoon's meeting - I'm afraid that I am completely blanking on any discussion of proactive versus reactive enforcement of our hacking policy in ads. I only recall that we said we would enforce.

>
>Is there any reason to limit enforcement to reactive?

[REDACTED] (10/14/2020 21:53:24 PDT):
>Not that I can think of. Team is now working with engineering to allow a proactive filter.

[REDACTED] (10/14/2020 21:56:34 PDT):
>Okay, we're moving to proactive (to extent possible) but please speak up if you have any concerns about that. (Very uncomfortable removing a rule when I don't know why it was established!)

Exhibit 8

Message

From: ██████████ [mailto:██████████@facebook.com] [/O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=53781AA26A03437E85AF7C858A5EDA62]
Sent: 10/14/2020 1:45:00 PM
To: ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com;
Subject: Message summary [{"otherUserFbId":null,"threadFbId":██████████}]

██████████ (10/14/2020 06:33:36 PDT):
 >FYI. Our legal team is reaching out to FBI on this.
 >
 ><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

██████████ (10/14/2020 06:55:39 PDT):
 >Busy morning, per ██████████'s comments on DOJ. ICYMI from Axios: The U.S. Justice Department is expected to charge Google with antitrust violations any day now, but that doesn't mean it will call for a breakup of the alleged monopoly. At least not yet.
 >
 >DOJ is said to be primarily focused on Google's core search business, rather than side products that could be more easily divested, according to Axios' Ashley Gold. It's still unclear if DOJ believes anticompetitive acquisitions contributed to the current condition.
 >Expect the process to go like this: DOJ sues, alleging bad behavior but without proposing specific remedies (save for a lawyerly version of "knock it off").
 >
 >Google files to dismiss, but that's largely performative.
 >The case moves into litigation, during which DOJ can get more information to bolster its case.
 >The two sides discuss possible remedies that would result in a settlement. Either they succeed, which is what both sides would probably prefer, or the case goes to trial.
 >What to know: DOJ has increasingly favored behavioral remedies over structural ones. That said, DOJ leadership may change come January, and Politico reports that there have been discussions about trying to require Google to sell off its Chrome browser.
 >
 >Wildcards: Predicting specifics of Trump administration actions is a bit like predicting whether or not a 5-year-old will like what you made for dinner. Even if he gobbled it up last Wednesday, it's possible that he'll toss it on the floor tonight.
 >
 >Meanwhile, Google reportedly is requiring employees to be cautious when discussing matters that could touch on antitrust – establishing a process for how such discussions should be memorialized, so that DOJ can't obtain the notes.
 >Bottom line: Any Big Tech company breakup would have wide-ranging ramifications, including for startup competition and the universe of strategic acquirers. But so far there's no reason to expect the delivery of Baby Googles, even if it soon gets served.

██████████ (10/14/2020 13:44:17 PDT):
 >Now for something just happy and fun!

██████████ (10/14/2020 13:44:42 PDT):
 ><https://thedcline.org/2020/10/14/facebook-kennedy-center-partnership-bolsters-anti-racism-in-the-performing-arts-while-offering-a-new-outlet-for-dc-artists/>

██████████ (10/14/2020 13:45:00 PDT):
 >👍👍👍 love that headline

Exhibit 9

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=FC04F5354C4141A1A2C3BA2C943F37B0>

To: [REDACTED]

Sent: 10/14/2020 7:10:45 PM

Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]

Attachments: 31749174_118143832395613_2865212093781508096_n.gif;
52286689_2344575149146222_8511502978731999232_n.gif;
53469541_2310592939221342_897605485773979648_n.gif;
120886463_257061805728718_2433750737572093545_n.gif;
121186603_630021014356002_5002011545448654826_n.jpg;
121574359_403213744400511_7118563285716987168_n.jpg;
121605944_1381160638744315_611390386845681113_n.png;
121662635_689773671646517_5207408251684467722_n.png; sticker.png; sticker1.png;
sticker2.png; sticker3.png; sticker4.png; sticker5.png; sticker6.png; sticker7.png

[REDACTED] (10/14/2020 07:18:41 PDT):

>I'm awake. Let me know if I need to do anything on the Hunter Biden stuff.

[REDACTED] (10/14/2020 07:18:47 PDT):

>And good morning!!!

[REDACTED] (10/14/2020 07:18:59 PDT):

>Lulz

[REDACTED] (10/14/2020 07:19:04 PDT):

>Define "good"

[REDACTED] (10/14/2020 07:19:09 PDT):

> [REDACTED] is reviewing for Misinfo Policy

[REDACTED] (10/14/2020 07:19:13 PDT):

>If we can enqueue it with 3PFCs, that would be useful.

[REDACTED] (10/14/2020 07:19:19 PDT):

>I guess the one question

[REDACTED] (10/14/2020 07:19:25 PDT):

>Yup what [REDACTED] said

[REDACTED] (10/14/2020 07:19:25 PDT):

>We have a briefer with CNN in 40 min

[REDACTED] (10/14/2020 07:19:28 PDT):

>Donie will be on

[REDACTED] (10/14/2020 07:19:32 PDT):

>So I expect he will ask.

[REDACTED] (10/14/2020 07:19:56 PDT):

>We are in reasonably good shape to explain, but if we can say it has been enqueued, at least we don't sound totally helpless.

[REDACTED] (10/14/2020 07:20:06 PDT):

>Closer to the end than we were yesterday.

[REDACTED] (10/14/2020 07:20:32 PDT):

>Is there a hold up on enqueueing?

[REDACTED] (10/14/2020 07:21:06 PDT):

>I just got the article, so haven't search for signal of falsity yet

[REDACTED] (10/14/2020 07:21:09 PDT):

[REDACTED] (10/14/2020 07:21:20 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 07:21:25 PDT):

>Sounds like predicted VPVs are massive

[REDACTED] (10/14/2020 07:21:30 PDT):

>Which is not surprising.

[REDACTED] (10/14/2020 07:21:46 PDT):

>I'll skim the article and look too. No statement from the campaign?

[REDACTED] (10/14/2020 07:21:56 PDT):

>Nope. I wouldn't touch it if I were them.

[REDACTED] (10/14/2020 07:22:18 PDT):

>Lots and lots of disinfo experts online calling out places where it is sketchy, untrustworthy, potentially false.

[REDACTED] (10/14/2020 07:22:52 PDT):

>This feels like one that will get looked at in a microscope retroactively for how fast we were.

[REDACTED] (10/14/2020 07:23:00 PDT):

>Can you put some here so [REDACTED] can make the falsity determination?

[REDACTED] (10/14/2020 07:25:13 PDT):

><https://twitter.com/ridt/status/1316363540421316609?s=21>

[REDACTED] (10/14/2020 07:26:58 PDT):

><https://twitter.com/juddlegum/status/1316359549843103744?s=21>

[REDACTED] (10/14/2020 07:27:20 PDT):

>Found this as well: <https://twitter.com/maggieNYT/status/1316364878924447746>

[REDACTED] (10/14/2020 07:27:26 PDT):

>[REDACTED] - the legum thread is good enough for media reporting. Let's enqueue.

[REDACTED] (10/14/2020 07:27:43 PDT):

>That's the right call.

[REDACTED] (10/14/2020 07:27:56 PDT):

>Yep that makes sense

[REDACTED] (10/14/2020 07:28:19 PDT):

>[REDACTED] mentioned separately that there are efforts underway to contact FBI (I'm entirely uncertain who is in on that process, but I'd advise caution in that exchange).

[REDACTED] (10/14/2020 07:28:20 PDT):

>Thank you!

[REDACTED] (10/14/2020 07:28:30 PDT):

>We've checked with them - no Intel back yet.

[REDACTED] (10/14/2020 07:28:39 PDT):

>And partnerships can do outreach because it's about Biden.

[REDACTED] (10/14/2020 07:28:50 PDT):

>There is a standing meeting btwn Ti and FBI for later today.

[REDACTED] (10/14/2020 07:29:43 PDT):

>Also calling out that if we wanted to, we could demote this as journalists are calling out that there is much about the story that is suspicious (our policy now allows us to do this). I wouldn't advocate that we do so since it sounds like this is just unproven at the moment but it is an option

[REDACTED] (10/14/2020 07:30:16 PDT):

>I'm chatting with [REDACTED] now (who is the Biden campaign contact on P&G). she has not heard from them on this. Should I ask her to proactively outreach?

[REDACTED] (10/14/2020 07:30:27 PDT):

>What are the projected VPVs?

[REDACTED] (10/14/2020 07:30:42 PDT):

>No, I think we have what we need.

[REDACTED] (10/14/2020 07:30:50 PDT):

>[REDACTED] analysis is great

[REDACTED] (10/14/2020 07:30:58 PDT):

>#vpv 3630932923627559

[REDACTED] (10/14/2020 07:32:40 PDT):

>Let's demote. I think the disbelief signals are there.

[REDACTED] (10/14/2020 07:33:29 PDT):

>I'll ask Ops to demote and enqueue to tier 1 of the queue

[REDACTED] (10/14/2020 07:33:50 PDT):

>We should figure out what we can say about this when it gets raised by Donie in the CNN brief in 30 min.

[REDACTED] (10/14/2020 07:33:59 PDT):

>Would love to be able to say we have demoted and enqueued.

[REDACTED] (10/14/2020 07:34:19 PDT):

>I have some good language to emphasize the role of the press here and whole of society/etc.

[REDACTED] (10/14/2020 07:34:30 PDT):

>But if we can say those two things, it's clear we are on it and doing our part.

[REDACTED] (10/14/2020 07:34:41 PDT):

>We have approved tps for enqueued content.

[REDACTED] (10/14/2020 07:35:13 PDT):

>Got it - where do I find those?

[REDACTED] (10/14/2020 07:35:14 PDT):

>I don't think we've ever talked about publicly about pre-fact checked demotions so please don't do so with comms sign off.

[REDACTED] (10/14/2020 07:35:34 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 07:35:44 PDT):

>Hey just coming online and catching up.

[REDACTED] (10/14/2020 07:35:57 PDT):

>We have publicly confirmed we temp demote pending fact-checker review.

[REDACTED] (10/14/2020 07:36:10 PDT):

>Oh great.

[REDACTED] (10/14/2020 07:36:34 PDT):

>May just be careful not to overstate the effect of demotions - something like this could go viral, regardless.

[REDACTED] (10/14/2020 07:36:38 PDT):

>Oh awesome.

[REDACTED] (10/14/2020 07:36:41 PDT):

>Can you pull the tps for [REDACTED]? I can't seem to share or copy from the doc. (Yay for good security practices)

Final Report 1042

[REDACTED] (10/14/2020 07:37:02 PDT):

>Back in 5 min as I drive through cell dead area in vt!

[REDACTED] (10/14/2020 07:37:25 PDT):

>Yes will grab then.

[REDACTED] (10/14/2020 07:37:31 PDT):

>[REDACTED] just said: "so on the CNN briefing, to be consistent with how we typically describe, we should say that the content is eligible to be fact checked and in the meantime, its distribution on-platform is being reduced"

[REDACTED] (10/14/2020 07:47:17 PDT):

>Some questions from [REDACTED] on urls. This one, <https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/> seems to be the one Legum calls out.

>

>There is also this one: https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook AND

>

><https://nypost.com/2020/10/14/obama-conference-call-leaked-to-burisma-biden-emails/>

>

>Are we enqueueing all 3?

[REDACTED] (10/14/2020 07:48:31 PDT):

>*sorry, [REDACTED] calls out (per [REDACTED] message above)

[REDACTED] (10/14/2020 07:49:41 PDT):

>The second one also purports to be information from the supposed laptop, which is being questioned by Legum, et al

[REDACTED] (10/14/2020 07:49:58 PDT):

>Given we aren't looking at specific claims here, more so that the underlying stories are being questioned by commentators, it seems appropriate to do all. But, am not so hot on the specifics of the case

[REDACTED] (10/14/2020 07:50:56 PDT):

>Okay - let's use the laptop as the trigger as it's what's being challenged by media, and treat content based on the laptop the same with demote and enqueue. And we should probably set up a badge cause it's gonna be a long day.

[REDACTED] (10/14/2020 07:50:56 PDT):

>I'd agree that we should enqueue all of them based on the overlap in the stories, but defer to @ [REDACTED] / @ [REDACTED] on the right policy action here.

[REDACTED] (10/14/2020 07:52:41 PDT):

>The third URL references that the Ukrainian prosecutor was investigating Burisma, which the Legum thread debunks. So I think we can demote and enqueue all 3. Assuming we're taking the position we'll demote and enqueue content that references the supposed Beau Biden laptop

[REDACTED] (10/14/2020 07:53:25 PDT):

>But the third URL does not specifically call out it came from the Beau Biden laptop (it just references "emails" obtained by the Post)

[REDACTED] (10/14/2020 07:54:38 PDT):

>Ok, am going to confirm on the esc thread that we are E&D all three, and will do same for other stories making the claim about the laptop. Agree [REDACTED] and [REDACTED]?

[REDACTED] (10/14/2020 07:55:03 PDT):

>Based on what [REDACTED] and [REDACTED] said that sounds ight to me

[REDACTED] (10/14/2020 07:55:09 PDT):

>Haven't read any of the articles yet

[REDACTED] (10/14/2020 09:13:00 PDT):

>Pinning

[REDACTED] (10/14/2020 09:19:39 PDT):

>"Today's situation" == the hunter/Biden drop?

[REDACTED] (10/14/2020 09:23:20 PDT):

>Yes.

[REDACTED] (10/14/2020 09:23:21 PDT):

>Wanted to make sure everyone was aware that [REDACTED] did tweet concurrently with this that this content was sent to fact-checkers: [https://twitter.com/\[REDACTED\]/status/1316395902479872000?s=20](https://twitter.com/[REDACTED]/status/1316395902479872000?s=20)

[REDACTED] (10/14/2020 09:23:48 PDT):

>But Partnerships is aware that we're not to reach out directly

[REDACTED] (10/14/2020 09:23:54 PDT):

>Perfect, thanks.

[REDACTED] (10/14/2020 09:24:37 PDT):

>Worth noting [REDACTED]'s tweet doesn't actually say it was sent to fact-checkers - just that it's eligible for fact checking. I know that was a line he was being careful about.

[REDACTED] (10/14/2020 09:25:06 PDT):

>[REDACTED] - let's pull down the meeting that's in five minutes and see if we can sneak it in tomorrow or friday morning?

[REDACTED] (10/14/2020 09:25:20 PDT):

>On it.

[REDACTED] (10/14/2020 09:28:22 PDT):

>This is so . . . something. [REDACTED], [REDACTED] and I are on the CNN brief now, and someone just said our energy is down.

[REDACTED] (10/14/2020 09:28:29 PDT):

>Not sure if they were joking or not

[REDACTED] (10/14/2020 09:29:57 PDT):

>Yeah. I feel punchy if anything.

[REDACTED] (10/14/2020 09:29:09 PDT):

>I just want to scream -- HEY YOU KNOW THERE STUFF IN THE WORLD GOING ON

[REDACTED] (10/14/2020 09:29:31 PDT):

>...do it.

[REDACTED] (10/14/2020 09:30:01 PDT):

>You should 'def' do that, [REDACTED]

[REDACTED] (10/14/2020 09:30:23 PDT):

>I'm just glad I managed to plug that we "warned about information dumps in the waning days of the campaign a few weeks ago" in the prez.

[REDACTED] (10/14/2020 09:31:18 PDT):

>it was a good one

[REDACTED] (10/14/2020 09:31:59 PDT):

>Fake news. [REDACTED]'s energy is always fully charged!

[REDACTED] (10/14/2020 09:38:49 PDT):

>So is all of this coming from Gulliani and the Trump campaign?

[REDACTED] (10/14/2020 09:39:21 PDT):

>The NY Post is essentially dedicating all of their resources to this, which tells you something

[REDACTED] (10/14/2020 09:40:27 PDT):

>Let's keep speculation to a minimum and focus on applying our policies evenly to whatever content comes to us. Final Report 1045

[REDACTED] (10/14/2020 09:42:21 PDT):

>Want to confirm we should still be enqueueing/demoting new articles that references these emails to be recovered from Beau Biden's laptop or refer to the Ukrainian prosecutor being fired while investigating Burisma (the company was no longer under scrutiny at the time of firing)?

>There's a Daily Mail piece and an NY Post opinion article with those claims. That's consistent with the NY Post decisions but wanted to double check after the direction from leadership not to reach out to 3PFCs

[REDACTED] (10/14/2020 09:46:16 PDT):

>@ [REDACTED] -- for your awareness, [REDACTED] just noted this in another thread:

[REDACTED] (10/14/2020 09:46:18 PDT):

>From a 3PFC in a Slack w/all of our US partners: "Hello, Facebook people. So, uh, what's up with this? Was distribution actually reduced on this story? And is he trying to get us to fact-check this?"

[REDACTED] (10/14/2020 09:51:39 PDT):

>All shark aside, I don't understand what that means?

[REDACTED] (10/14/2020 09:52:11 PDT):

>I think that they are wondering if they should prioritize.

[REDACTED] (10/14/2020 09:52:36 PDT):

>my impression is that we would have done outreach on stuff we want them to prioritize.

[REDACTED] (10/14/2020 09:53:09 PDT):

>[REDACTED] also said that even though the content is marked at Tier 1, it is lower in the queue (I don't understand her explanation for why, but maybe [REDACTED] can explain)

[REDACTED] (10/14/2020 09:53:45 PDT):

>I think it's because Community Review (crowdsourcing) has not yet rated the content, which would then get re-prioritized in the queue after their rating

[REDACTED] (10/14/2020 09:53:57 PDT):

>Ah, okay.

[REDACTED] (10/14/2020 09:54:10 PDT):

>Does [REDACTED] typically respond to comments like that or do we just leave it alone?

[REDACTED] (10/14/2020 09:54:47 PDT):

>It's in a Slack channel so think she generally responds. I think the hesitancy was we enqueue/demoted but affirmatively did not want to do outreach.

[REDACTED] (10/14/2020 09:56:05 PDT):

>Okay - I'll pass to leadership.

[REDACTED] (10/14/2020 09:00:44 PDT):

>So the NY Post stories do contain the emails themselves, with private email addresses. (At the least gmail address is "private" -- even if we don't know if it is real). And I assume Hunter Biden's email address was also private. I doubt the email addresses themselves are in the thumbnails that show up on platform. But I will flag for OCP to see if any of these violate for PII.

[REDACTED] (10/14/2020 09:01:47 PDT):

>[REDACTED] and can we add the OCP on call here?

[REDACTED] (10/14/2020 09:02:31 PDT):

>Sorry - I thought I'd replied. We're seeking leadership guidance on this.

[REDACTED] (10/14/2020 09:03:18 PDT):

>Adding @ [REDACTED] who is OCP on-call and @ [REDACTED] who is IPOC lead today for OCP

[REDACTED] (10/14/2020 09:04:27 PDT):
>@ [REDACTED] - whatever comment you made earlier today about how this content isn't factcheck-able is now being used as a bludgeon against us doing anything to address this content.

[REDACTED] (10/14/2020 09:04:36 PDT):
>?

[REDACTED] (10/14/2020 09:04:52 PDT):
>Defer to leadership but can we answer in straightforward way... we were getting incoming questions from press on our response so we needed to reply but we defer to 3PFC on whether to engage?

[REDACTED] (10/14/2020 09:04:55 PDT):
>Oh - on the internal 2020 discussion thread?

[REDACTED] (10/14/2020 09:05:15 PDT):
>Want me to recant / clarify?

[REDACTED] (10/14/2020 09:06:28 PDT):
> [REDACTED] and [REDACTED] -- to bring you all up to date -- the NY Post and the Daily Mail have posted stories (see above) that are on-platform. The content has been demoted and enqueued for fact-checkers. The stories contain supposed emails between a Ukrainian and Hunter Biden (Joe Biden's son). The stories publish their email addresses. Can you review to see if these qualify for removal for PII (though I don't think that the email addresses are on the story thumbnails).

[REDACTED] (10/14/2020 09:06:36 PDT):
>And let me see if I can pull the UIDs for the content

[REDACTED] (10/14/2020 09:06:41 PDT):
>It's probably too late but may be worth trying.

[REDACTED] (10/14/2020 09:09:51 PDT):
>Still no decision on continuing to enqueue/demote/badge.

[REDACTED] (10/14/2020 09:10:14 PDT):
>For press, I think we keep responding with what [REDACTED] initially said. It continues to be accurate, right?

[REDACTED] (10/14/2020 09:10:29 PDT):
>Here's a NY Post Facebook post in which the story contains email addresses/PII

[REDACTED] (10/14/2020 09:10:31 PDT):
><https://www.facebook.com/NYPost/posts/10166129714110206>

[REDACTED] (10/14/2020 09:10:59 PDT):
>This one as well

[REDACTED] (10/14/2020 09:11:01 PDT):
><https://www.facebook.com/NYPost/posts/10166129598755206>

[REDACTED] (10/14/2020 09:11:29 PDT):
>So my question is, would these violate for PII, or does the PII need to be in the thumbnail or otherwise on platform?

[REDACTED] (10/14/2020 09:13:11 PDT):
>As far as I'm aware, [REDACTED] to confirm nothing has changed with respect to initial 3 (?) urls being enqueued with demotion.

[REDACTED] (10/14/2020 09:15:01 PDT):
>Yes, that should still be accurate. I enqueued/demoted a couple other lower-profile URLs but nothing else like Daily Mail, other NY Post URLs

[REDACTED] (10/14/2020 09:15:51 PDT):
>Thanks [REDACTED], let me look now

[REDACTED] (10/14/2020 09:19:24 PDT):

>Are any of us joining [REDACTED] call now on this?

Final Report 1047

[REDACTED] (10/14/2020 09:19:50 PDT):

>I'm on

[REDACTED] (10/14/2020 09:19:54 PDT):

> [REDACTED] was trying to get you, @ [REDACTED]

[REDACTED] (10/14/2020 09:20:05 PDT):

>Cool. I'll dial in. I know [REDACTED] is on too.

[REDACTED] (10/14/2020 09:20:24 PDT):

>i am in the middle of an interview right now. [REDACTED] [REDACTED] and [REDACTED] are running on this right now. I can jump off and get on [REDACTED] call in a few if needed

[REDACTED] (10/14/2020 09:26:33 PDT):

>Call has been worthwhile, if for no other reason than that [REDACTED] surfaced we were no longer demoting for unknown reasons -- he's digging in with Product.

[REDACTED] (10/14/2020 09:27:23 PDT):

>Yeah oh god

[REDACTED] (10/14/2020 09:28:03 PDT):

>seriously

[REDACTED] (10/14/2020 09:28:27 PDT):

>@ [REDACTED] nice job answer questions with clear answers.

[REDACTED] (10/14/2020 09:44:00 PDT):

>Hi all.

> [REDACTED] will circle back shortly with a full assessment that he's working on right now, but our initial assessment is that there is no PII violation. We have found both emails (Vadym's email v.pocharskyi.ukraine@gmail.com and Hunter's hbiden@rosemontseneca.com) in a public gov't document from AUG 2020:

>[https://www.hsgac.senate.gov/imo/media/doc/2020-08-28-Tramontano 20Interview 20with 20Exhibits.pdf](https://www.hsgac.senate.gov/imo/media/doc/2020-08-28-Tramontano%20Interview%20with%20Exhibits.pdf)

[REDACTED] (10/14/2020 09:44:27 PDT):

>you will get the full assessment in the next 10min.

[REDACTED] (10/14/2020 09:47:57 PDT):

>Thanks @ [REDACTED] -- this is what I figured, but wanted to make sure we had the call from OCP

[REDACTED] (10/14/2020 09:48:32 PDT):

> [REDACTED] and [REDACTED] - noting one minor thing

[REDACTED] (10/14/2020 09:48:38 PDT):

>it won't change the assessment

[REDACTED] (10/14/2020 09:49:50 PDT):

>because the fact remains these two emails are found by easy google search and publically available

[REDACTED] (10/14/2020 09:48:58 PDT):

>(not to mention the Rosemont website is down and it is probably there too)

[REDACTED] (10/14/2020 09:49:08 PDT):

>but these two links and reports are from the Homeland Security committee

[REDACTED] (10/14/2020 09:49:12 PDT):

>notably chaired by Johnson.

[REDACTED] (10/14/2020 09:49:25 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 09:49:35 PDT):

>so just to be aware on for the obvious reasons that folks close to this will recognize and call out quicklky

[REDACTED] (10/14/2020 09:50:30 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 09:51:12 PDT):

>Hi all - confirming that our assessment is non-violating, with a detailed assessment here:
>

[REDACTED] (10/14/2020 09:54:11 PDT):

>Update from the SR call: (1) Publishers including NY Post and Daily Mail are upset we're demoting journalist, (2) Twitter chatter inc Don Jr criticizing stifling of what they see as bad press for the left, (3) We're still waiting to respond to 3PFCs who are also wondering what we want them to do, (4) We're still holding on enqueuing/demoting new claims pending leadership decision. And not to make things too complicated, but it sounds like the NY Post URLs might not be demoted at all due to a filter protecting top publishers

[REDACTED] (10/14/2020 09:54:58 PDT):

>Well that last piece is an interesting twist. Who is running that to ground?

[REDACTED] (10/14/2020 09:55:14 PDT):

>We are. Sounds like it's solvable, though

[REDACTED] (10/14/2020 09:55:55 PDT):

>I think key things to align on are 1) do we want to stand behind decision to demote, hopefully yes since said we're doing it. 2) how much detail should we share about relevant policies, as we haven't been public about manual enqueueing previously and our language on auto enqueueing could come across as vague.

[REDACTED] (10/14/2020 09:57:47 PDT):

>From leadership - tell the inquiring 3PFCs to use their judgment.

[REDACTED] (10/14/2020 09:58:21 PDT):

>and we're back - noting that this other article has a different email for Hunter (under Richard Biden - his full name)

[REDACTED] (10/14/2020 09:58:24 PDT):

>and for a Devon Archer

[REDACTED] (10/14/2020 09:58:26 PDT):

>we are looking now

[REDACTED] (10/14/2020 09:58:27 PDT):

>https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook&fbclid=IwAR3qnQZrvM7eH3su0eZEy611ld4r62219q0enOF-KCjZ2P0hqGWQub7yrVt

[REDACTED] (10/14/2020 09:58:53 PDT):

>From leadership - do not manually enqueue, demote, or badge additional content.

[REDACTED] (10/14/2020 09:59:16 PDT):

>This is like their 5th article today on this

[REDACTED] (10/14/2020 09:59:22 PDT):

> can you update other threads with those two updates from [REDACTED] now?

[REDACTED] (10/14/2020 09:59:31 PDT):

>(Or let me know if you're focused on Product stuff and I will.)

[REDACTED] (10/14/2020 10:00:12 PDT):

>indeed. from my old NY days, i can speak from experience tht when the Post decides to go after someone they really do!

[REDACTED] (10/14/2020 10:00:35 PDT):

>Yes. Just for visibility, they will be applying a bespoke solution to bypass the filter

and demote 2 NY Post URLs that should've already been demoted. But will ask them to stand down on anything else, including the 3rd NY Post already that should've already been demoted/enqueued but wasn't

[REDACTED] (10/14/2020 10:01:13 PDT):
>Remind me why we are treating 2 vs 3rd NY Post differently?

[REDACTED] (10/14/2020 10:02:02 PDT):
>It sounds like there was miscommunication and they didn't demote/enqueue. I don't think we specified how many URLs we were demoting

[REDACTED] (10/14/2020 10:02:32 PDT):
>Publicly, that is

[REDACTED] (10/14/2020 10:03:09 PDT):
>OK, so principle is that we are following through and demoting the two specific urls we specifically gave instruction to demote, given we have confirmed to press content was demoted, but per leadership guidance are not taking any further action?

[REDACTED] (10/14/2020 10:03:52 PDT):
>that's correct

[REDACTED] (10/14/2020 10:05:10 PDT):
>Let's give Product the go ahead, [REDACTED]!

[REDACTED] (10/14/2020 10:05:52 PDT):
>I thought [REDACTED] gave instructions to demote 3 posts

[REDACTED] (10/14/2020 10:05:59 PDT):
>Sorry, meetings stacked and I'm heading to an AG briefing. Anything I can help with other than witty retorts and tortured metaphors?

[REDACTED] (10/14/2020 10:06:01 PDT):
>hey guys - so quick update on teh Devon Archer and Richard Biden emails

[REDACTED] (10/14/2020 10:06:07 PDT):
>in this latest link

[REDACTED] (10/14/2020 10:06:21 PDT):
>He did. But there were crossed wires and 1 wasn't demoted. Since leadership has asked not to take any new actions, we're leaving the third one alone

[REDACTED] (10/14/2020 10:06:31 PDT):
>1) Richard Biden - we can't find it based on cursory search. Except obviously in things dating over the last day. So this may indeed qualify as a link to PII.

[REDACTED] (10/14/2020 10:07:12 PDT):
>2) Devon Archer - we have found in a wikileaks link that includes a spreadsheet of donors. So technically available though by wikileaks. Thoguh noting again that the Rosemont website is down, so not clear if it is listed on there.

[REDACTED] (10/14/2020 10:12:42 PDT):
>Note: we are working on a separate assessment - will circle back shortly

[REDACTED] (10/14/2020 10:12:58 PDT):
>Does this fall in line of "take no further action" right now [REDACTED] ?

[REDACTED] (10/14/2020 10:14:37 PDT):
>note that as of now, we cannot find either of these emails before about 8 hours ago

[REDACTED] (10/14/2020 10:14:49 PDT):
>so we are drawing up assessment now that this likely violates our policies

[REDACTED] (10/14/2020 10:15:05 PDT):
>if there is anyone with search skills nad bandwidth

[REDACTED] (10/14/2020 10:15:10 PDT):
>to double down and make sure they can't find the emails

[REDACTED] (10/14/2020 10:15:15 PDT):

>we welcome search parties on this

[REDACTED] (10/14/2020 10:15:34 PDT):

>When we have the assessment, we'll need to go to leadership.

[REDACTED] (10/14/2020 10:17:50 PDT):

>Is the potential PII in one of the links that is NOT being demoted?

[REDACTED] (10/14/2020 10:18:33 PDT):

>And can we include our protocols around PII for when it's not on platform but a link to off platform? (Which I'm assuming is the case here -- sorry, struggling to keep up with the thread!)

[REDACTED] (10/14/2020 10:19:23 PDT):

> - fyi - IS topline related to PII is: Do not share and/or ask for any of the listed private information types, either on our products or through external links.

[REDACTED] (10/14/2020 10:19:23 PDT):

>This was the article accidentally not enqueued: <https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 10:19:54 PDT):

>in short, and i will confirm, we don't have protocols related to this since we explicitly do not allow PII even in external links on the platform.

[REDACTED] (10/14/2020 10:20:10 PDT):

>but confirming this was your question and point.

[REDACTED] (10/14/2020 10:29:35 PDT):

>What's ETA on the PII assessment? Sorry to push.

[REDACTED] (10/14/2020 10:31:27 PDT):

>coming in 1 minute

[REDACTED] (10/14/2020 10:31:28 PDT):

>literally

[REDACTED] (10/14/2020 10:32:51 PDT):

>

[REDACTED] (10/14/2020 10:33:36 PDT):

>Is this one of the enqueued articles or one of the others?

[REDACTED] (10/14/2020 10:34:43 PDT):

>that is don't know - [REDACTED]?

[REDACTED] (10/14/2020 10:34:59 PDT):

>Checking

[REDACTED] (10/14/2020 10:35:01 PDT):

>This is the one NY Post article that was not enqueued by accident: <https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 10:35:05 PDT):

>if this was the one accidentally not enqueued, then it's another one!

[REDACTED] (10/14/2020 10:35:19 PDT):

><https://www.facebook.com/NYPost/posts/10166129598755206>

>This one is enqueued

[REDACTED] (10/14/2020 10:35:43 PDT):

>and that's the one the assessment is for!

[REDACTED] (10/14/2020 10:35:50 PDT):

>I'm so sorry, but I'm having trouble following the chat.

[REDACTED] (10/14/2020 10:36:14 PDT):

>Is the content with the PII link already enqueued and demoted or not?

[REDACTED] (10/14/2020 10:36:47 PDT):

>@ [REDACTED] is that what you're saying?

[REDACTED] (10/14/2020 10:36:50 PDT):

>Sorry for confusion.

>Yes, enqueued!

>Will let [REDACTED] confirm as well.

[REDACTED] (10/14/2020 10:36:50 PDT):

>@ [REDACTED] - here is the link that [REDACTED] wants to confirm:

[REDACTED] (10/14/2020 10:36:52 PDT):

>https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook&fbclid=IwAR3qnQZcvM7eH3suOeZEy6111d4z62218q0enOF-KCjZ2P0hqGWQub7ycVh

[REDACTED] (10/14/2020 10:37:08 PDT):

>OK, thanks. [REDACTED] and I can triple check.

[REDACTED] (10/14/2020 10:41:04 PDT):

>Waiting for Ops...

[REDACTED] (10/14/2020 10:46:16 PDT):

>I'm getting on a leadership call now, so will prolly be pinging a lot of question here.

[REDACTED] (10/14/2020 10:46:25 PDT):

>Apologies in advance.

[REDACTED] (10/14/2020 10:46:27 PDT):

>There are 2 very similar URLs. This one is currently enqueued with demotion:

<https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/>

[REDACTED] (10/14/2020 10:46:27 PDT):

>we are ready for you!

[REDACTED] (10/14/2020 10:46:50 PDT):

>This one is not enqueued/demoted: https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook&fbclid=IwAR3qnQZcvM7eH3suOeZEy6111d4z62218q0enOF-KCjZ2P0hqGWQub7ycVh

[REDACTED] (10/14/2020 10:47:10 PDT):

> [REDACTED] - is this the same one as I linked above?

[REDACTED] (10/14/2020 10:47:22 PDT):

>think [REDACTED] just needs a straight answer on if what we assessed was demoted or not

[REDACTED] (10/14/2020 10:47:35 PDT):

>This is the one you shared [REDACTED]

[REDACTED] (10/14/2020 10:47:41 PDT):

>It has not been enqueued and demoted.

[REDACTED] (10/14/2020 10:48:01 PDT):

>But that may be misleading for your purpose

[REDACTED] (10/14/2020 10:48:10 PDT):

>in that a very similar url has been enqueued and demoted

[REDACTED] (10/14/2020 10:48:22 PDT):

>I think OCP should look at the first url [REDACTED] shared

[REDACTED] (10/14/2020 10:48:40 PDT):

>to see if content that your assessment is based on is in that url

Final Report 1052

[REDACTED] (10/14/2020 10:48:44 PDT):
>if that makes sense

[REDACTED] (10/14/2020 10:49:07 PDT):
>which URL? sorry - way too many URLs.

[REDACTED] (10/14/2020 10:49:13 PDT):
>This one

[REDACTED] (10/14/2020 10:49:32 PDT):
>Let us know if helpful to get on phone so we can spare [REDACTED] back and forth.

[REDACTED] (10/14/2020 10:49:56 PDT):
>[REDACTED] - separately making sure you are seeing [REDACTED] updates on other thread re: Twitter likely removing.

[REDACTED] (10/14/2020 10:50:29 PDT):
>[REDACTED] those are the same exact article though.

[REDACTED] (10/14/2020 10:50:59 PDT):
>So sorry - I still don't understand on the PII. How many articles is it in and have those articles been enqueued?

[REDACTED] (10/14/2020 10:51:44 PDT):
>Sorry [REDACTED] - I just side-pinged to spare you and so we can get this answer ASAP for you

[REDACTED] (10/14/2020 10:51:45 PDT):
>We may need help from Product understanding url functionality, as they are telling us that there are two urls that appear to the naked eye exactly the same, but one has been enqueue and demoted and one hasn't.

[REDACTED] (10/14/2020 10:55:30 PDT):
>[REDACTED] - there are two links - both the NYPost with the exact same headline and with the emails referenced in the 2nd assessment.

[REDACTED] (10/14/2020 10:55:56 PDT):
>Article 1: was not demoted and here it is: https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/?utm_campaign=SocialFlow&sr_share=facebook&utm_medium=SocialFlow&utm_source=NYPFacebook&fbclid=IwAR3qnQZzvM7eH3suOeZEy611ld4zc62218q0enOF-KCjZ2P0hqGWQub7yzVk

[REDACTED] (10/14/2020 10:56:16 PDT):
>Article 2: was demoted and here it is: <https://nypost.com/2020/10/14/hunter-biden-emails-show-leveraging-connections-with-dad-to-boost-burisma-pay/>

[REDACTED] (10/14/2020 11:02:22 PDT):
>Okay, we're likely going to remove the content with links to PII.

[REDACTED] (10/14/2020 11:02:46 PDT):
>sounds good

[REDACTED] (10/14/2020 11:02:52 PDT):
>[REDACTED] - was there discussion on the twitter front

[REDACTED] (10/14/2020 11:02:54 PDT):
>We want to advise the Post what we're doing. Can someone reach out to partnerships and comms to start drafting exactly what we'll say to the Post.

[REDACTED] (10/14/2020 11:02:56 PDT):
>and whether we want to consider as hacked

[REDACTED] (10/14/2020 11:03:39 PDT):
>assumption being that unless the person had a password to the laptop it was unauthorized access and therefore to consider this hacked.

[REDACTED] (10/14/2020 11:03:44 PDT):

>Not a final decision, but let's get ready on the PII piece.

Final Report 1053

[REDACTED] (10/14/2020 11:03:54 PDT):

>copy that and sounds good

[REDACTED] (10/14/2020 11:04:14 PDT):

>I think we need a hacked assessment plus a newsworthy assessment

[REDACTED] (10/14/2020 11:04:44 PDT):

>I'm presuming we'll make a newsworthy determination overall, but let's do the work.

[REDACTED] (10/14/2020 11:04:53 PDT):

>got it

[REDACTED] (10/14/2020 11:04:58 PDT):

>just to make sure i am understanding and move out

[REDACTED] (10/14/2020 11:05:05 PDT):

>we will make an assessment under our hacked policy

[REDACTED] (10/14/2020 11:05:18 PDT):

>and then layer on top of that the newsworthiness consideration and whetehr this meets public interest

[REDACTED] (10/14/2020 11:05:24 PDT):

>we will get to work on that now

[REDACTED] (10/14/2020 11:05:42 PDT):

>assume @ [REDACTED] or @ [REDACTED] - you two are leading on [REDACTED] point above on partnerships/comms outreach?

[REDACTED] (10/14/2020 11:06:02 PDT):

>Yes, I think: (1) we need to assess whether the content violates our policies against hacked materials (sounds like that is how twitter is handling) and (2) is the content newsworthy?

[REDACTED] (10/14/2020 11:06:25 PDT):

>got it. moving out now.

[REDACTED] (10/14/2020 11:06:32 PDT):

>Justto be crystal clear - we need to be ready on outreach but it shouldn't happen until we have further green light.

[REDACTED] (10/14/2020 11:06:54 PDT):

>@ [REDACTED] and I are talking about this on another thread as well.

[REDACTED] (10/14/2020 11:07:14 PDT):

>On the Comms piece - that will need to await the assessment, right? So they can put together a comms statement?

[REDACTED] (10/14/2020 11:07:30 PDT):

>Or should we use the PII assessment?

[REDACTED] (10/14/2020 11:07:36 PDT):

>No. [REDACTED] is saying the PII assessment

[REDACTED] (10/14/2020 11:07:47 PDT):

>to reach out now to partnerships/Comms on that side of it

[REDACTED] (10/14/2020 11:07:58 PDT):

>Got it -- will do

[REDACTED] (10/14/2020 11:09:05 PDT):

>whether the hack/newsworthiness will be considered will come in a bit but in the meantime, should move out on that piece!

[REDACTED] (10/14/2020 11:09:30 PDT):

>(FYSA: Twitter on Gov/Industry call -- ongoing -- confirm they'll be removing)

[REDACTED] (10/14/2020 11:08:39 PDT):

> let me and [REDACTED] know if we can help you connect with people on Comms and Partnerships who have been engaging on misinfo side.

[REDACTED] (10/14/2020 11:08:42 PDT):

>Adding [REDACTED] and [REDACTED] here

[REDACTED] (10/14/2020 11:09:04 PDT):

> [REDACTED] - OCP needs all your factual information and details regarding the laptop, access to the emails, etc.

[REDACTED] (10/14/2020 11:09:13 PDT):

>for the OCP assessment w/r/t hacking

[REDACTED] (10/14/2020 11:09:30 PDT):

>can you send bullet points in an email in the next 10 minutes to me, [REDACTED] and [REDACTED]?

[REDACTED] (10/14/2020 11:09:33 PDT):

>toplines

[REDACTED] (10/14/2020 11:09:36 PDT):

>Yeah

[REDACTED] (10/14/2020 11:09:45 PDT):

>Reposting something I send in a separate thread a second ago

[REDACTED] (10/14/2020 11:09:46 PDT):

>I think this is a good argument. I'd structure it as

>

>These are private communications that - if authentic - belong to the person who owns the laptop

>

>The repair guy disclosed those communications to third parties without approval of the story (his own claims)

>

>Those communications were further disseminated by individuals also without approval of the owner (their own claims)

[REDACTED] (10/14/2020 11:09:54 PDT):

>we can clean that up and add addl info ([REDACTED] should have it)

[REDACTED] (10/14/2020 11:10:01 PDT):

>tldr: our hacked policy is based on the fact that someone who was not authorized accessed information and distributed it.

[REDACTED] (10/14/2020 11:10:04 PDT):

>please send in an email

[REDACTED] (10/14/2020 11:10:07 PDT):

>to spare the thread

[REDACTED] (10/14/2020 11:10:14 PDT):

>yep, drafting now

[REDACTED] (10/14/2020 11:10:19 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 11:11:33 PDT):

>For visibility - [REDACTED] is POC for Comms on the NY Post removal (if it happens) and she is currently working on Comms for it.

[REDACTED] (10/14/2020 11:12:01 PDT):

>Can I share the OCP assessment with her [REDACTED]?

[REDACTED] (10/14/2020 11:12:19 PDT):

>yeah i don't see why not

[REDACTED] (10/14/2020 11:12:23 PDT):
>would just caveat that this is rough

[REDACTED] (10/14/2020 11:12:26 PDT):
>for internal CP

[REDACTED] (10/14/2020 11:12:40 PDT):
>but has the substance and framing she needs and we are happy to clarify / polish if she needs at any point

[REDACTED] (10/14/2020 11:13:40 PDT):
>Can SRP get a single source of truth document going that we can share with comms/partnerships/etc as decisoin get made?

[REDACTED] (10/14/2020 11:14:14 PDT):
>[REDACTED] as you're probably tracking this is what SR had pulled together earlier:
<https://docs.google.com/document/d/1lYsJWhxUJeXnpAkvyrQElSuhM4hvjf4qcRp9m0FOGtw/edit>

[REDACTED] (10/14/2020 11:14:34 PDT):
>We likely need some reactive comms indicating our standards are separate and apart from any local law (ie. we don't care about 'abandoned property' arguments, etc).

[REDACTED] (10/14/2020 11:15:38 PDT):
>Twitter's blocking of the link about to happen, and then blocking the articles themselves coming shortly after.

[REDACTED] (10/14/2020 11:16:27 PDT):
>@ [REDACTED] is the Partnerships SPM for NY Post [REDACTED] or someone else?

[REDACTED] (10/14/2020 11:16:44 PDT):
>Checking

[REDACTED] (10/14/2020 11:18:14 PDT):
>[REDACTED] I think it's [REDACTED] but [REDACTED] has been tracking this actively re NY Post as well

[REDACTED] (10/14/2020 11:18:27 PDT):
>I'll ping both of them.

[REDACTED] (10/14/2020 11:19:44 PDT):
>@ [REDACTED] I don't have access to this doc -- and [REDACTED] said in another thread that they weren't adding people while decisions are outstanding. So I'm just going to create my own. It's extra work, but I think it is will be useful to have a Content Policy document for now and can merge/add, if we need to.

[REDACTED] (10/14/2020 11:20:42 PDT):
>@ [REDACTED] - can you send whatever you have as of now?

[REDACTED] (10/14/2020 11:20:54 PDT):
>Yes

[REDACTED] (10/14/2020 11:21:14 PDT):
>also, if not already shared, Twitter plans to denylist several of the articles and repositories of this content

[REDACTED] (10/14/2020 11:21:20 PDT):
>I can share the specific URLs if useful

[REDACTED] (10/14/2020 11:21:57 PDT):
>just need facts of the laptop as we know it now

[REDACTED] (10/14/2020 11:21:59 PDT):
>thanks!

[REDACTED] (10/14/2020 11:22:06 PDT):
>or whatever you have ready

[REDACTED] (10/14/2020 11:23:07 PDT):

>rgr

[REDACTED] (10/14/2020 11:23:10 PDT):

>2 minutes, cleaning it u

[REDACTED] (10/14/2020 11:24:10 PDT):

>Pls do include [REDACTED]@fb.com, @ [REDACTED]

[REDACTED] (10/14/2020 11:24:36 PDT):

> anyone else besides you and [REDACTED]

[REDACTED] (10/14/2020 11:24:51 PDT):

>yes - the people above

[REDACTED] (10/14/2020 11:24:56 PDT):

>me, [REDACTED]

[REDACTED] (10/14/2020 11:25:07 PDT):

>thanks [REDACTED]

[REDACTED] (10/14/2020 11:28:53 PDT):

>sent!

[REDACTED] (10/14/2020 11:30:06 PDT):

>fascinating

[REDACTED] (10/14/2020 11:30:07 PDT):

>thank you

[REDACTED] (10/14/2020 11:30:09 PDT):

>folding in now

[REDACTED] (10/14/2020 11:30:15 PDT):

>we will revert shortly with the full assessment doc

[REDACTED] (10/14/2020 11:30:18 PDT):

>thanks [REDACTED]

[REDACTED] (10/14/2020 11:30:29 PDT):

>Thanks for pulling that so quickly [REDACTED]

[REDACTED] (10/14/2020 11:30:41 PDT):

>all credit to @ [REDACTED] for centralizing it!

[REDACTED] (10/14/2020 11:30:54 PDT):

shared: 31749174_118143832395613_2965212093791509096_n.gif

[REDACTED] (10/14/2020 11:52:11 PDT):

>Feel free to ignore me if this is a distraction and may no longer be relevant, but Comms is looking for input on how we message the decision to temp demote IF we end up not taking any other action on the content we temp demoted earlier today. The issue is that we manually temp demoted based on credible signal of falsity from journalists. This is per policy. But we haven't been public about that policy. So options are 1) Just use high-level language about temp demotions that we have already used publicly before ("When we see that a post shows signs of being false, we may temporarily reduce its distribution pending review by a third-party fact-checker. This might be triggered because we see a high number of reports from users or comments expressing disbelief. The goal is to take action faster before it goes viral and give our fact-checkers time to do their job.") OR 2) specifically, and more accurately add into the above "or other signals from experts", which is what we relied on here, but may invite questions about which experts we rely on and whether FB employees are involved in those decisions. [REDACTED] if you come up for air and believe this is relevant, let me know if you have a view. I have a slight preference for (1) even though I find it a tad misleading for this particular case.

[REDACTED] (10/14/2020 11:53:12 PDT):

>What's the status of the hacked/newsworthy assessments?

Final Report 1057

[REDACTED] (10/14/2020 11:54:22 PDT):

>Wrapping it up - will drop in 2mins

[REDACTED] (10/14/2020 11:54:54 PDT):

>What's the tldr?

[REDACTED] (10/14/2020 11:55:42 PDT):

>Violates hacked policy, we are not in favor of the NW allowance but are providing arguments on both sides

[REDACTED] (10/14/2020 11:56:39 PDT):

[REDACTED] (10/14/2020 11:59:03 PDT):

>requested access

[REDACTED] (10/14/2020 11:59:12 PDT):

>me too

[REDACTED] (10/14/2020 12:00:00 PDT):

>done and done

[REDACTED] (10/14/2020 12:00:13 PDT):

>thank you.

[REDACTED] (10/14/2020 12:00:16 PDT):

>All should have access, but shout if you need it

[REDACTED] (10/14/2020 12:02:04 PDT):

>So this assessment only applies to one NY Post article, not all of their articles about it this morning?

[REDACTED] (10/14/2020 12:04:35 PDT):

>Should this apply to any stories that reprint the source materials?

[REDACTED] (10/14/2020 12:06:21 PDT):

>yes -

[REDACTED] (10/14/2020 12:06:26 PDT):

>anything with a link to source materials

[REDACTED] (10/14/2020 12:09:42 PDT):

>That analysis looks excellent

[REDACTED] (10/14/2020 12:09:53 PDT):

>Thank you to OCP for jamming on it so quickly!

[REDACTED] (10/14/2020 12:10:05 PDT):

>I think it lays out the facts and our choices here well.

[REDACTED] (10/14/2020 12:10:22 PDT):

>@ [REDACTED] @ [REDACTED] Let us know if you need more from Security Policy as this gets escalated.

[REDACTED] (10/14/2020 12:10:41 PDT):

>Note that it looks like Twitter's action has landed, and covered articles are coming down from their platform.

[REDACTED] (10/14/2020 12:25:03 PDT):

>Importing issue raised in separate thread. I read the assessment to flag any quick lines in the event this escalation is reviewed externally down the line.

>

>Raising for the group whether this may overstate: "3. No evidence that this is Hunter Biden's laptop save some stickers."

>

>If we're judging signals within the article itself (though the coverage may not be

accurate), we may want to assume a reasonable person could infer the presence of personal correspondence and sensitive images is at least 'some' evidence the hardware is linked to Hunter or someone with access to Hunter's files.

>Could re-state: "No **direct** evidence that this is Hunter Eiden's laptop save some stickers."

[REDACTED] (10/14/2020 12:35:10 PDT):
>I've started tracking things here: [REDACTED]

[REDACTED] (10/14/2020 12:35:18 PDT):
>Everyone should have access

[REDACTED] (10/14/2020 12:35:34 PDT):
>what a fun day!

[REDACTED] (10/14/2020 12:35:38 PDT):
>everyone hydrating?!

[REDACTED] (10/14/2020 12:35:41 PDT):
>stay hydrated people!

[REDACTED] (10/14/2020 12:35:52 PDT):
>go yourself some gatorade and ritz crackers

[REDACTED] (10/14/2020 12:36:16 PDT):
>I've go to go get my boys in about 30 minutes, and will be out of pocked for a little bit, but just got off of a VC with [REDACTED] and gave her the low down (with some of the twists and turns) and she'll take over

[REDACTED] (10/14/2020 12:36:39 PDT):
>go get the boys [REDACTED]!

[REDACTED] (10/14/2020 12:37:00 PDT):
>Don't worry. We aren't going anywhere.

[REDACTED] (10/14/2020 12:37:02 PDT):
>do i have to???

[REDACTED] (10/14/2020 12:37:03 PDT):
>@ [REDACTED] - welcome to the party

[REDACTED] (10/14/2020 12:37:09 PDT):
>LOL

[REDACTED] (10/14/2020 12:37:12 PDT):
>I'll go!

[REDACTED] (10/14/2020 12:37:24 PDT):
>hahah

[REDACTED] (10/14/2020 12:37:29 PDT):
>[REDACTED] - I won't

[REDACTED] (10/14/2020 12:42:55 PDT):
>Looks like everyone is having the most fun in this chat. Still getting caught up so feel free to @ me if there is anything you need immediately!

[REDACTED] (10/14/2020 12:47:24 PDT):
>glad you asked [REDACTED].

[REDACTED] (10/14/2020 12:47:35 PDT):
>i think i can speak for everyone when i say we all need margaritas.

[REDACTED] (10/14/2020 12:47:42 PDT):
>i would like mine on the rocks

[REDACTED] (10/14/2020 12:47:43 PDT):
>with salt.

[REDACTED] (10/14/2020 12:47:45 PDT):
>stat.

[REDACTED] (10/14/2020 12:47:59 PDT):
>agave or simple syrup?

[REDACTED] (10/14/2020 12:48:35 PDT):
>i don't think it matters if you are making it with enough tequila.

[REDACTED] (10/14/2020 12:49:31 PDT):
shared: 53469541_2310592939221342_997605485773979648_n.gif

[REDACTED] (10/14/2020 12:49:56 PDT):
>FYI - fact checkers are having a hard time rating this. here's from LeadStories (one of our most aggressive fact-checkers): "Lead Stories: "It's a tough one to fact check quickly. We are looking, researching, reaching out, though. We have been very aggressively debunk the other crazy conspiracy about Biden plotting to murder Seal Team 6. We have a lot of good primary reporting on it." also, i am being inspired to drink

[REDACTED] (10/14/2020 12:56:15 PDT):
>@ [REDACTED] and @ [REDACTED] -- can I get you all to add in any details about 3PFC in the document above. I started a 3PFC section, but want to make sure you all put the latest details

[REDACTED] (10/14/2020 13:02:29 PDT):
shared: 120886463_257061805728718_2433750737572093545_n.gif

[REDACTED] (10/14/2020 13:02:36 PDT):
>FYI since [REDACTED] just flagged to thread with [REDACTED] and [REDACTED] we got a HERO escalation on a Breitbart article re: Hunter Biden. It's about FB demoting NY Post. <https://www.facebook.com/Breitbart/posts/10166338277205354>

[REDACTED] (10/14/2020 13:02:52 PDT):
>did someone say margarita? i'm def in the right chat

[REDACTED] (10/14/2020 13:02:59 PDT):
shared: 52286689_2344575149146222_8511502978731999232_n.gif

[REDACTED] (10/14/2020 13:33:45 PDT):
>OCP, not sure if this is the same email being evaluated earlier, but this post by the press secretary just came through HERO: <https://www.facebook.com/KayleighMcEnany7/photos/a.675511112508409/3521177921275033/?type=1&theater>

[REDACTED] (10/14/2020 13:34:42 PDT):
>We would consider this screenshot to be source material, correct?

[REDACTED] (10/14/2020 13:37:08 PDT):
>we would need folks to tell us the source of this email

[REDACTED] (10/14/2020 13:37:13 PDT):
>is this coming from the laptop

[REDACTED] (10/14/2020 13:37:16 PDT):
>this tranche?

[REDACTED] (10/14/2020 13:37:32 PDT):
shared: sticker.png

[REDACTED] (10/14/2020 13:37:38 PDT):
>to be clear we didn't assess individual emails - just the overall theory of the hacked computer

[REDACTED] (10/14/2020 13:37:45 PDT):

>yes this appears to be the same email that was seen in the same tranche

[REDACTED] (10/14/2020 13:39:19 PDT):

>then would be considered violating as hacked material

[REDACTED] (10/14/2020 13:38:23 PDT):

>unless newsworthiness is applied

[REDACTED] (10/14/2020 13:39:44 PDT):

>Is the email there one of the PII emails?

[REDACTED] (10/14/2020 13:40:04 PDT):

>no

[REDACTED] (10/14/2020 13:40:08 PDT):

>it is the hunter rosemont email

[REDACTED] (10/14/2020 13:40:11 PDT):

>which does not violate

[REDACTED] (10/14/2020 13:40:14 PDT):

>is publically available

[REDACTED] (10/14/2020 13:41:12 PDT):

>Is Pocharsky's Gmail considered PII?

[REDACTED] (10/14/2020 13:43:59 PDT):

>looks to be publically available so not violating - [https://www.hsgac.senate.gov/imo/media/doc/2020-09-28-Tramontano 20Interview 20with 20Exhibits.pdf](https://www.hsgac.senate.gov/imo/media/doc/2020-09-28-Tramontano%20Interview%20with%20Exhibits.pdf)

[REDACTED] (10/14/2020 13:44:08 PDT):

>not surprisingly - the same homeland security report

[REDACTED] (10/14/2020 13:44:30 PDT):

>[https://www.hsgac.senate.gov/imo/media/doc/2020-09-31-Painter 20Interview 20with 20Exhibits.pdf](https://www.hsgac.senate.gov/imo/media/doc/2020-09-31-Painter%20Interview%20with%20Exhibits.pdf)

[REDACTED] (10/14/2020 13:44:42 PDT):

>Ah. Thanks.

[REDACTED] (10/14/2020 13:45:19 PDT):

> [REDACTED] is pinging me: "hey is the press secretary post being reviewed for PII". is there anything i can relate? apologies if this has been discussed

[REDACTED] (10/14/2020 13:45:45 PDT):

>I think [REDACTED] just confirmed above it's not PII

[REDACTED] (10/14/2020 13:45:56 PDT):

>you can let her know

[REDACTED] (10/14/2020 13:46:04 PDT):

>that I have confirmed it would not qualify as PII

[REDACTED] (10/14/2020 13:46:11 PDT):

>since both emails are publically available

[REDACTED] (10/14/2020 13:51:05 PDT):

>A Washington past time. I am caught behind a VP motorcade movement....

[REDACTED] (10/14/2020 13:52:22 PDT):

>"this material is allowed for public awareness, even though it may contain material from a hacked source" is the leadership language in [REDACTED] doc right now.

[REDACTED] (10/14/2020 13:52:36 PDT):

>Okay - we're winding to a decision.

[REDACTED] (10/14/2020 13:53:00 PDT):

>We'll label content that includes or links to the source material. (Don't act on any of this yet but want to keep you guys looped)

[REDACTED] (10/14/2020 13:53:24 PDT):

>If 3PFCs all confirm they're never gonna fact check, we will remove the demotion on the demoted articles

[REDACTED] (10/14/2020 13:53:38 PDT):

>If they say they will fact check, we'll start enqueueing related content (without demotion)

[REDACTED] (10/14/2020 13:53:46 PDT):

>'hacked' could imply all the docs are real -- any way to cover possibility they're fabricated?

[REDACTED] (10/14/2020 13:53:49 PDT):

>Reach out to Post re PII

[REDACTED] (10/14/2020 13:54:13 PDT):

>Important point

[REDACTED] (10/14/2020 13:54:15 PDT):

>No, and hacked was the conclusion we passed up the chain. If they're fake, we don't do anything.

[REDACTED] (10/14/2020 13:54:49 PDT):

>And then remove content and links that contain the PII.

[REDACTED] (10/14/2020 13:55:43 PDT):

>when you give the go ahead, we'll ask partnerships to report back on 3PFC plans either way. as of now, my understanding is they're still looking into it

[REDACTED] (10/14/2020 13:55:53 PDT):

>Will provide final guidance once a decision is made.

[REDACTED] (10/14/2020 13:56:20 PDT):

>Realistically, with 3PFCs we'll see some respond to us to say they aren't going to fact check, but we won't hear from all of them. So not sure we would get to a place where we have clarity on lifting demotion, checking that's OK?

[REDACTED] (10/14/2020 13:57:09 PDT):

>[Fine to take this off-thread, but real or purported 'hack' puts it in our policy scope, regardless of whether they are what they purport to be -- but what we message could really make a difference here: "include unverified information that may have been hacked" is an alternative] cc @ [REDACTED]

[REDACTED] (10/14/2020 14:04:32 PDT):

>@ [REDACTED] the questions on the [REDACTED] call are specific to what inform treatment would/would not apply to for PII

[REDACTED] (10/14/2020 14:04:40 PDT):

>I dont have much background on this - are you able to join?

[REDACTED] (10/14/2020 14:06:16 PDT):

>The PII will be removed

[REDACTED] (10/14/2020 14:06:50 PDT):

>The inform treatment will go on content that shows or links to the source material (emails or anything else purportedly from the laptop).

[REDACTED] (10/14/2020 14:07:02 PDT):

>Content that discusses but does not display the source material is left alone.

[REDACTED] (10/14/2020 14:09:12 PDT):

>and we are good to socialize this now?

[REDACTED] (10/14/2020 14:11:14 PDT):

>Questions from another thread:

>
 >Triggering team prioritizing as follows:
 >P0 - Content with the NYPost URL
 >P1 - High VPV content with the hacked material directly uploaded
 >P2 - How to start applying this automatically (we're planning manual application now)
 >We need clarity on the following:
 >1) Who can approve treatments on other links/articles that contain the hacked materials?
 >2) Should we add the treatment to articles that link to the hacked material (but don't host it directly), or quote the hacked material vs. attach it?
 >3) Do we have a POV on ads?

[REDACTED] (10/14/2020 14:13:18 PDT):
 >#2 is yes on link and no on quote. I don't know what attach means here?

[REDACTED] (10/14/2020 14:16:59 PDT):
 >Decisions:
 >1. Label hacked materials (source materials or links to source materials)
 >2. Partnerships reaches out to Post re PII to say remove or redact or we'll remove
 >3. After #2, we remove PII from Post and any other place we find it
 >4. Ongoing convos with 3PFCs

[REDACTED] (10/14/2020 14:17:05 PDT):
 >[REDACTED] is running #1.

[REDACTED] (10/14/2020 14:17:19 PDT):
 >Partnerships has #2.

[REDACTED] (10/14/2020 14:17:34 PDT):
 >Once Partnerships is done, we should work with Ops on #3.

[REDACTED] (10/14/2020 14:17:38 PDT):
 >I'll circle back on #4.

[REDACTED] (10/14/2020 14:17:54 PDT):
 >Leadership is meeting again at 3:30

[REDACTED] (10/14/2020 14:18:59 PDT):
 >I'm sure this will result in more questions and answers, so start compiling ones that we need leadership to weigh in on.

[REDACTED] (10/14/2020 14:24:02 PDT):
 >On this, if there will be a bunch of questions, let's put them in a gdoc because I won't be able to keep track in the thread.

[REDACTED] (10/14/2020 14:24:21 PDT):
 >we can leverage our sot doc

[REDACTED] (10/14/2020 14:24:32 PDT):
 >[REDACTED]

[REDACTED] (10/14/2020 14:25:02 PDT):
 >[REDACTED] to close the loop on one item that came up before, we reportedly could not demote content enqueued to 3PFCs because of the Alexa filter (which blocks temp demotion for content from the most visited websites). turns out we did manually enqueue/demote, but our tools were broken so we didn't know it at the time. the alexa filter does block temp demotion for content our classifiers auto-enqueue, but doesn't affect manually enqueued content. will note this in the doc [REDACTED] shared

[REDACTED] (10/14/2020 14:26:07 PDT):
 >do we happen to know who from partnerships is owning this and where they will confirm its complete?

[REDACTED] (10/14/2020 14:26:35 PDT):
 >I don't. Maybe check with [REDACTED]?

[REDACTED] (10/14/2020 14:26:49 PDT):
 >[REDACTED], one outstanding question from our team on messaging is in there. As I believe leadership is aware, we have Congresspeople + publishers reaching out re temp demotion

policies (which now seem like the smallest part of this but may still be a big deal to those audiences), so ideally we can get Comms to align on clear reactive messaging we can use with those audiences on how our policies applied, including the temp demotions.

[REDACTED] (10/14/2020 14:27:14 PDT):

> [REDACTED] reach out to [REDACTED] and [REDACTED] on that thread I added you into

[REDACTED] (10/14/2020 14:27:16 PDT):

>Oh wait. They're polling the 3PFCs on fact checking before making the PII call to the post.

[REDACTED] (10/14/2020 14:27:20 PDT):

>So it might be a bit.

[REDACTED] (10/14/2020 14:27:39 PDT):

>They are the N.Y. POST SPMs

[REDACTED] (10/14/2020 14:27:45 PDT):

>From partnerships

[REDACTED] (10/14/2020 14:28:26 PDT):

>can we help in chatting with [REDACTED]? we haevn't discussed what outreach to 3PFCs is still needed--please let me know, and i can ping her on our running chat

[REDACTED] (10/14/2020 14:28:40 PDT):

>are we allowing ads to run this content?

[REDACTED] (10/14/2020 14:29:56 PDT):

>We didn't discuss. I can take that to leadership.

[REDACTED] (10/14/2020 14:30:05 PDT):

>Are there ads running that include the source content?

[REDACTED] (10/14/2020 14:30:11 PDT):

>Or the PII?

[REDACTED] (10/14/2020 14:31:34 PDT):

> [REDACTED] is looking

[REDACTED] (10/14/2020 14:35:49 PDT):

>so sorry - just seeing this. was on another call.

[REDACTED] (10/14/2020 14:35:54 PDT):

>assume this is OBE

[REDACTED] (10/14/2020 14:36:01 PDT):

>but let me know if anything is needed on OCP side

[REDACTED] (10/14/2020 14:38:05 PDT):

>UC has just joined! It is still on right now. Here are the outstanding questions I have (included in the SOT):

>

>What is the approval path for other links that contain the hacked materials?

>Do these apply to ads for PII/?

>Articles that link to hacked material or embedded are enforceable under this decision?

Quote the hacked materials?

[REDACTED] (10/14/2020 14:38:45 PDT):

>i don't understand the frist question

[REDACTED] (10/14/2020 14:39:09 PDT):

>if links include the hacked materials per [REDACTED]'s direction above, would add the interstitial. But should confirm that.

[REDACTED] (10/14/2020 14:39:53 PDT):

>and for the third question, I would say yes to the interstitial for consistency but [REDACTED] can confirm that. Also by enforced - assume you are saying add an interstitial not remove.

[REDACTED] (10/14/2020 14:41:02 PDT):

>Content with the source material or links to the source material will be labeled. Reporting on the existence, including quotes, are allowed and unlabeled.

[REDACTED] (10/14/2020 14:41:19 PDT):

>Ads with PII should be rejected.

[REDACTED] (10/14/2020 14:41:30 PDT):

>I'll ask leadership about ads with the source materials.

[REDACTED] (10/14/2020 14:42:55 PDT):

>the first is if all new links need to be escalated for approval prior to actioning (removal or label), or if guidance is good to push out

[REDACTED] (10/14/2020 14:43:31 PDT):

>Okay, I'll take that to leadership.

[REDACTED] (10/14/2020 14:43:54 PDT):

>Adding [REDACTED] here as well for questions/points related to the interstitial application since she was close to this development in the past with [REDACTED], etc

[REDACTED] (10/14/2020 14:43:58 PDT):

>I think the answer will be the guidance will be universal. If it isn't, I might fall down and die.

[REDACTED] (10/14/2020 14:44:10 PDT):

>preach.

[REDACTED] (10/14/2020 14:47:49 PDT):

>It sounds like Partnerships is still waiting on final approval to do outreach

[REDACTED] (10/14/2020 15:00:07 PDT):

>@ [REDACTED] for the call at 3pm with [REDACTED] and [REDACTED], here are the outstanding questions we have been asked (and you have answered) in case handy

[REDACTED] (10/14/2020 15:00:08 PDT):

shared: 121662635_689773671646517_5207408251684467722_n.png

[REDACTED] (10/14/2020 15:02:00 PDT):

>Partnership is awaiting Comms talking points on demoting, as Partnerships never answered an earlier inquiry from NY Post about why we demoted.

[REDACTED] (10/14/2020 15:02:20 PDT):

>I assume [REDACTED] is in a meeting or still working on this, as she hasn't read my ping yet

[REDACTED] (10/14/2020 15:02:27 PDT):

>Yes, can we please raise? I put this in SRP doc as outstanding question.

[REDACTED] (10/14/2020 15:03:57 PDT):

>@ [REDACTED] I would add to your list: 4. Can we get approval on messaging to use reactively with partners (News Partnerships and US PP who are fielding questions from Congress) on temp demotion. Comms most recently proposed this language: "When we see that a post shows signs of being false, we may temporarily reduce its distribution pending review by a third-party fact-checker. This might be triggered because we see a high number of reports from users, comments expressing disbelief or other signals from experts. The goal is to take action faster before it goes viral and give our fact-checkers time to do their job."

[REDACTED] (10/14/2020 15:04:40 PDT):

>and this is for leadership approval?

[REDACTED] (10/14/2020 15:05:19 PDT):

>Hey guys - qq to confirm and sorry for the basic question

[REDACTED] (10/14/2020 15:05:27 PDT):

>Yes, ideally Comms would first sign off and then we can surface to leadership, as I'm not sure if that's the latest from Comms, but if Comms + other leadership are on call together I would just raise there.

[REDACTED] (10/14/2020 15:05:37 PDT):

> [REDACTED] - think this is for you but if you provided above and I missed someone weigh in

[REDACTED] (10/14/2020 15:05:54 PDT):

>Is the decision that this is a newsworthiness allowance?

[REDACTED] (10/14/2020 15:06:18 PDT):

>Comms needs to bring that to the leadership discussoin. They need to ping [REDACTED]

[REDACTED] (10/14/2020 15:06:23 PDT):

>If so, [REDACTED], [REDACTED], [REDACTED] and I just need to follow up on our side with the documentation etc

[REDACTED] (10/14/2020 15:06:24 PDT):

>Yes.

[REDACTED] (10/14/2020 15:06:29 PDT):

>Super.

[REDACTED] (10/14/2020 15:06:31 PDT):

>Thank you!

[REDACTED] (10/14/2020 15:06:34 PDT):

>Hacked but newsy

[REDACTED] (10/14/2020 15:09:10 PDT):

>I'm super late to the game on this one, but why are we linking to the Community Standards in the label now that we've dropped the language saying that we are allowing for public awareness? People will just see that hacked materials are in violation of our policies....

[REDACTED] (10/14/2020 15:09:39 PDT):

>@ [REDACTED] are you on-call? I just got added to yet another chat about the WH Press Secretary and the email she shared (which I believe form above does not violate because that is in the public sphere already, but want to make sure OCP has eyes and I'm not confusing pieces of content.)

[REDACTED] (10/14/2020 15:09:45 PDT):

>I agree with [REDACTED] that I'm not sure what we are trying to convey here

[REDACTED] (10/14/2020 15:09:52 PDT):

>I am on the call, yes

[REDACTED] (10/14/2020 15:10:27 PDT):

>on call or on the call?

[REDACTED] (10/14/2020 15:12:05 PDT):

>Doesn't violate

[REDACTED] (10/14/2020 15:12:52 PDT):

>Does it have source materials, [REDACTED]?

[REDACTED] (10/14/2020 15:12:59 PDT):

>But, if we start to label, will be labeled.

[REDACTED] (10/14/2020 15:13:47 PDT):

>This is the latest email with hunter's rose rosemont email. So it doesn't violate. But yes looks to be source material

[REDACTED] (10/14/2020 15:14:06 PDT):

>And therefore would be labeled per [REDACTED] above if we label

[REDACTED] (10/14/2020 15:16:35 PDT):

><https://twitter.com/realDonaldTrump/status/1316501350659707456>

[REDACTED] (10/14/2020 15:17:03 PDT):

>I thought we hadn't taken anything down???

[REDACTED] (10/14/2020 15:17:09 PDT):
>we haven't

[REDACTED] (10/14/2020 15:17:32 PDT):
>don't let the truth get in the way of a good soundbite, [REDACTED]

[REDACTED] (10/14/2020 15:22:44 PDT):
>at this point we might as well do it since we're being accused of it ??

[REDACTED] (10/14/2020 15:54:13 PDT):
>Okay - we're not taking any additional action tonight.

[REDACTED] (10/14/2020 15:54:35 PDT):
>If an ad comes in with the source material or a link to the source material, we should reject the ad.

[REDACTED] (10/14/2020 15:55:26 PDT):
>Does this mean we are not removing for PII violation?

[REDACTED] (10/14/2020 15:55:42 PDT):
>If the ad quotes from the source material, do not treat it as the source, treat it as non-violating discussion of the source material.

[REDACTED] (10/14/2020 15:55:49 PDT):
>Correct.

[REDACTED] (10/14/2020 15:56:00 PDT):
>Is the decision for all the source material/content? Or just ads?

[REDACTED] (10/14/2020 15:56:11 PDT):
>Just ads.

[REDACTED] (10/14/2020 15:56:23 PDT):
>We are not doing anything on organic content at this time.

[REDACTED] (10/14/2020 15:56:34 PDT):
>Leadership is meeting again at 9am.

[REDACTED] (10/14/2020 15:56:51 PDT):
>ok, we will start to cascade this to other XFN chat threads

[REDACTED] (10/14/2020 15:57:04 PDT):
>I'm just going to quote this language

[REDACTED] (10/14/2020 15:58:24 PDT):
>@ [REDACTED] do you know if Comms is still planning to work on messaging? I know a lot of the XFN teams have outstanding questions from their partners

[REDACTED] (10/14/2020 15:58:37 PDT):
>I hope so.

[REDACTED] (10/14/2020 15:58:46 PDT):
>They need to go to [REDACTED].

[REDACTED] (10/14/2020 15:58:50 PDT):
>I saw [REDACTED] just confirm they are still working on one of the chats.

[REDACTED] (10/14/2020 16:00:18 PDT):
>And if an ad includes the PII, reject the ad.

[REDACTED] (10/14/2020 16:01:39 PDT):
>So we can/should reject ads like this?

[REDACTED] (10/14/2020 16:02:09 PDT):

shared: 121186603_630021014356002_5002011545448654826_n.jpg

[REDACTED] (10/14/2020 16:02:32 PDT):

[REDACTED] (10/14/2020 16:02:34 PDT):
>Is that the email underneath? If so, yes, reject.

[REDACTED] (10/14/2020 16:02:50 PDT):
>Do we know how many ads we've found?

[REDACTED] (10/14/2020 16:03:19 PDT):
>I don't think we've started proactively looking for them as this was one of the outstanding questions for leadership

[REDACTED] (10/14/2020 16:03:39 PDT):
>[REDACTED] is asking after what the ads rejection tag would be as well

[REDACTED] (10/14/2020 16:03:50 PDT):
>Also what should we reject the ads for?

[REDACTED] (10/14/2020 16:03:58 PDT):
>Also what should we reject the ads for?

[REDACTED] (10/14/2020 16:04:14 PDT):
>The ads violate our privacy community standards for including hacked materials.

[REDACTED] (10/14/2020 16:04:53 PDT):
>I think it's Part II, section II.

[REDACTED] (10/14/2020 16:06:24 PDT):
>It shows up in the IS as 11.1 under "Information obtained from hacked sources"

[REDACTED] (10/14/2020 16:07:09 PDT):
>And we shouldn't proactively search for the ads.

[REDACTED] (10/14/2020 16:11:22 PDT):
>have added guidance to our SOT for tracking:

[REDACTED] (10/14/2020 16:11:22 PDT):

shared: 121605944_1391160639744315_611390396945691113_n.png

[REDACTED] (10/14/2020 16:12:50 PDT):
>Once things (somewhat) settle down, if [REDACTED] [REDACTED] [REDACTED] etc. could take a look at the SOT and make sure it is up to date that would be wonderful:
[REDACTED]

[REDACTED] (10/14/2020 16:13:13 PDT):
>lots of moving pieces on this one, and want to make sure our APAC/EMEA teams have the latest!

[REDACTED] (10/14/2020 16:15:51 PDT):
>this looks up to date from me on the 3PFC side, added one comment

[REDACTED] (10/14/2020 16:18:03 PDT):
>Sounds like pictures allegedly from the laptop are starting to surface. We may have more to do tonight.

[REDACTED] (10/14/2020 16:19:26 PDT):
>The bathtub photos or different ones?

[REDACTED] (10/14/2020 16:24:35 PDT):
>A bathtub one and one with a crack pipe allegedly.

[REDACTED] (10/14/2020 16:24:49 PDT):
><https://www.dailymail.co.uk/news/article-9841255/Man-Hunter-Bidens-emails-Trump-voter-say-told-FBI-came-him.html>

[REDACTED] (10/14/2020 16:25:03 PDT):
>yeah i've seen both of those

[REDACTED] (10/14/2020 16:25:26 PDT):

>right now are we only considering "source material" for the purposes of rejecting ads to be the images of the two emails?

[REDACTED] (10/14/2020 16:25:39 PDT):

>Q: Have we had our AI red team check to see whether these videos look manipulated?

[REDACTED] (10/14/2020 16:25:49 PDT):

>Would be useful to get a signal on that if we haven't.

[REDACTED] (10/14/2020 16:26:17 PDT):

>They are actually in the NY Post story

[REDACTED] (10/14/2020 16:26:22 PDT):

><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-bio-man-to-dad/>

[REDACTED] (10/14/2020 16:27:34 PDT):

>I did not know that.

[REDACTED] (10/14/2020 16:27:46 PDT):

>towards the bottom there's a series of four images

[REDACTED] (10/14/2020 16:28:02 PDT):

>the bathtub one, the crackpipe one, one of hunter smoking a cigarette in bed, and one of him taking a selfie in front of a mirror

[REDACTED] (10/14/2020 16:28:06 PDT):

>they've been in the story since this morning

[REDACTED] (10/14/2020 16:28:32 PDT):

>Right, but I'm not sure whether we've actually assessed to see if we see signs of manipulation.

[REDACTED] (10/14/2020 16:28:48 PDT):

>Either way it would give us valuable context for what to expect next

[REDACTED] (10/14/2020 16:28:52 PDT):

>And photos, fwiw

[REDACTED] (10/14/2020 16:29:06 PDT):

>right -- I meant photos.

[REDACTED] (10/14/2020 16:29:36 PDT):

>i havent seen any video yet (although i've seen allegations that there is video on the hard drive of hunter smoking crack while engaging in a sex act)

[REDACTED] (10/14/2020 16:29:54 PDT):

>nod -- it's photos at this point.

[REDACTED] (10/14/2020 16:30:15 PDT):

>I can ask [REDACTED] to route this, but [REDACTED] are you guys in a place to kick this off?

[REDACTED] (10/14/2020 16:30:32 PDT):

>I don't believe anyone in the misinfo world has looked into this.

[REDACTED] (10/14/2020 16:31:06 PDT):

>I am not personally (bedtime madness) But [REDACTED] and [REDACTED] are here for SRP

[REDACTED] (10/14/2020 16:31:09 PDT):

>hey guys, i have to run and grab my kids before they sell them to the highest bidder. Back in about an hour!

[REDACTED] (10/14/2020 16:31:29 PDT):

>[REDACTED] is on call for us and can assist as needed

[REDACTED] (10/14/2020 16:31:40 PDT):

>[REDACTED] would you guys want to take this? Feels like we should be using all tools to try to get a sense of how legit / illegit this is. Will help inform leadership's decisions tomorrow and how we handle going forward.

[REDACTED] (10/14/2020 16:31:59 PDT):

>But [REDACTED] would be super helpful for [REDACTED] to kick off the right process as we don't know who to send these to for technical evaluation of manipulation

[REDACTED] (10/14/2020 16:32:33 PDT):

>We can start outreach or glad for [REDACTED] to. Our contact will be on Misinfo Product side. Not sure if there are others in TI that [REDACTED] would loop in?

[REDACTED] (10/14/2020 16:32:40 PDT):

>Isn't MMV video?

[REDACTED] (10/14/2020 16:33:07 PDT):

>Yes that policy applies to video only. But we can ask Misinfo Product team if they have classifiers that could try to detect photo manipulation.

[REDACTED] (10/14/2020 16:33:07 PDT):

>I don't know if the AI red team can analyze photos in any structured way, but we've asked them to look before, so I think it's doable in a one-off context.

[REDACTED] (10/14/2020 16:33:11 PDT):

>I don't know if they do.

[REDACTED] (10/14/2020 16:33:33 PDT):

>ok. I'll kick a thread off to ask. This could also get tasked up in the am tomorrow.

[REDACTED] (10/14/2020 16:33:38 PDT):

>Ok. So I'd say SRP isn't the right team on this then

[REDACTED] (10/14/2020 16:33:49 PDT):

>I'll include you [REDACTED].

[REDACTED] (10/14/2020 16:33:52 PDT):

>Anyone else want to be on?

[REDACTED] (10/14/2020 16:34:31 PDT):

>me (he says reluctantly) :)

[REDACTED] (10/14/2020 16:34:53 PDT):

>"want"

[REDACTED] (10/14/2020 16:34:54 PDT):

>Happy to join the chat

[REDACTED] (10/14/2020 16:35:09 PDT):

>if we find a manipulated image, what policy would apply?

[REDACTED] (10/14/2020 16:35:12 PDT):

>i do not think misinfo product has classifiers to detect manipulated photos, but it's worth asking. they detect false photos based on comparison to known manipulated photos, not based on signs of manipulation in the abstract

[REDACTED] (10/14/2020 16:35:51 PDT):

>if we find a manipulated image, we would enqueue with demotion as we have already, but i'd think we could also tell 3PFCs we found evidence of that and see if they can validate it. we've never done that...but i don't see why not

[REDACTED] (10/14/2020 16:37:20 PDT):

>yeah - pictures were also in the dailymail articles this morning

[REDACTED] (10/14/2020 16:39:19 PDT):

>On this... I added to SRP SGT doc: Do not enqueue or demote any further content making claims related to this story. If we become aware of new signals of falsity, please escalate to Content Policy leadership.

[REDACTED] (10/14/2020 16:39:32 PDT):

>Given sensitivity, I'd suggest we clear with this group before demoting any content based on manipulation signals.

[REDACTED] (10/14/2020 16:39:57 PDT):

>Even though it's our policy to demote if we see evidence of manipulation, just seems we should play it safe since leadership said don't demote any more of this.

[REDACTED] (10/14/2020 16:45:54 PDT):

>@ [REDACTED] one question from BI-esc I wanted to make sure you're aligned on...They are asking whether we should enforce at the ad level or the component level? If we enforce at the component level, other ads/advertisers that use the exact tagged/rejected component will also get their ads taken down (so closer to proactive detection and automated action for new ads).

>However, ad level enforcement seems much more aligned with the decision above as it's on an ad by ad basis and much more reactive.

[REDACTED] (10/14/2020 16:46:53 PDT):

> [REDACTED] /myself think we should go with ad level as to avoid enforcement that goes out and automatically finds other ads.

[REDACTED] (10/14/2020 16:54:02 PDT):

>considering the guidance not to do any proactive sweeps above

[REDACTED] (10/14/2020 16:54:28 PDT):

>Twitter's policy explanation for their enforcement: <https://twitter.com/TwitterSafety/status/1316525303930458115?s=20>

[REDACTED] (10/14/2020 16:57:43 PDT):

>Ad level for now.

[REDACTED] (10/14/2020 17:05:16 PDT):

>Not assuming any policy applies at this point -- mainly just trying to inform leadership's analysis of how sketchy this is and how future analysis is likely to break.

[REDACTED] (10/14/2020 17:06:32 PDT):

>Manipulated image would be for fact checkers to rate as altered (depending on the manipulation). I don't think a manipulated media violates anything on its face.

[REDACTED] (10/14/2020 17:09:06 PDT):

>Agree. Evidence that the images were manipulated could inform our assessment of how the public will react and whether we'll see additional debunking stories.

[REDACTED] (10/14/2020 17:15:38 PDT):

>Okay - leadership wants to stay the course overnight.

[REDACTED] (10/14/2020 17:16:25 PDT):

>Right -- analyzing the photos is just to see if we can get more signal for leadership for their discussion in the am.

[REDACTED] (10/14/2020 17:16:31 PDT):

>no suggestion we should take action ahead of that.

[REDACTED] (10/14/2020 17:18:30 PDT):

>But can I ask APAC and then EMEA to work with Ops to see what's out there in terms of these images and whether they're being posted by publications in the NPI and/or by other users? If we are able to identify the scale of posts containing these images, that would be really helpful.

[REDACTED] (10/14/2020 17:19:37 PDT):

>the thought here is that they are hacked and not newsworthy as they are private images of the adult child of a candidate so we would remove under our hack policy, but it would be helpful to know the scope and if we can informally gauge whether news entities think the images are newsworthy.

[REDACTED] (10/14/2020 17:28:17 PDT):

[REDACTED] (10/14/2020 17:29:21 PDT):

><https://www.washingtonpost.com/politics/2020/10/14/hunter-bidens-alleged-laptop-an-explainer/>

[REDACTED] (10/14/2020 17:29:59 PDT):

>Basically says none of the NY post story has been verified and that VP Biden and Hunter both deny

[REDACTED] (10/14/2020 17:32:36 PDT):

>What specifically are they denying?

[REDACTED] (10/14/2020 17:33:03 PDT):

>That laptop was Hunter Biden's? That the emails are from him? Or the underlying allegations?

[REDACTED] (10/14/2020 17:33:26 PDT):

>Andrew Bates, a Biden campaign spokesman, said a review of Biden's schedules from 2015 finds no record of any such meeting. Officials who worked for Biden at the time told The Fact Checker that no such meeting took place.?">"I was with the vice president in all of his meetings on Ukraine," said Michael Carpenter, Biden's foreign policy advisor in 2015. "He never met with this guy. In fact I had never heard of this guy until the New York Post story broke."

[REDACTED] (10/14/2020 17:33:37 PDT):

>More detail in the article

[REDACTED] (10/14/2020 17:34:03 PDT):

>Asked to verify whether the email is genuine, Hunter Biden's attorney George Mesires told The Fact Checker: "We have no idea where this came from, and certainly cannot credit anything that Rudy Giuliani provided to the NY Post, but what I do know for certain is that this purported meeting never happened."

[REDACTED] (10/14/2020 17:34:23 PDT):

>Interesting,

[REDACTED] (10/14/2020 17:37:13 PDT):

>Also from the article

[REDACTED] (10/14/2020 17:37:16 PDT):

>The New York Post article also cites an email from Pocharskyi to Hunter Biden saying he was "going to share this information with the US embassy here in Kyiv, as well as the office of Mr Amos Hochstein in the States."?">"I know for a fact he never contacted me or my office," said Hochstein, who at the time worked closely with Biden as Special Envoy and Coordinator for International Energy Affairs. "I provided every record to the Senate investigation and no mention of this guy was ever made, no emails, no correspondence. I know almost every player in the energy sector in Ukraine. I never met this guy."?">Carpenter said that the vice president wouldn't have had a meeting with a company executive. "He was the vice president of the United States," he said. "He met with prime ministers."

[REDACTED] (10/14/2020 17:50:04 PDT):

>[REDACTED] you're asking for the prevalence of the four images of hunter right?

[REDACTED] (10/14/2020 17:50:21 PDT):

>Yep.

[REDACTED] (10/14/2020 17:53:52 PDT):

>Ops is asking the proactive pod how to determine prevalence on those images - do we have any on plat content with the images yet that we are aware of?

[REDACTED] (10/14/2020 17:54:44 PDT):

>i'm only aware of the URLs with the images embedded

[REDACTED] (10/14/2020 17:57:12 PDT):

>That's really good news actually.

[REDACTED] (10/14/2020 18:00:59 PDT):

>+ [REDACTED], next OCP on call

Final Report 1072

[REDACTED] (10/14/2020 19:01:40 PDT):

[REDACTED] what about NPI publishers that post articles that contain links back to the NY Post story with the images?

[REDACTED] (10/14/2020 18:04:04 PDT):

><https://www.facebook.com/Breitbart/posts/10166339582620354>

[REDACTED] (10/14/2020 18:19:39 PDT):

>It's like some sort of MC Escher disinformation hellscape.

[REDACTED] (10/14/2020 18:19:52 PDT):

>Honestly - whatever is easy for people to categorize. I'm not trying to create huge amounts of work - just trying to get a sense of what we're seeing. If it's something we can easily detect, then by all means. But if it requires jumping through kooky hoops, not worth it.

[REDACTED] (10/14/2020 18:20:53 PDT):

[REDACTED] due to the fact that these ads would be removed as Privacy violations under IS, these would be removed from the Ad Library altogether instead of receiving the normal overlay for less egregious violations. This proposal was approved in March under Option 1 here [REDACTED]

>

>Before we proceed, I wanted to make sure we're ok to apply this protocol and remove these ads from the Library?

[REDACTED] (10/14/2020 18:21:02 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 18:21:32 PDT):

>Interesting.

[REDACTED] (10/14/2020 18:21:43 PDT):

>Sorry, the thumb got away from me.

[REDACTED] (10/14/2020 18:21:56 PDT):

>Did we ever end up with a "trace" for this situation?

[REDACTED] (10/14/2020 18:22:22 PDT):

>We were going to try to leave a record of the ad while still removing the content, but I can't remember if it happened.

[REDACTED] (10/14/2020 18:23:16 PDT):

>I believe trace work was de-pried due to COVID, but good callout. Lemme check status.

[REDACTED] (10/14/2020 18:24:59 PDT):

>If we don't have the trace, I think that, if it's possible, we should probably just do the overlay. They're as core political ads as you can get and the content isn't overtly harmful so it feels weird to remove all signs of the ad.

[REDACTED] (10/14/2020 18:25:12 PDT):

>Especially since we aren't removing in organic.

[REDACTED] (10/14/2020 18:25:56 PDT):

>that makes sense to me, and the overlay is the default for when these are disapproved, so this will happen. I'll chase the trace!

[REDACTED] (10/14/2020 18:29:50 PDT):

>Terrific, thanks. Very good call out.

[REDACTED] (10/14/2020 18:33:56 PDT):

>Well. I've found at least one copy. From my own newsfeed. With [REDACTED] tagged in it ??

[REDACTED] (10/14/2020 18:34:05 PDT):

shared: 121574359_403213744400511_7118563285716987168_n.jpg

[REDACTED] (10/14/2020 18:34:35 PDT):
>Everyone needs to be very nice to [REDACTED]

[REDACTED] (10/14/2020 18:34:46 PDT):
>Agreed.

[REDACTED] (10/14/2020 18:34:55 PDT):
>Yeah, this is exactly what we need to know if it's floating around.

[REDACTED] (10/14/2020 18:35:18 PDT):
>Maybe they can just track where [REDACTED] is being tagged.

[REDACTED] (10/14/2020 18:35:51 PDT):
>Yeah. Poor
>[REDACTED]

[REDACTED] (10/14/2020 19:10:26 PDT):
>[REDACTED] - where Ops is collecting info on posts of the personal hunter Biden photos, including VPVs and who posted

[REDACTED] (10/14/2020 19:10:45 PDT):
>working doc here: [http://\[REDACTED\]](http://[REDACTED])

Exhibit 10

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 7/15/2020 12:17:20 PM
To: [REDACTED] [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbId": [REDACTED], "threadFbId": null}]
Attachments: 51969112_646151632471827_5287496115975880704_n.gif;
 51969112_646151632471827_5287496115975880704_n.gif;
 51969112_646151632471827_5287496115975880704_n.gif

[REDACTED] (7/15/2020 11:57:20 PDT):
 >how is the meeting going? riveting?

[REDACTED] (7/15/2020 12:14:42 PDT):
 >Fine but plagued with some tech issues

[REDACTED] (7/15/2020 12:14:53 PDT):
 >Nothing relevant for us yet

[REDACTED] (7/15/2020 12:15:44 PDT):
 >its a really dry meeting

[REDACTED] (7/15/2020 12:16:00 PDT):
 shared: 51969112_646151632471827_5287496115975880704_n.gif

[REDACTED] (7/15/2020 12:16:03 PDT):
 shared: 51969112_646151632471827_5287496115975880704_n.gif

[REDACTED] (7/15/2020 12:16:04 PDT):
 shared: 51969112_646151632471827_5287496115975880704_n.gif

[REDACTED] (7/15/2020 12:16:04 PDT):
 >of course, wouldn't expect anything less from USG!!!

[REDACTED] (7/15/2020 12:16:05 PDT):
 >hahaha

[REDACTED] (7/15/2020 12:16:20 PDT):
 >The slide deck is decent but REALLY dense

[REDACTED] (7/15/2020 12:16:30 PDT):
 >yeah, it's almost too high level.

[REDACTED] (7/15/2020 12:16:34 PDT):
 >Yeah

[REDACTED] (7/15/2020 12:17:05 PDT):
 >But, when we get hauled up to the hill to testify on why we influenced the 2020 elections we can say we have been meeting for YEARS with USG to plan for it.

[REDACTED] (7/15/2020 12:17:07 PDT):
 >We were just encouraged to read some academic studies on vote shifting after election day, before results are announced

[REDACTED] (7/15/2020 12:17:20 PDT):
 >Soooo if you need me, I'll be at my college library

Exhibit 11

"For several years, tech companies have worked together, and with U.S. government agencies tasked with protecting the integrity of elections, to counter election threats across our respective platforms. As we approach the November election, we continue to prepare, meet regularly, and share updates on the threats we see. At today's meeting, we specifically discussed:

1. Ways to help provide real-time, clear information about the voting process and election results given expected logistical disruptions posed by COVID-19.
2. Ways to counter targeted attempts to undermine the election conversation before, during, and after the election. This includes preparing for possible so-called "hack and leak" operations attempting to use platforms and traditional media to amplify unauthorized information drops.
3. Detection efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.

As the global pandemic poses unprecedented challenges for the 2020 U.S. election, we will continue this ongoing communication and close work between industry and U.S. institutions tasked with election security to share key findings and operational insights in the weeks to come."

FACEBOOK

Go g^oe reddit Microsoftverizon
media PinterestLinked  WIKIMEDIA
FOUNDATION

Exhibit 12

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]>
To: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Sent: 8/5/2020 9:12:03 PM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]
Attachments: sticker.png

[REDACTED] (8/05/2020 07:47:08 PDT):
 ><https://newsroom.tiktok.com/en-us/combating-misinformation-and-election-interference-on-tiktok>

[REDACTED] (8/05/2020 07:47:32 PDT):
 >Countering foreign interference
 >
 >In 2018, the Department of Homeland Security (DHS) established the Countering Foreign Influence Task Force (CFITF) as part of the National Risk Management Center within the Cyber and Infrastructure Security Agency. We're proud to work with the CFITF to help stop the threat and dangers of foreign influence on elections. In addition to sharing insight about possible disinformation campaigns across the industry, the task force connects local election officials with online platforms and law enforcement so that we can help protect the integrity of the vote.
 >
 >We're also working with a number of industry-leading threat assessment platforms to bolster our ability to detect inauthentic activity and improve our safeguards against it.

[REDACTED] (8/05/2020 07:48:04 PDT):
 >have they ever joined industry/gov mtgs?

[REDACTED] (8/05/2020 07:48:48 PDT):
 >they haven't

[REDACTED] (8/05/2020 07:48:56 PDT):
 >I don't think they've actually asked

[REDACTED] (8/05/2020 07:49:03 PDT):
 >Although I could see that coming up.

[REDACTED] (8/05/2020 07:49:14 PDT):
 >Probably worth having the group start to think about it for our meeting this week

[REDACTED] (8/05/2020 07:49:17 PDT):
 >For next week, can you all take a look at this doc and comment: <https://fb.quip.com/iajbAzMI1vc4>

[REDACTED] (8/05/2020 07:49:35 PDT):
 >if MSFT buys them, they'll be repped:)

[REDACTED] (8/05/2020 07:49:59 PDT):
 >And then we discuss before our meeting tomorrow? Was about to make the MSFT joke, but [REDACTED] got there first. :-)

[REDACTED] (8/05/2020 07:50:12 PDT):
 >EDITORIAL: President Trump wants to undermine the election. Here's one way to stop him., Washington Post
 >
 >"...Mr. Trump has no rational basis for his claims. Voting by mail presents logistical and administrative challenges, but it has been proved safe in blue states and red states alike. Yet this coronavirus-inflected election will feel different from what many Americans are used to, and Mr. Trump will exploit that reality to sow doubt about the results – for his own benefit, even if it corrodes faith in U.S. democracy."
 >
 >"The best antidote is for states to prepare now, both for increased mail-in voting and for safe in-person voting; and for Congress to give them the funds to do so, which so far Republicans are resisting."

[REDACTED] (8/05/2020 07:50:26 PDT):

>Also, FYSA from WaPo this a.m.

[REDACTED] (8/05/2020 07:50:30 PDT):

>We should go back to twitter and google with our proposal

[REDACTED] (8/05/2020 07:53:59 PDT):

>By EOD today before tomorrow's industry sync to prepare for next week?

[REDACTED] (8/05/2020 07:54:20 PDT):

>yep

[REDACTED] (8/05/2020 08:00:09 PDT):

>Got it, defer to [REDACTED] and others, but main points highlighted on risks are there, including mail in ballot uncertainty. On naming companies, would maybe remove Reddit as they have not been steady participants and would need to get their buy in first? MSFT would presumably want to be included but haven't been part of this aside from a sync a few weeks ago, we would need to confirm with them, especially given current environment and their news presence? If others have any inputs by mid day EST today, maybe you could share with Google and Twitter and we would have signal on what they would want before tomorrow's prep meeting and then could engage the other companies or let them know this was coming? Defer to everyone, but my two cents, and thank you for the opportunity to engage.

[REDACTED] (8/05/2020 08:01:19 PDT):

>Can we raise the comms plan with the industry group this week?

[REDACTED] (8/05/2020 08:01:32 PDT):

>Agree with [REDACTED] -- I think if we want to do a release around the next meeting, we need to tell all the partners

[REDACTED] (8/05/2020 08:01:46 PDT):

>we'd want T and G be ok with that, but yeah dont see why not

[REDACTED] (8/05/2020 08:02:55 PDT):

>Can you circle with your comms colleagues and make sure they're comfortable with talking about it?

[REDACTED] (8/05/2020 08:03:03 PDT):

>The industry pre-meet is tomorrow, and that'll be our best chance to raise

[REDACTED] (8/05/2020 08:03:30 PDT):

>yep, once we have a proposal to go back with

[REDACTED] (8/05/2020 08:03:31 PDT):

[REDACTED] (and anyone else), would this be OK for [REDACTED] to share back the draft while circling up?

[REDACTED] (8/05/2020 08:03:36 PDT):

>i hope to do that mid day today

[REDACTED] (8/05/2020 08:04:21 PDT):

[REDACTED], would be good to get your quick gut check on what's included now and whether any of it would raise red flags with Twitter, Google

[REDACTED] (8/05/2020 08:09:03 PDT):

>Also flagging that if we mention the USG agency level engagement by Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the FBI's Foreign Influence Task Force, DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI), will maybe need to clear with their Comms teams (defer to [REDACTED] and [REDACTED] there).

[REDACTED] (8/05/2020 08:14:52 PDT):

>Generally looks good

[REDACTED] (8/05/2020 08:14:53 PDT):

>thoughts:

[REDACTED] (8/05/2020 08:15:04 PDT):

>(1) if we talk about USG partners we should reference CISA as opposed to DHS

[REDACTED] (8/05/2020 08:15:41 PDT):

>(2) Can we reserve ability to add an extra clause or two about what we talk about? For example, we could mention that we're discussing the upcoming conventions and any risks they could pose, or something similar (or will that generate too much churn)

[REDACTED] (8/05/2020 08:16:15 PDT):

>We kinda need this to make it slightly interesting

[REDACTED] (8/05/2020 08:16:39 PDT):

>(3) I'd add into the first sentence that we've not just been working "across platforms" but also with USG. Don't want this to come across as if this is the first time we're talking to USG. Probably worth emphasizing that we've been meeting regularly w/USG for months/years or something similar

[REDACTED] (8/05/2020 08:17:28 PDT):

>Agree -- it will be tricky, but I think we at least need a sentence on the trends we shared or some insight from it.

[REDACTED] (8/05/2020 08:17:59 PDT):

>Maybe mention hack/leak and increased risk of activity around major events like the conventions?

[REDACTED] (8/05/2020 08:18:34 PDT):

>Agree and this will be known from the press coverage around the July 2018 and September 2019 meetings.

[REDACTED] (8/05/2020 08:18:39 PDT):

>great feedback, we'll incorporate! is there an agenda for the mtg we can draw from?

[REDACTED] (8/05/2020 08:18:49 PDT):

>Yeah. We can find some vanilla-ish stuff. Conventions is a good example. Like, of course we are going to be thinking about these things. No brained. But gives a bit more specificity. Same w hack/leak as it's been in news recently.

[REDACTED] (8/05/2020 08:19:16 PDT):

>(4) What about adding a sentence about how it's clear that FBI/CISA and Industry partners are all taking this seriously and have tools in place to ensure the protection and legitimacy of the election?

[REDACTED] (8/05/2020 08:19:38 PDT):

>I'm looking for some way to put out a plug that this election is legitimate and trustworthy

[REDACTED] (8/05/2020 08:20:12 PDT):

>to counter fears that it will be "hacked" and limit the ability for anyone to claim it was illegitimate...

[REDACTED] (8/05/2020 08:20:38 PDT):

>Not yet, but we're working on it! (Aim is to finalize that with industry tomorrow)

[REDACTED] (8/05/2020 08:20:44 PDT):

>But assume that the conventions will be a prominent topic

[REDACTED] (8/05/2020 08:20:48 PDT):

>On agenda, the points [REDACTED] is going over now go to the agenda -- there is a standing threat trends discussion and various deep dives, like on mail in ballots or state actor efforts, with mention of domestic activity of late.

[REDACTED] (8/05/2020 09:04:37 PDT):

>how do we all feel now about leaning in too heavy into USG/Industry collaboration? i feel like it could backfire

[REDACTED] (8/05/2020 09:05:03 PDT):

>hence the 1st sentence is about industry and then we go into USG mtgs

[REDACTED] (8/05/2020 09:09:35 PDT):
>I agree it is a delicate balance.

[REDACTED] (8/05/2020 09:09:42 PDT):
>That's partly why we should talk about CISA and not DHS

[REDACTED] (8/05/2020 09:10:49 PDT):
>I'd honestly be interested even in just starting with a statement from the companies on the work we're doing together that eschewed our USG engagement completely -- but my sense from you and @ [REDACTED] is that we need a hook to these meetings for it to be relevant/make sense.

[REDACTED] (8/05/2020 09:11:36 PDT):
>we need it in there because Google wanted USG but we both started with industry only and then added USG in the 2nd sentence

[REDACTED] (8/05/2020 09:14:36 PDT):
shared: sticker.png

[REDACTED] (8/05/2020 09:25:22 PDT):
>pls take a look at the current version, will be copy/pasting to the shared google doc for Twitter/Google's feedback at 10am

[REDACTED] (8/05/2020 09:25:59 PDT):
>the point about years of collaboration w USG is in background

[REDACTED] (8/05/2020 09:33:48 PDT):
>added some edits!

[REDACTED] (8/05/2020 09:41:38 PDT):
>responded! thank you! [REDACTED] - are there points in the trends section that we dont need or you think industry wont be cofortable with?

[REDACTED] (8/05/2020 09:41:42 PDT):
>comfortable*

[REDACTED] (8/05/2020 09:42:09 PDT):
>we dont need them all in here, if not helpful

[REDACTED] (8/05/2020 09:43:22 PDT):
>I'd probably cut it to 3, just for consummabilty

[REDACTED] (8/05/2020 09:44:04 PDT):
>which ones would you reommend cutting

[REDACTED] (8/05/2020 09:44:48 PDT):
>(1) blurs the line into content a bit; (2) I like the most but I suspect could generate tricky questions (I'd keep it and see what industry says); (3) is a bit hard to understand so I'd probably cut it; (5) is super safe, but not that interesting, so trade that off against some of the more interesting but tricky ones.

[REDACTED] (8/05/2020 09:46:41 PDT):
> [REDACTED] can you take a look before i share w google and twitter?

[REDACTED] (8/05/2020 09:50:26 PDT):
>I think it's in a decent place to share. Thx [REDACTED].

[REDACTED] (8/05/2020 10:32:55 PDT):
>Twitter's in the doc, editing, so things are moving:)

[REDACTED] (8/05/2020 10:33:30 PDT):
>Are we OK to share tomorrow even if edits are ongoing, or should we just sit tight and see where we are mid-day tomorrow? Meetings are late afternoon timeframe.

[REDACTED] (8/05/2020 10:34:19 PDT):
>lets see how it goes there, you guys are probably in the best position to judge?

[REDACTED] (8/05/2020 10:38:55 PDT):

>so you all are tracking: [REDACTED]

Final Report 1083

[REDACTED] (8/05/2020 10:42:29 PDT):

>Thank you so much -- good call -- just requested access.

[REDACTED] (8/05/2020 10:43:10 PDT):

>just added

[REDACTED] (8/05/2020 10:43:37 PDT):

>we should plan to share tomorrow regardless -- we'll need everyone bought in to do this.

[REDACTED] (8/05/2020 10:45:52 PDT):

>FYSA on the Google election security/account security roundtable right now, there is discussion about whether there would be a desire for coordination among the platforms (who are all engaged here) in publicizing account security best practices as part of election security efforts -- sharing in case that is something we would want to amplify

[REDACTED] (8/05/2020 14:17:18 PDT):

>Was just in the document and the Google and Twitter edits are very positive -- [REDACTED] will you share back if [REDACTED] and Yoel give signal about tomorrow re the Comms piece?

[REDACTED] (8/05/2020 14:28:20 PDT):

[REDACTED], in the doc, it has a table for "Company Approvers" -- do you know who that would be for each company?

[REDACTED] (8/05/2020 14:29:15 PDT):

>likely comms and policy for each + legal

[REDACTED] (8/05/2020 14:31:12 PDT):

>working on it

[REDACTED] (8/05/2020 14:31:28 PDT):

> [REDACTED] first suggestion was just to leave it to the comms teams, so I'm explaining to him this is about bringing the other companies in/up to speed :)

[REDACTED] (8/05/2020 14:55:26 PDT):

>Google castrated the statement and background quite a bit, not sure i'm a fan. [REDACTED] - any insights as to why?

[REDACTED] (8/05/2020 14:56:14 PDT):

>i'll try calling [REDACTED] today to see where her head is

[REDACTED] (8/05/2020 14:58:09 PDT):

>Saw [REDACTED] was in there after I wrote the above and hacking away -- the Twitter edits were good.

[REDACTED] (8/05/2020 14:58:41 PDT):

>yeah Twitter's edits were good, i wish she left them alone:)

[REDACTED] (8/05/2020 14:59:21 PDT):

>Wow -- just went in again. Google eviscerated this.

[REDACTED] (8/05/2020 14:59:30 PDT):

>yup

[REDACTED] (8/05/2020 14:59:58 PDT):

>This is why we can't have nice things

[REDACTED] (8/05/2020 14:59:59 PDT):

>Can they do that if Twitter and Facebook are supportive? I can understand some of those edits, but not all?

[REDACTED] (8/05/2020 15:01:06 PDT):

>Google just emailed: "Thanks [REDACTED] and [REDACTED]! At the risk of proliferating the number of versions, I've added a V3 (marries V1 with some of the added details in V2). Also, I like

the idea of being able to give a bit of additional background, but suggest we stick to the facts of when the working group started and who was at the meeting. I think the other points are basically made in the statement. What do you all think? Seems that if we want to have this ready to go on Wednesday, and we still need to get it to the right USG folks to take a look, we should have this locked down on our side by tomorrow morning."

[REDACTED] (8/05/2020 15:02:00 PDT):

>We don't need to have this locked down by tomorrow? That is false urgency.

[REDACTED] (8/05/2020 15:04:46 PDT):

>Why can't the facts also include the threat trends and efforts there? This version is skeletal and unhelpful and not receptive to Facebook's and Twitter's very substantive and solid inputs.

[REDACTED] (8/05/2020 21:12:03 PDT):

>spoke w Google, a few things:

>

>* their edits are mainly driven by the fact that if we say too much about non-USG mtg related stuff their chances of getting it thru the approval process are much slimmer

>

>* [REDACTED] heard us about the importance to share a bit more on the substance and trends.

>

>* She'll go back to her team to see if she can make a case for some of the points we proposed.

>

>* if not, Google would be fine with us and Twitter sharing things separately with press about our respective efforts against IO.

>

>* Google will come back first thing tomorrow with proposed language for us and Twitter to consider. It wont be LESS, but likely more that what they currently have

>

>* For tomorrow, Google comms wants to make sure we position this as: here is what F, G, T will share -- pls let us know if you want to join (so we dont have to be stuck waiting for other companies' approvals)

Produced to HJC

Exhibit 13

Produced to HJC

Exhibit 14

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 10/13/2020 4:57:31 PM
To: Joel Kaplan [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbId": [REDACTED], "threadFbId": null}]
Attachments: sticker.png

Joel D. Kaplan (10/13/2020 10:37:55 PDT):

>Can you remind me of the details of the "perception hack" Pre 2018 that Sheryl keeps talking about?

[REDACTED] (10/13/2020 10:40:05 PDT):

>Yeah. I've actually got my team writing them up to send to leadership.

[REDACTED] (10/13/2020 10:40:09 PDT):

>So you have them in detail.

[REDACTED] (10/13/2020 10:40:17 PDT):

>Can I send that around later today, or do you need them right this instance?

[REDACTED] (10/13/2020 10:40:19 PDT):

>instant?

Joel D. Kaplan (10/13/2020 10:41:33 PDT):

>If you could shoot me the bare bones in next 30 that would be helpful

Joel D. Kaplan (10/13/2020 10:41:39 PDT):

>Just a couple sentences

[REDACTED] (10/13/2020 10:41:58 PDT):

>yep -- stand by!

Joel D. Kaplan (10/13/2020 10:55:27 PDT):

>Can you also let me know what we are doing to prepare for "late attempts at foreign interference"? (This is on a slide nick is using to brief the BoD)

[REDACTED] (10/13/2020 10:57:50 PDT):

>(1) We have teams proactively hunting for operations like this, and close partnerships with the FBI who have been giving us rapid access to tips to we can stop these operations -- including some of the Russian ops we took down just a couple weeks ago.

[REDACTED] (10/13/2020 10:58:16 PDT):

>(2) We have a rapid response team set up in our elections operations center, so we can observe new threats as they emerge and handle them very quickly.

[REDACTED] (10/13/2020 10:59:04 PDT):

>(3) We have combined our own scaled detection with close partnerships with civil society groups, state elections officials, our industry partners, and the federal government, so we catch these things early and quickly.

[REDACTED] (10/13/2020 11:00:10 PDT):

>And (if you want) (4) We've been running red team exercises to prepare for 2020 since early 2019, so we're in a good place to see and stay ahead of how these threat actors evolve.

[REDACTED] (10/13/2020 11:03:26 PDT):

>Here is the overview of the midterms story:

[REDACTED] (10/13/2020 11:03:28 PDT):

><https://fb.quip.com/AIa/A12CptWu>

[REDACTED] (10/13/2020 11:03:29 PDT):

>Does that do what you need?

[REDACTED] (10/13/2020 11:03:36 PDT):

>Can shorten further if you want

Joel D. Kaplan (10/13/2020 11:06:12 PDT):

shared: sticker.png

[REDACTED] (10/13/2020 11:06:12 PDT):
>Also dropped here:

[REDACTED] (10/13/2020 11:06:13 PDT):
>Midterms Story

>
>Two days before the US midterm elections in 2018, a group claiming to be the Internet Research Agency, a Russia-based troll farm, launched an off-platform website called "the IRA in the USA" where they claimed to have a large presence on social media that they would use to control the outcome of the midterms. They publicly shared a list of Instagram accounts to support their allegations. There was no evidence of such a widespread operation, and these accounts had been created only weeks before. In addition to creating the website, IRA-linked actors separately reached out to prominent security journalists, peddling a story about a supposed "second troll farm" operating from St. Petersburg and targeting US public debate in the lead-up to the elections.

>
>This is a classic example of a perception hack. Rather than running a large IO campaign, they tried to create the impression of such a campaign built off a tiny seed of truth and relied on the expectation of widespread manipulation to lend credibility to their claims.

>
>This operation ultimately had little impact for two reasons. First, the reporters that the Russians approached checked other sources, and concluded there was no evidence of a second troll farm. When they ultimately did write a story, it was about how Russian actors attempted to trick them by peddling a false story. Second, based on initial information from the FBI and a rapid investigation by our IO investigative team, we had already identified and publicly removed almost all of the FB and IG accounts that they referenced (<https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/> (https://l.workplace.com/l.php?u=https%3A%2F%2Fnewsroom.fb.com%2Fnews%2F2018%2F11%2Flast-weeks-takedowns%2F&h=AT202CC1eE9_gRwXJwM_4idR-x6asu1TgKzm-CTabWjRT1Td-nCSZB_MJy4IPmMzKx-zwzjMgGs56-0bgs-oCbOY4wIjHieIP9g9FeFuPVXIORdmwSkXBURsh_7wPPB2seeuh0SMjj8L9dbQnc7UOg)). We were able to be clear that there was no evidence of a larger operation, and our partners in government and civil society sent the same message. This undermined Russian efforts at manipulation and stopped them from having significant impact.

[REDACTED] (10/13/2020 11:08:00 PDT):
>Let me know if you need anything else!

Joel D. Kaplan (10/13/2020 11:51:54 PDT):
>Have we seen any down ballot foreign interference?

[REDACTED] (10/13/2020 11:53:49 PDT):
>You mean directly engaging with more local races?

[REDACTED] (10/13/2020 11:53:52 PDT):
>Not in any sustained way.

[REDACTED] (10/13/2020 11:54:04 PDT):
>It's worth noting that the network we took down linked to Roger Stone

Joel D. Kaplan (10/13/2020 11:54:04 PDT):
>Yes. Content related to senate, house, state races

[REDACTED] (10/13/2020 11:54:11 PDT):
>did use IO techniques around local florida candidates

[REDACTED] (10/13/2020 11:54:23 PDT):
>but that is obv not foreign interference.

[REDACTED] (10/13/2020 11:54:49 PDT):
>People overestimate how precisely targeted these foreign campaigns are.

[REDACTED] (10/13/2020 11:54:59 PDT):
>They rarely have the incentive or capacity to narrowly target a specific local race.

[REDACTED] (10/13/2020 11:55:24 PDT):
>domestic actors often target local races (we've seen it in Australia, Spain, Romania, here in the US), but foreign actors are higher level.

[REDACTED] (10/13/2020 16:55:52 PDT):

>Just wanted to make sure you saw the email from [REDACTED] today about IB enforcements and the uptick we've seen in inauthentic behavior. This is *NOT* about CIB, but rather an increase we've seen recently in largely financially-motivated efforts, by both foreign and domestic actors.

[REDACTED] (10/13/2020 16:56:21 PDT):
>we've been delivering warnings, and the remediation for almost all the Pages will only be soft actions (a few are getting removed).

[REDACTED] (10/13/2020 16:56:47 PDT):
>I don't anticipate this sparking any huge alarm bells, but I know you've been keeping an eye on our domestic IB work, so wanted to make sure you saw this one.

Joel D. Kaplan (10/13/2020 16:57:12 PDT):
[REDACTED] who?

[REDACTED] (10/13/2020 16:57:18 PDT):
>sorry -- [REDACTED]

[REDACTED] (10/13/2020 16:57:20 PDT):
>on my team.

[REDACTED] (10/13/2020 16:57:31 PDT):
>I forget sometimes that there is another, slightly more prominent [REDACTED] at this company.

Produced to HJC

Exhibit 15

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 1/6/2020 8:25:08 PM
To: [REDACTED]@google.com]; [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CB) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF)(FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CRM) [REDACTED]@usdoj.gov; [REDACTED] (AJ) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED]@google.com] [REDACTED]@google.com]
Subject: FITF Meeting with Google
Location: 1001 North Shoreline Blvd, Mountain View
Start: 2/10/2020 11:00:00 PM
End: 2/11/2020 12:30:00 AM
Show Time As: Tentative

Recurrence: (none)

Tentative agenda: (1) IRA update, and (2) DOJ discussion of election crimes

From: [REDACTED]@google.com]
Sent: Monday, January 06, 2020 12:15 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] ([REDACTED]@google.com) <[REDACTED]@google.com>
Subject: Re: Next FITF Meeting

Hi Elvis,

I hope you enjoyed the holidays. Either time on February 10 works for us. As we have done for the past meetings, we're happy to host. Thank you.

On Fri, Jan 3, 2020 at 3:45 PM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Hi [REDACTED],

Happy New Year! I know you and [REDACTED] may have some conflicts, but we wanted to gauge your team's availability to meet with FITF next month. Here are the open dates/times:

February 10, 1 PM, 3 PM
 February 14, 10 AM, 1 PM

The tentative agenda will include discussion of election related crimes with DOD and an IRA update. Hope all is well.

Regards,
 Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security Cyber
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Confidential - Not For Public Release

Exhibit 16

Thanks!

Regards,
Elvis

Final Report 1097

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division
Federal Bureau of Investigation
W: [REDACTED]
C: [REDACTED]

From: Chan, Elvis M. (SF) (FBI)
Sent: Tuesday, October 6, 2020 2:15:36 AM (UTC) Coordinated Universal Time
To: Chan, Elvis M. (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] (CD) (FBI);
Dehmlow, Laura E. (CD) (FBI); [REDACTED] (MH) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (OGC) (FBI); [REDACTED]
(SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (CID) (FBI)
Cc: [REDACTED] (TD) (FBI); [REDACTED] (CYD) (FBI); [REDACTED] (SF) (FBI)
Subject: FITF Meeting with Facebook
When: Wednesday, October 14, 2020 5:00 PM-6:00 PM.
Where: [REDACTED]

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have OGA attend if they can get information approved for sharing.

From: [REDACTED]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: Chan, Elvis M. (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

Elvis,
For the next FITF meeting in order of preference we'd like to meet:
1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

FACEBOOK

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.

<https://www.facebook.com/GoVoteKY/>

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you.

Thanks!
Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent

W: [REDACTED]
C: [REDACTED]

Produced to HJC

Exhibit 17

Message

From: [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov
Sent: 1/31/2020 10:36:34 PM
To: [REDACTED]@google.com
Subject: War room / Command Post

Hi [REDACTED]:

We are looking forward to the FITF meeting with Google the afternoon of February 10th.

Is there any possibility that earlier on the 10th we could also have a smaller meeting with you focused exclusively on the potential "war room" / "command post"?

We are working to ensure that any such venture would be designed in a manner that both helps protect the American people and respects and abides by the Constitution and laws of the United States. To maximize legal compliance, respect for civil liberties, and effectiveness we want to make sure we have a strong understanding of your vision of the scope of such potential venture.

>From our end, attendees would include three to four lawyers and hopefully one operational leader.

Thank you so much for your attention to this. Have a wonderful weekend.

Respectfully,

[REDACTED]
Assistant General Counsel -- Foreign Influence Taskforce
Office of the General Counsel
(O) [REDACTED] || (C) [REDACTED]

Exhibit 18

Message

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=CB41AB97A72A43D69BE84835781154F9-[REDACTED]]

Sent: 1/9/2020 11:09:13 AM

To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b47ad1e0d3d94720bd39ffe30a31bd01-[REDACTED]]
 [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c97a38fede0f4b71b9cc0ba3f53c6f90-[REDACTED]] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=acf3fad1e8f4f27b41b3d62823a453d-[REDACTED]] [REDACTED]
 [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b17836bba2b445b0b186b9c2baec2179-[REDACTED]] [REDACTED]; [REDACTED]
 [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4c318ea7472445b8a022fbd1355c9430-[REDACTED]] [REDACTED]
 [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7e0acc320c214954b766d69d2fd89f1e-[REDACTED]]

Subject: Re: Next FITF Meeting

I can only make the Feb 11th date, since I'm on DTO the rest of that week. Thanks!

[REDACTED]
 Threat Prevention
 Trust & Safety

On 1/9/20, 10:57 AM, [REDACTED]@linkedin.com> wrote:

[REDACTED]

I will be on the road during all of those days, but between [REDACTED] [REDACTED] and [REDACTED] one of them should be able to cover -- please make sure one of them is available on whichever date is chosen. Thanks so much.

-----Original Message-----

From: [REDACTED]@linkedin.com>
 Sent: Thursday, January 9, 2020 10:45 AM
 To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>
 Subject: RE: Next FITF Meeting

Hi Elvis,

Happy New Year! My apologies for the delay. I added a mini vacation to our company shut down and I'm still catching up. We can make the following work:

February 11, 1 PM, 3 PM
 February 12, 3 PM
 February 13, 10 AM, 1 PM

Thanks so much,



-----Original Message-----

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>
 Sent: Monday, January 6, 2020 2:13 PM
 To: [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>
 Subject: RE: Next FITF Meeting

Thanks [REDACTED] For your awareness, Feb. 12 and 10 am and 1 pm are taken now. I also want to add February 10 at 3 pm and February 14 at 10 am as options.

Regards,
 Elvis

Elvis M. Chan
 Supervisory Special Agent
 Squad CY-1, National Security Cyber
 FBI San Francisco

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

-----Original Message-----

From: [REDACTED]@linkedin.com]
Sent: Monday, January 06, 2020 1:52 PM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>
Subject: [SOCIAL NETWORK] Re: Next FITF Meeting

[REDACTED] to help with scheduling.

Thanks Elvis! We'll figure out a time and let you know.

Happy New Year!

[REDACTED]
Threat Prevention
Trust & Safety

On 1/3/20, 3:48 PM, "Chan, Elvis M. (SF) (FBI)" <[REDACTED]@fbi.gov> wrote:

All,

Happy New Year! We wanted to gauge your availability to meet with FITF next month. Here are the open dates/times:

- February 11, 10 AM, 1 PM, 3 PM
- February 12, 10 AM, 1 PM, 3 PM
- February 13, 10 AM, 1 PM, 3 PM

The tentative agenda will include discussion of election related crimes by DOJ and an IRA update. Hope all is well.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security Cyber
FBI San Francisco

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 19

Subject: FITF Meeting with Verizon Media
Location: Yahoo, 110 5th St, San Francisco, CA 94103, USA
Start: Wed, 12 Feb 2020 6:00:00 PM
End: Wed, 12 Feb 2020 7:30:00 PM
Organizer: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov >
Required Attendees: [REDACTED]@verizonmedia.com;

Tentative agenda: (1) IRA update, and (2) DOJ discussion of election crimes.

From: [REDACTED]@verizonmedia.com]
Sent: Monday, January 06, 2020 12:27 PM
To: Chan, Elvis M. (SF) (FBI)
Subject: Re: Next FITF Meeting

Hey Elvis! Let's pick the February 12, 10AM time slot.

Thank you!

On Fri, Jan 3, 2020 at 3:46 PM Chan, Elvis M. (SF) (FBI) > wrote:

Happy New Year! We wanted to gauge your availability to meet with FITF next month. Here are the open dates/times:

February 11, 10 AM, 1 PM, 3 PM
February 12, 10 AM, 1 PM, 3 PM
February 13, 10 AM, 1 PM, 3 PM

The tentative agenda will include discussion of election related crimes by DOJ and an IRA update. Hope all is well.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security Cyber
FBI San Francisco

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

--
[REDACTED]
[REDACTED]
Senior Director, Cyber Defense
The Paranoids

[REDACTED]
@TheParanoids
110 Fifth St
San Francisco, CA 94103

Exhibit 20

From: "Chan, Elvis M. (SF) (FBI)" [REDACTED]@fbi.gov >
To: [REDACTED]@verizonmedia.com >
CC: [REDACTED]@verizonmedia.com) " [REDACTED]@verizonmedia.com >
Subject: RE: Next FITF Meeting
Date: Mon, 13 Apr 2020 21:00:16 +0000
Message-ID: <BN3P110MB0420C9BF99FE638D1A5AA6CBCBDD0@BN3P110MB0420.NAMP110.PROD.OUTLOOK.COM >

You responded first so you got first dibs. Thanks.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED]@verizonmedia.com >
Sent: Monday, April 13, 2020 1:52 PM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov >
Cc: [REDACTED]@verizonmedia.com) [REDACTED]@verizonmedia.com >
Subject: Re: Next FITF Meeting

Hey Elvis - Can we reserve the Monday 10am time? Thanks!

On Mon, Apr 13, 2020 at 4:15 PM Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov > wrote:

All,

We're looking to set up a teleconference for our next FITF quarterly meeting. The tentative agenda will include: (1) IRA/EBLA update, (2) PRC influence activities, (3) Iranian influence activities, (4) Iranian cyber activities, and (5) planning for the general elections. Let me know if you would like to add or modify any agenda items.

Here are the proposed dates/times. Please select a 1.5 hour block and let me know. I'll send a calendar invitation with the dial-in information to lock it in. Looking forward to catching up. Stay well.

- Monday, May 18, 10 am to 3 pm PT
- Tuesday, May 19, 10 am to 3 pm PT
- Wednesday, May 20, 12 pm to 3 pm PT
- Thursday, May 21, 10 am to 3 pm PT
- Friday, May 22, 10 am to 3 pm PT

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

[REDACTED]

[REDACTED]

Senior Manager
Paranoids - Advanced Cyber Threats Team

M [REDACTED]

Washington, DC 20006

Exhibit 21

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 4/14/2020 9:51:21 PM
To: [REDACTED]@google.com); [REDACTED]@google.com); [REDACTED]@google.com); [REDACTED]@google.com); [REDACTED]@google.com); [REDACTED]@google.com); [REDACTED]@verizonmedia.com); [REDACTED]@google.com); [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CD) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (MH) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (OGC)(FBI) [REDACTED]@fbi.gov]; [REDACTED] (WF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (AI) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@FBI.GOV]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (DO) (FBI) [REDACTED]@fbi.gov]

Subject: FITF Meeting with Google/YouTube
Location: [REDACTED]

Start: 5/19/2020 8:30:00 PM
End: 5/19/2020 10:00:00 PM
Show Time As: Tentative

Recurrence: (none)

The tentative agenda will include: (1) IRA/EBLA update, (2) PRC influence activities, (3) Iranian influence activities, (4) Iranian cyber activities, and (5) planning for the general elections. Let me know if you would like to add or modify any agenda items. Forward to whomever you deem appropriate

USA only dial: [REDACTED]
 USA/Canada (Toll Free): [REDACTED]
 Guest Passcode: [REDACTED]

Confidential - Not For Public Release

Exhibit 22

Exhibit 23

Subject: FITF Meeting with Verizon Media
Location: [REDACTED], Guest Passcode: [REDACTED]
Start: Mon, 18 May 2020 5:00:00 PM
End: Mon, 18 May 2020 6:30:00 PM
Organizer: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov >
Required Attendees: [REDACTED]@verizonmedia.com;

The tentative agenda will include: (1) IRA/EBLA update, (2) PRC influence activities, (3) Iranian influence activities, (4) Iranian cyber activities, and (5) planning for the general elections. Let me know if you would like to add or modify any agenda items. Forward to whomever you deem appropriate

USA only dial: [REDACTED]
USA/Canada (Toll Free): [REDACTED]
Guest Passcode: [REDACTED]

Exhibit 24

Appointment

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7E0ACC320C214954B766D69D2FD89F1E-[REDACTED]]
Sent: 5/20/2020 8:58:56 AM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7114ab00281241b99e223b29739c5854-[REDACTED]]
Subject: FW: FITF Meeting with LinkedIn
Location: [REDACTED], Guest Passcode: [REDACTED]
Start: 5/20/2020 12:00:00 PM
End: 5/20/2020 1:30:00 PM
Show Time As: Tentative
Recurrence: (none)

Hi [REDACTED], we are meeting with the FBI today. Would be great to have you attend if you are available. Thanks, [REDACTED]

From: Chan, Elvis M. (SF) (FBI)
Sent: Tuesday, May 19, 2020 5:00:12 PM (UTC-08:00) Pacific Time (US & Canada)
To: Chan, Elvis M. (SF) (FBI); [REDACTED]; [REDACTED] (CD) (FBI); Dehmlow, Laura E. (CD) (FBI); [REDACTED], [REDACTED] (MH) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (WF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (AJ) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Subject: FITF Meeting with LinkedIn
When: Wednesday, May 20, 2020 12:00 PM-1:30 PM.
Where: [REDACTED], Guest Passcode: [REDACTED]

Hey there –

Yes it is! [REDACTED] and [REDACTED] are on the invite list. Not sure why you weren't. Hope this helps!

[REDACTED]
 Head of Threat Prevention
 Trust & Safety
 LinkedIn

From: [REDACTED]@fbi.gov
When: 12:00 PM - 1:30 PM May 20, 2020
Subject: FITF Meeting with LinkedIn
Location: [REDACTED], Guest Passcode: [REDACTED]

The tentative agenda will include: (1) IRA/EBLA update, (2) PRC influence activities, (3) Iranian influence activities, (4) Iranian cyberactivities, and (5) planning for the general elections. Let me know if you would like to add or modify any agenda items. Forward to whomever you deem appropriate

USA only dial: [REDACTED]
 USA/Canada (Toll Free): [REDACTED]
 Guest Passcode: [REDACTED]

From: Chan, Elvis M. (SF) (FBI)
Sent: Monday, April 13, 2020 11:21:24 PM (UTC) Coordinated Universal Time
To: Chan, Elvis M. (SF) (FBI); [REDACTED] (CD) (FBI); Dehmlow, Laura E. (CD) (FBI); [REDACTED] (MH) (FBI);
[REDACTED] (OGC) (FBI); [REDACTED] (WF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (AJ) (FBI); [REDACTED]
[REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED]
[REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Subject: FITF Meeting with LinkedIn
When: Wednesday, May 20, 2020 7:00 PM-8:30 PM.
Where: [REDACTED], Guest Passcode: [REDACTED]

The tentative agenda will include: (1) IRA/EBLA update, (2) PRC influence activities, (3) Iranian influence activities, (4) Iranian cyber activities, and (5) planning for the general elections. Let me know if you would like to add or modify any agenda items. Forward to whomever you deem appropriate

USA only dial: [REDACTED]
USA/Canada (Toll Free): [REDACTED]
Guest Passcode: [REDACTED]

Exhibit 25

From: "Chan, Elvis M. (SF) (FBI)" [REDACTED]@fbi.gov>
 [REDACTED]@verizonmedia.com>, [REDACTED]@fbi.gov>, "Dehmlow, Laura E. (CD) (FBI)" [REDACTED]@fbi.gov>, [REDACTED]@fbi.gov>
 To: [REDACTED]@fbi.gov>, [REDACTED]@fbi.gov>, [REDACTED]@fbi.gov>, [REDACTED]@fbi.gov>, [REDACTED]@fbi.gov>, [REDACTED]@fbi.gov>
 CC: [REDACTED]@verizonmedia.com) " [REDACTED]@verizonmedia.com>
 Subject: FITF Meeting with Verizon Media
 Date: Tue, 14 Jul 2020 20:44:58 +0000
 Message-ID: <BN3P110MB0274D0BD0568BA11D1D8E080CB610@BN3P110MB0274.NAMP110.PROD.OUTLOOK.COM>
 Attachments: image001.jpg

[REDACTED]

From: [REDACTED]@verizonmedia.com >
 Sent: Tuesday, July 14, 2020 11:24 AM
 To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>
 Cc: [REDACTED]@verizonmedia.com) [REDACTED]@verizonmedia.com >
 Subject: Re: Next FITF Meetings

Let's do the 13th at 10:30 am PT then. Thanks!

[REDACTED]

[REDACTED]

Senior Manager
 Paranoids - Advanced Cyber Threats Team

[REDACTED]

Washington, DC 20006

On Tue, Jul 14, 2020 at 2:16 PM Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov> wrote:

[REDACTED] – someone just reminded me the DHS/ODNI/FBI meetings are scheduled for the 12th at 11 am PT. I think you guys participate in that one too, right? If so, do you have an alternative date/time which works? Thanks.

Regards,
 Elvis

Elvis M. Chan
 Supervisory Special Agent
 Squad CY-1, National Security
 FBI San Francisco

Cell: [REDACTED]
Email: [REDACTED]
[REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED]@verizonmedia.com >
Sent: Tuesday, July 14, 2020 11:13 AM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov >
Cc: [REDACTED]@verizonmedia.com) [REDACTED]@verizonmedia.com >
Subject: Re: Next FITF Meetings

Hi Elvis,

August 12 at 10:30PT works well for my team. We're multi-coastal and that appeared to be the happy medium.

[REDACTED]

[REDACTED]

Senior Manager
Paranoids - Advanced Cyber Threats Team

[REDACTED]

Washington, DC 20006

On Tue, Jul 14, 2020 at 1:58 PM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

[REDACTED]

We'd like to get the next round of FITF meetings scheduled. The tentative agenda looks like this:

- Russia Status
 - IRA Update
 - OGA briefing (Russian software & influence campaign against Ukraine)
- China Status
 - General PRC Update
 - [REDACTED] briefing
- Global Status
 - Iran Update
 - Venezuela briefing
 - North Korea briefing
- Planning for U.S. Elections
 - FBI Posture
 - Your Posture
 - Information sharing channels and methods

Here are the proposed dates/times for a 1.5 hour meeting:

- August 10, 1:00 pm PT
- August 11, 10:30 am or 1:00 pm PT
- August 12, 10:30 am or 1:00 pm PT
- August 13, 10:30 am or 1:00 pm PT
- August 14, 10:30 am or 1:00 pm PT

Please let us know what works for you and I'll set up a teleconference call. Any materials we have to provide will be sent in advance. Thanks!

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco



This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 26

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 7/14/2020 8:54:17 PM
To: [REDACTED]@google.com]; [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CB) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (MH) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CID)(FBI) [REDACTED]@fbi.gov]; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (AJ) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CG) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (NY) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED]@google.com) [REDACTED]@google.com]
Subject: FITF Meeting with Google
Location: [REDACTED]
Start: 8/14/2020 5:30:00 PM
End: 8/14/2020 8:00:00 PM
Show Time As: Tentative
Recurrence: (none)

[REDACTED]
 Guest Passcode: [REDACTED]
 Forward to anyone who needs to be on this call.

From: [REDACTED]@google.com>
Sent: Tuesday, July 14, 2020 1:22 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED]@google.com) [REDACTED]@google.com>
Subject: Re: Next FITF Meetings

Hi Elvis,

We're good on Friday, August 14 at 10:30 pt. If you send me an invitation with call-in details, I can make sure it is distributed. Thank you.

On Tue, Jul 14, 2020 at 11:10 AM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Thanks [REDACTED] I forgot about the big meeting. The 1 pm meeting on the 15th is viable if you guys are willing to go back-to-back. Also, I'm awaiting final approval to share something with you regarding Iran. Stay tuned.

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED]@google.com>
Sent: Tuesday, July 14, 2020 11:08 AM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED]@google.com) <[REDACTED]@google.com>
Subject: Re: Next FITF Meetings

Hi Elvis,

Thank you for this. We'll check with the team and get back to you. (I think we are having the larger meeting on 8/12 so we may want to take that off the list of options.)

[REDACTED]

On Tue, Jul 14, 2020 at 10:59 AM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Hi [REDACTED],

We'd like to get the next round of FITF meetings scheduled. The tentative agenda looks like this:

Russia Status

- IRA Update
- OGA briefing (Russian software & influence campaign against Ukraine)

China Status

- General PRC Update
- [REDACTED] briefing

Global Status

- Iran Update
- Venezuela briefing
- North Korea briefing

Planning for U.S. Elections

- FBI Posture
- Your Posture

- Information sharing channels and methods

Here are the proposed dates/times for a 1.5 hour meeting:

August 10, 1:00 pm PT

August 11, 10:30 am or 1:00 pm PT

August 12, 10:30 am or 1:00 pm PT

August 13, 10:30 am or 1:00 pm PT

August 14, 10:30 am or 1:00 pm PT

Please let us know what works for you and I'll set up a teleconference call. Any materials we have to provide will be sent in advance. Thanks!

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 27

Appointment

From: Google Calendar [redacted]@google.com
 on behalf of [redacted] [redacted]@google.com
Sent: 7/14/2020 10:13:05 PM
To: [redacted] [redacted]@google.com]; [redacted]@linkedin.com; [redacted]@verizonmedia.com; [redacted]@medium.com; [redacted]@verizonmedia.com; [redacted]@fb.com]; [redacted]@medium.com; [redacted]@microsoft.com; [redacted]@pinterest.com; [redacted] [redacted]@fb.com]; [redacted] [redacted]@google.com]; [redacted]@wikimedia.org; [redacted] [redacted]@fb.com]; [redacted]@fb.com]; [redacted] [redacted]@google.com]; [redacted] [redacted]@fb.com]; [redacted]@fb.com]; [redacted] reddit.com; [redacted]@reddit.com; [redacted]@fb.com]; [redacted]@twitter.com; [redacted]@verizonmedia.com; [redacted]@twitter.com; [redacted]@fb.com]; [redacted]@fb.com]; [redacted]@twitter.com; [redacted]@verizonmedia.com; [redacted]@twitter.com; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted]@microsoft.com
CC: [redacted]@linkedin.com]; [redacted] [redacted]@linkedin.com]
Subject: Monthly USG | Industry Call
Attachments: invite.ics
Location: [redacted]
Start: 10/14/2020 6:00:00 PM
End: 10/14/2020 7:30:00 PM
Show Time As: Tentative
Recurrence: (none)

This event has been changed.

Monthly USG | Industry Call
 When Wed Oct 14, 2020 11am – 12:30pm Pacific Time - Los Angeles
 Where [redacted] (map)
 Calendar [redacted]
 Who

- [redacted] - organizer
- [redacted] - creator
- [redacted]@linkedin.com
- [redacted]@verizonmedia.com
- [redacted]@medium.com
- [redacted]@verizonmedia.com
- [redacted]
- [redacted]@medium.com
- [redacted]@microsoft.com
- [redacted]@pinterest.com

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [REDACTED]
- [REDACTED]
- [REDACTED]@reddit.com
- [REDACTED]@reddit.com
- [REDACTED]
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@twitter.com
- [REDACTED]
- [REDACTED]
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@twitter.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED] - optional
- [REDACTED] - optional

more details »

Changed: To join the meeting on a computer or mobile phone:

One-Touch: [REDACTED] Meeting ID: [REDACTED] Participant Passcode: [REDACTED] To join via phone: () Dial: [REDACTED] 2) Enter Conference ID: [REDACTED] Enter Participant Passcode: [REDACTED] Want to test your video connection? [REDACTED]

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [REDACTED]@fb.com.

Invitation from Google Calendar

You are receiving this email at the account [REDACTED]@google.com because you are subscribed for updated invitations on calendar [REDACTED]

To stop receiving these emails, please log in to <https://www.google.com/calendar/> and change your notification settings for this calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. [Learn More](#).

Confidential - Not for Public Release

Exhibit 28

From: "Chan, Elvis M. (SF) (FBI)" <[REDACTED]@fbi.gov>
 [REDACTED]@verizonmedia.com >, [REDACTED]@fbi.gov >, "Dehmlow, Laura E. (CD) (FBI)" <[REDACTED]@fbi.gov>
 [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >
To: [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >
 [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >
 [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >
 [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >
CC: [REDACTED]@verizonmedia.com >, [REDACTED]@verizonmedia.com >
 [REDACTED]@fbi.gov >, [REDACTED]@fbi.gov >
Subject: FITF Meeting with Verizon Media
Date: Fri, 24 Jul 2020 16:21:20 +0000
Message-ID: <CY1P110MB0280A0B95DEB6AB9F57CA669CB770@CY1P110MB0280.NAMP110.PROD.OUTLOOK.COM >

Attachments: image001.jpg; image002.jpg

USA/Canada (Toll Free): [REDACTED]

Guest Passcode: [REDACTED]

Please forward to anyone else you need to attend. Thanks!

From: [REDACTED]@verizonmedia.com <mailto:[REDACTED]@verizonmedia.com >>
Sent: Tuesday, July 14, 2020 11:24 AM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov <mailto:[REDACTED]@fbi.gov >>
Cc: [REDACTED]@verizonmedia.com <mailto:[REDACTED]@verizonmedia.com >
 <[REDACTED]@verizonmedia.com <mailto:[REDACTED]@verizonmedia.com >>
Subject: Re: Next FITF Meetings

Let's do the 13th at 10:30 am PT then. Thanks!

[Image removed by sender.]<<http://www.verizonmedia.com/>>

[REDACTED]
Senior Manager
Paranoids - Advanced Cyber Threats Team

M [REDACTED]
[REDACTED]
Washington, DC 20006

On Tue, Jul 14, 2020 at 2:16 PM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov <mailto:[REDACTED]@fbi.gov >>> wrote:

[REDACTED] – someone just reminded me the DHS/ODNI/FBI meetings are scheduled for the 12th at 11 am PT. I think you guys participate in that one too, right? If so, do you have an alternative date/time which works?
Thanks.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov <mailto:[REDACTED]@fbi.gov>

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED]@verizonmedia.com <mailto:[REDACTED]@verizonmedia.com >>
Sent: Tuesday, July 14, 2020 11:13 AM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov <mailto:[REDACTED]@fbi.gov>>
Cc: [REDACTED]@verizonmedia.com <mailto:[REDACTED]@verizonmedia.com >
<[REDACTED]@verizonmedia.com <mailto:[REDACTED]@verizonmedia.com >>
Subject: Re: Next FITF Meetings

Hi Elvis,

August 12 at 10:30PT works well for my team. We're multi-coastal and that appeared to be the happy medium.

[Image removed by sender.] <<http://www.verizonmedia.com/> >

[REDACTED]
Senior Manager
Paranoids - Advanced Cyber Threats Team

M [REDACTED]
[REDACTED]
Washington, DC 20006

On Tue, Jul 14, 2020 at 1:58 PM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov <mailto:[REDACTED]@fbi.gov>> wrote:
[REDACTED],

We'd like to get the next round of FITF meetings scheduled. The tentative agenda looks like this:

- Russia Status
 - IRA Update
 - OGA briefing (Russian software & influence campaign against Ukraine)
- China Status
 - General PRC Update
 - [REDACTED] briefing
- Global Status
 - Iran Update
 - Venezuela briefing
 - North Korea briefing
- Planning for U.S. Elections
 - FBI Posture

- Your Posture
- Information sharing channels and methods

Here are the proposed dates/times for a 1.5 hour meeting:

August 10, 1:00 pm PT
August 11, 10:30 am or 1:00 pm PT
August 12, 10:30 am or 1:00 pm PT
August 13, 10:30 am or 1:00 pm PT
August 14, 10:30 am or 1:00 pm PT

Please let us know what works for you and I'll set up a teleconference call. Any materials we have to provide will be sent in advance. Thanks!

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov <mailto:[REDACTED]@fbi.gov>

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 29

- AGENDA:
- Russia Status
- * IRA Update
- * OGA briefing (Software & influence campaign against Ukraine)
- China Status
- * General PRC Update
- * [REDACTED] briefing
- Global Status
- * Iran Update
- * Venezuela briefing
- * North Korea briefing
- Planning for U.S. Elections
- * FBI Posture
- * Your Posture
- * Information sharing channels and methods

From: Chan, Elvis M. (SF) (FBI)
Sent: Thursday, July 16, 2020 10:10:10 PM (UTC) Coordinated Universal Time
To: Chan, Elvis M. (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] (CD) (FBI); Dehmlow, Laura E. (CD) (FBI); [REDACTED] (MH) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (CD) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (CD) (FBI); [REDACTED] (CG) (FBI); [REDACTED] (NY) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (PH) (FBI); [REDACTED] (PH) (FBI); [REDACTED] (PH) (FBI)
Cc: [REDACTED] (DO) (FBI)
Subject: FITF Meeting with Facebook
When: Monday, August 10, 2020 8:00 PM-9:30 PM.
Where: [REDACTED]

CENTURY LINK UNCLASSIFIED AUDIO/TELEPHONE ONLY BRIDGE
 USA only dial [REDACTED]
 USA/Canada (Toll Free): [REDACTED]
 Guest Passcode: [REDACTED]
 IF YOU HAVE ANY ISSUES WITH THIS CALL PLEASE CALL CENTURY LINK SUPPORT AT [REDACTED]
 AGENDA:

- Russia Status
- * IRA Update
- * OGA briefing (Software & influence campaign against Ukraine)
- China Status
- * General PRC Update
- * [REDACTED] briefing
- Global Status
- * Iran Update
- * Venezuela briefing
- * North Korea briefing
- Planning for U.S. Elections
- * FBI Posture
- * Your Posture
- * Information sharing channels and methods

Exhibit 30

From: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
To: [REDACTED]
CC: [REDACTED]
Sent: 8/11/2020 5:03:18 PM
Subject: Attendee List

[REDACTED],

Here is the list of attendees from our meeting yesterday:

FITF-Russia

UC [REDACTED]
SSA [REDACTED]
IA [REDACTED]
IA [REDACTED]
AGC [REDACTED]

FITF-China

UC Laura Dehmlow
SIA [REDACTED]
SSA [REDACTED]

FITF-Global

UC [REDACTED]
SSA [REDACTED]
SIA [REDACTED]

Cyber Division

SSA [REDACTED]
SSA [REDACTED]

Criminal Investigative Division

IA [REDACTED]
IA [REDACTED]

Field Offices

SA [REDACTED] (PH)
SA [REDACTED] (PH)
IA [REDACTED] (PH)
SOS [REDACTED] (PH)
SA [REDACTED] (NY)
SA [REDACTED] (CG)
SA [REDACTED] (SF)
SSA [REDACTED] (SF)
SSA [REDACTED] (SF)
IA [REDACTED] (SF)

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]

Produced to HJC

Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

Final Report 1140

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Monday, August 10, 2020 12:37 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Re: [EXTERNAL EMAIL] - Re: FITF Meeting with Facebook

Elvis,

We have tried to round out our group to include investigators, le outreach, legal and policy. Our attendees for our meeting in about 25 minutes are expected to be:

[REDACTED]

Produced to HJC

Speak soon.

[REDACTED]

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>
Date: Thursday, August 6, 2020 at 4:58 PM
To: [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: [EXTERNAL EMAIL] - Re: FITF Meeting with Facebook

Hi [REDACTED],

Yes I have seen the invitation accepted notifications. I would appreciate a list of attendees. From our side it will be FBI only. OGA will not be joining this time, but [REDACTED] will brief their materials. Thanks. Final Report 1141

Regards,

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

On Aug 6, 2020 1:51 PM, [REDACTED] <[REDACTED]@fb.com> wrote:
Elvis –

I hope you have seen the folks to whom I have forwarded the invitation to our Monday meeting. I'm going to forward to three more investigators and that should be it. Let me know if you'd like a list of the folks who are attending from our side. We are trying to be as complete as possible with SMEs.

[REDACTED]

FACEBOOK

From: [REDACTED]@fbi.gov
When: 4:00 PM - 5:30 PM August 10, 2020
Subject: FITF Meeting with Facebook
Location: [REDACTED]

CENTURY LINK UNCLASSIFIED AUDIO/TELEPHONE ONLY BRIDGE

USA only dial: [REDACTED]

USA/Canada (Toll Free): [REDACTED]

Guest Passcode: [REDACTED]

IF YOU HAVE ANY ISSUES WITH THIS CALL PLEASE CALL CENTURY LINK SUPPORT AT [REDACTED]
AGENDA:

Russia Status

- * IRA Update
- * OGA briefing (Software & influence campaign against Ukraine)

China Status

- * General PRC Update
- * [REDACTED] briefing

Global Status

- * Iran Update
- * Venezuela briefing
- * North Korea briefing

- * FBI Posture
- * Your Posture
- * Information sharing channels and methods

Produced to HJC

Exhibit 31

Appointment

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7E0ACC320C214954B766D69D2FD89F1E-[REDACTED]]
Sent: 8/10/2020 1:16:51 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7114ab00281241b99e223b29739c5854-[REDACTED]]
Subject: FW: FITF Meeting with LinkedIn
Location: [REDACTED], PIN [REDACTED]
Start: 8/12/2020 1:00:00 PM
End: 8/12/2020 2:30:00 PM
Show Time As: Tentative
Recurrence: (none)

Big day of meetings. Thanks for taking notes!

From: Chan, Elvis M. (SF) (FBI)
Sent: Tuesday, July 14, 2020 1:49:14 PM (UTC-08:00) Pacific Time (US & Canada)
To: Chan, Elvis M. (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] (CD) (FBI);
 Dehmlow, Laura E. (CD) (FBI); [REDACTED] (MH) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (OGC)
 (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (AJ) (FBI); [REDACTED] (NY)
 (FBI); [REDACTED] (CG) (FBI); [REDACTED] (CD) (FBI); [REDACTED] (CID) (FBI); [REDACTED]
 (CD) (FBI); [REDACTED] (PH) (FBI); [REDACTED] (PH) (FBI); [REDACTED] (PH) (FBI)
Cc: [REDACTED]; [REDACTED]; [REDACTED] (OGC) (FBI)
Subject: FITF Meeting with LinkedIn
When: Wednesday, August 12, 2020 1:00 PM-2:30 PM.
Where: [REDACTED], PIN [REDACTED]

USA/Canada (Toll Free): [REDACTED]
 Guest Passcode: [REDACTED]

From: [REDACTED]@linkedin.com>
Sent: Tuesday, July 14, 2020 11:32 AM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED]
 <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>
Cc: [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>
Subject: [SOCIAL NETWORK] Re: Next FITF Meetings

Thanks, Elvis. Hope you are well.

How about August 12 at 1 pm PT for LinkedIn? Alternatively, August 13 at 1 pm PT?

Thanks,
[REDACTED]

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov<mailto:emchan@fbi.gov>>
Sent: Tuesday, July 14, 2020 11:02 AM
To: [REDACTED] <[REDACTED]@linkedin.com<mailto:[REDACTED]@linkedin.com>>; [REDACTED]
 <[REDACTED]@linkedin.com<mailto:[REDACTED]@linkedin.com>>; [REDACTED]
 [REDACTED]@linkedin.com<mailto:[REDACTED]@linkedin.com>>; [REDACTED]
 <[REDACTED]@linkedin.com<mailto:[REDACTED]@linkedin.com>>
Cc: [REDACTED] <[REDACTED]@linkedin.com<mailto:[REDACTED]@linkedin.com>>; [REDACTED]
 <[REDACTED]@linkedin.com<mailto:[REDACTED]@linkedin.com>>

Subject: Next FITF Meetings

All,

We'd like to get the next round of FITF meetings scheduled. The tentative agenda looks like this:

Russia Status

- IRA Update
- OGA briefing (Russian software & influence campaign against Ukraine)

China Status

- General PRC Update
- [REDACTED] briefing

Global Status

- Iran Update
- Venezuela briefing
- North Korea briefing

Planning for U.S. Elections

- FBI Posture
- Your Posture
- Information sharing channels and methods

Here are the proposed dates/times for a 1.5 hour meeting:

August 10, 1:00 pm PT

August 11, 10:30 am or 1:00 pm PT

August 12, 10:30 am or 1:00 pm PT

August 13, 10:30 am or 1:00 pm PT

August 14, 10:30 am or 1:00 pm PT

Please let us know what works for you and I'll set up a teleconference call. Any materials we have to provide will be sent in advance. Thanks!

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov<mailto:[REDACTED]@fbi.gov>

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 32

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 9/10/2020 4:32:22 PM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b48d6f5efa9640af9d49ecb0f63fdd91-[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b17836bba2b445b0b186b9c2baec2179-[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4c318ea7472445b8a022fbd1355c9430-[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7e0acc320c214954b766d69d2fd89f1e-[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d6915d479cd74fc99079271b15f73467-[REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CD) (FBI) [REDACTED]@fbi.gov; [REDACTED] (MH) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CYD) (FBI) [REDACTED]@fbi.gov; [REDACTED] (NY) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c7d2d77006a842be9b0761ed156a4f8d-[REDACTED] (LA) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CYD) (FBI) [REDACTED]@fbi.gov; [REDACTED] (NY) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c7d2d77006a842be9b0761ed156a4f8d-[REDACTED] (LA) (FBI) [REDACTED]@fbi.gov]
Subject: FITF Meeting with LinkedIn
Location: [REDACTED]
Start: 9/22/2020 10:00:00 AM
End: 9/22/2020 11:00:00 AM
Show Time As: Busy
Recurrence: (none)

- Russia influence update – [REDACTED]
- China influence update (Dehmlow)
- Iran influence update [REDACTED]
- [REDACTED] Post Indictment Discussion [REDACTED]
- Iran briefing on [REDACTED] intrusion set [REDACTED]
- Election logistics (Chan/All)

From: [REDACTED]@linkedin.com>
Sent: Thursday, September 10, 2020 4:27 PM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com> [REDACTED]@linkedin.com>
Subject: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: Next FITF Meetings

Hi Elvis,

Hope all is well. If the 22 September slot from 10-11 PDT is still available, we'll take it.

Thanks!

[REDACTED]

--

[REDACTED]

Advanced Threats

Trust & Safety

 The link

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>
Sent: Thursday, September 10, 2020 2:13 PM
To: [REDACTED]@linkedin.com> [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>; [REDACTED]@linkedin.com>
Subject: Next FITF Meetings

LinkedIn folks,

We wanted to hold our next round of FITF meetings the week of September 21st. I haven't nailed down the agenda yet, but thought it would be good to put something on the calendar.

- Monday, September 21, 10-11 am or 1-2 pm PDT
- Tuesday, September 22, 10-11 am or 1-2 pm PDT
- Wednesday, September 23, 10-11 am or 1-2 pm PDT
- Thursday, September 24, 1-2 pm PDT
- Friday, September 25, 1-2 pm PDT

Pick a time slot and I'll send a calendar invitation to lock it in. I'm tentatively penciling in the week of October 12th for our last set of meetings before the elections. Let me know what you think.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 33

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 9/11/2020 7:05:57 PM
To: [REDACTED] [REDACTED]@google.com]; [REDACTED] [REDACTED]@google.com) [REDACTED]@google.com]; [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CD) (FBI) [REDACTED]@fbi.gov]; [REDACTED] a T. (MH) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CID)(FBI) [REDACTED]@fbi.gov]; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov]; [REDACTED] NY) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED] (DO) (FBI) [REDACTED]@fbi.gov]
Subject: FITF Meeting with Google
Location: [REDACTED]
Start: 9/22/2020 8:00:00 PM
End: 9/22/2020 9:00:00 PM
Show Time As: Tentative

Recurrence: (none)

Alcon – please forward to whomever you deem appropriate. Agenda TBD, but we will have a briefing from New York on the Iranian intrusion set known as [REDACTED] or [REDACTED]

From: [REDACTED] <[REDACTED]@google.com>
Sent: Thursday, September 10, 2020 5:20 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] ([REDACTED]@google.com) <[REDACTED]@google.com>
Subject: [EXTERNAL EMAIL] - Re: Next FITF Meetings

Hi Elvis,

Tuesday, September 22 from 1-2 works for all of us. Thank you.

On Thu, Sep 10, 2020 at 2:13 PM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

[REDACTED]

We wanted to hold our next round of FITF meetings the week of September 21st. I haven't nailed down the agenda yet, but thought it would be good to put something on the calendar.

Monday, September 21, 10-11 am or 1-2 pm PDT
 Tuesday, September 22, 10-11 am or 1-2 pm PDT
 Wednesday, September 23, 10-11 am or 1-2 pm PDT
 Thursday, September 24, 1-2 pm PDT
 Friday, September 25, 1-2 pm PDT

Pick a time slot and I'll send a calendar invitation to lock it in. I'm tentatively penciling in the week of October 12th for our last set of meetings before the elections. Let me know what you think.

Regards,

Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Confidential - Not For Public Release

Exhibit 34

From: "Chan, Elvis M. (SF) (FBI)" [REDACTED]@fbi.gov>
 [REDACTED]@verizonmedia.com [REDACTED]@verizonmedia.com [REDACTED]
 [REDACTED]@verizonmedia.com' [REDACTED]@verizonmedia.com [REDACTED]@fbi.gov>,
 To: "Dehmlow, Laura E. (CD) (FBI)" [REDACTED]@fbi.gov [REDACTED]@fbi.gov>,
 [REDACTED]@fbi.gov>,' [REDACTED]@fbi.gov> [REDACTED]@fbi.gov> [REDACTED]
 [REDACTED]@fbi.gov>
 CC: [REDACTED]@fbi.gov>
 Subject: [E] FITF Meeting with Verizon Media
 Date: Mon, 14 Sep 2020 21:49:08 +0000
 Message-ID: <DM3P110MB0361C265783E22DB1BFB1541CB230@DM3P110MB0361.NAMP110.PROD.OUTLOOK.COM
 >
 Attachments: image001.jpg

Forward to whomever you deem appropriate. Monthly Touchpoint – agenda TBD, but we will definitely be providing an update on a Russian-backed news site and provide an overview of the Iranian intrusion set known as [REDACTED] or [REDACTED].
 [REDACTED] Thanks!

From: [REDACTED] [REDACTED]@verizonmedia.com >
 Sent: Monday, September 14, 2020 2:26 PM
 To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>
 Cc: [REDACTED]@verizonmedia.com >; [REDACTED]@verizonmedia.com) <[REDACTED]@verizonmedia.com >
 Subject: [EXTERNAL EMAIL] - Re: [E] Next FITF Meeting

Let's do the 24th at 1 PDT.

On Mon, Sep 14, 2020 at 5:21 PM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Paranoids,

Just touching base to see when you can meet for our next touch point. We will have a threat briefing on the Iranian intrusion set known as [REDACTED] or [REDACTED] I know we have one Russian-backed media site to share with you as well. The rest

is TBD. Please pick one of the remaining dates/times below. We'll only need an hour of your time. Thanks!

September 21, 10 am or 1 pm PDT

September 23, 10 am PDT

September 24, 1 pm PDT

September 25, 1 pm PDT

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

[REDACTED]

[REDACTED]

[REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is

loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

[Redacted]

[Redacted]

Senior Manager
Paranoids - Advanced Cyber Threats Team

[Redacted]

Exhibit 35

From: "Chan, Elvis M. (SF) (FBI)" <[REDACTED]@fbi.gov>
Sent: Fri 9/18/2020 5:56:06 PM (UTC)
To: [REDACTED]@google.com>, [REDACTED]@google.com>, [REDACTED] (CD) (FBI)" <[REDACTED]@fbi.gov>, "Dehmlow, Laura E. (CD) (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] (MH) (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] (CID) (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] OGC (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] (NY) (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] (SF) (FBI)" <[REDACTED]@fbi.gov>, [REDACTED] (SF) (FBI)" <[REDACTED]@fbi.gov>
Subject: FITF Meeting with Google

Please forward to whomever you deem appropriate.

Agenda:

- Russian Influence Overview & discussion of recent information passed [REDACTED]
- Chinese Influence Overview (Dehmlow)
- Global/Iranian Influence Overview [REDACTED]
- [REDACTED] Post Indictment Discussion [REDACTED]
- [REDACTED] Overview [REDACTED]
- Election Coordination Discussion (Chan/FITF/Google)

From: [REDACTED] <[REDACTED]@google.com>
Sent: Friday, September 18, 2020 8:28 AM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] ([REDACTED]y@google.com) <[REDACTED]@google.com>
Subject: [EXTERNAL EMAIL] - Re: Next Week's FITF Meeting

This is getting pretty tricky now. We may be able to do Sept 21 from 1:30-2:30. Would that work from your end?

Exhibit 36

From: [REDACTED] [/O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]237] Final Report 1160
Location: [REDACTED] passcode [REDACTED]
Importance: Normal
Subject: FW: FITF Meeting with Facebook
Start Time: Mon 9/21/2020 10:00:00 AM (UTC-07:00)
End Time: Mon 9/21/2020 11:00:00 AM (UTC-07:00)
Required Attendees: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] (CD) (FBI); Dehmlow, Laura E. (CD) (FBI); [REDACTED] (MH) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (NY) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (CID) (FBI)

From: [REDACTED]@fbi.gov
When: 1:00 PM - 2:00 PM September 21, 2020
Subject: FITF Meeting with Facebook
Location: [REDACTED] passcode [REDACTED]

Please forward to whomever you deem appropriate. At this time, there will only be FBI employees from the USG side. No other agencies are scheduled to attend. I don't anticipate we'll need the full hour unless you have updates for us. Thanks!

- Tentative agenda:
1. Russia influence update - [REDACTED]
 2. China influence update
 3. Iran influence update
 4. Iran briefing on [REDACTED] intrusion set
 5. Election logistics

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, September 17, 2020 12:10 PM
To: [REDACTED] (SF) (FBI) <[REDACTED]@fbi.gov>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Re: [EXTERNAL EMAIL] - Re: Next FITF Meetings

Elvis,
Our preference is for September 21 at 10 am PT. Second choice would be Sept. 21 at 1 pm PT.

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>
Date: Monday, September 14, 2020 at 5:23 PM
To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: RE: [EXTERNAL EMAIL] - Re: Next FITF Meetings

Just touching base to see when you can meet for our next touch point. We will have a threat briefing on the Iranian intrusion set known as [REDACTED] or [REDACTED]. I know we have one Russian-backed media site to share with you as well. The rest is TBD. Please pick one of the dates/times below. We'll only need an hour of your time. Thanks!

- September 21, 10 am or 1 pm PDT
- September 23, 10 am PDT
- September 24, 1 pm PDT
- September 25, 1 pm PDT

Regards,
Elvis
Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, September 10, 2020 2:52 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Re: [EXTERNAL EMAIL] - Re: Next FITF Meetings

That works for us. We'll get back to you.

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>
Date: Thursday, September 10, 2020 at 5:51 PM
To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: [EXTERNAL EMAIL] - Re: Next FITF Meetings

[REDACTED] it would be one hour tops. I'm trying to get NY to discuss [REDACTED] but haven't gotten confirmation yet. I think the influence updates will be pretty light but we just wanted to put something on the calendar so we can have a touchpoint at an increased cadence. Let me know what you think. Thanks.

Regards,
Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco

Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

On Sep 10, 2020 2:44 PM, [REDACTED] <[REDACTED]@fb.com> wrote:

Elvis,
Are you looking for 90 minutes again? Also, are we breaking out the [REDACTED] discussion or keeping it here?

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>
Date: Thursday, September 10, 2020 at 5:12 PM
To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Next FITF Meetings

Facebook folks,
We wanted to hold our next round of FITF meetings the week of September 21st. I haven't nailed down the agenda yet, but thought it would be good to put something on the calendar.

- Monday, September 21, 10-11 am or 1-2 pm PDT
- Tuesday, September 22, 10-11 am or 1-2 pm PDT
- Wednesday, September 23, 10-11 am or 1-2 pm PDT
- Thursday, September 24, 1-2 pm PDT
- Friday, September 25, 1-2 pm PDT

Pick a time slot and I'll send a calendar invitation to lock it in. I'm tentatively penciling in the week of October 12th for our last set of meetings before the elections. Let me know what you think.

Regards,
Elvis
Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco

Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: Chan, Elvis M. (SF) (FBI)
Sent: Thursday, September 17, 2020 7:17:46 PM (UTC) Coordinated Universal Time
To: Chan, Elvis M. (SF) (FBI); [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED] (CD) (FBI); Dehmlow, Laura E. (CD) (FBI); [REDACTED] (MH) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (SF) (FBI); [REDACTED] (NY) (FBI); [REDACTED] (CID) (FBI); [REDACTED] (CID) (FBI)
Subject: FITF Meeting with Facebook
When: Monday, September 21, 2020 5:00 PM-6:00 PM.
Where: 877-446-3914, passcode 130254

Please forward to whomever you deem appropriate. At this time, there will only be FBI employees from the USG side. No other agencies are scheduled to attend. I don't anticipate we'll need the full hour unless you have updates for us. Thanks!

Tentative agenda:

- Russia influence update - [REDACTED]
- China influence update
- Iran influence update
- Iran briefing on [REDACTED] intrusion set
- Election logistics

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, September 17, 2020 12:10 PM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Re: [EXTERNAL EMAIL] - Re: Next FITF Meetings

Elvis,
Our preference is for September 21 at 10 am PT. Second choice would be Sept. 21 at 1 pm PT.

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>
Date: Monday, September 14, 2020 at 5:23 PM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: RE: [EXTERNAL EMAIL] - Re: Next FITF Meetings

Alcon,
Just touching base to see when you can meet for our next touch point. We will have a threat briefing on the Iranian intrusion set known as [REDACTED] or [REDACTED]. I know we have one Russian-backed media site to share with you as well. The rest is TBD. Please pick one of the dates/times below. We'll only need an hour of your time. Thanks!

- September 21, 10 am or 1 pm PDT
- September 23, 10 am PDT
- September 24, 1 pm PDT
- September 25, 1 pm PDT

Regards,
Elvis
Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco

Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED] <[REDACTED]@fb.com>

Sent: Thursday, September 10, 2020 2:52 PM

To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>

Cc: [REDACTED] <[REDACTED]@fb.com>

Subject: Re: [EXTERNAL EMAIL] - Re: Next FITF Meetings

That works for us. We'll get back to you.

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>

Date: Thursday, September 10, 2020 at 5:51 PM

To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>

Cc: [REDACTED] <[REDACTED]@fb.com>

Subject: [EXTERNAL EMAIL] - Re: Next FITF Meetings

[REDACTED] - it would be one hour tops. I'm trying to get NY to discuss [REDACTED] but haven't gotten confirmation yet. I think the influence updates will be pretty light but we just wanted to put something on the calendar so we can have a touchpoint at an increased cadence. Let me know what you think. Thanks.

Regards,

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email: [REDACTED]@fbi.gov

On Sep 10, 2020 2:44 PM, [REDACTED] <[REDACTED]@fb.com> wrote:

Elvis,

Are you looking for 90 minutes again? Also, are we breaking out the [REDACTED] discussion or keeping it here?

FACEBOOK

From: Elvis Chan <[REDACTED]@fbi.gov>

Date: Thursday, September 10, 2020 at 5:12 PM

To: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>

Cc: [REDACTED] <[REDACTED]@fb.com>

Subject: Next FITF Meetings

Facebook folks,

We wanted to hold our next round of FITF meetings the week of September 21st. I haven't nailed down the agenda yet, but thought it would be good to put something on the calendar.

Monday, September 21, 10-11 am or 1-2 pm PDT

Tuesday, September 22, 10-11 am or 1-2 pm PDT

Wednesday, September 23, 10-11 am or 1-2 pm PDT

Thursday, September 24, 1-2 pm PDT

Friday, September 25, 1-2 pm PDT

Pick a time slot and I'll send a calendar invitation to lock it in. I'm tentatively penciling in the week of October 12th for our last set of meetings before the elections. Let me know what you think.

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Produced to HJC

Exhibit 37

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 9/18/2020 11:06:33 AM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b48d6f5efa9640af9d49ecb0f63fdd91-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b17836bba2b445b0b186b9c2baec2179-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4c318ea7472445b8a022fbd1355c9430-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7e0acc320c214954b766d69d2fd89f1e-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d6915d479cd74fc99079271b15f73467-[REDACTED]]; [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CD) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (MH) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CYD) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED] (NY) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c7d2d77006a842be9b0761ed156a4f8d-[REDACTED]]; [REDACTED] (LA) (FBI) [REDACTED]@fbi.gov]
Subject: FITF Meeting with LinkedIn
Location: [REDACTED] passcode [REDACTED]
Start: 9/22/2020 10:00:00 AM
End: 9/22/2020 11:00:00 AM
Show Time As: Tentative
Recurrence: (none)

- Russia influence update ([REDACTED])
- China influence update (Dehmlow)
- Iran influence update ([REDACTED])
- [REDACTED] Post Indictment Discussion ([REDACTED])
- Iran briefing on [REDACTED] intrusion set ([REDACTED])
- Election logistics (Chan/All)

From: [REDACTED] <[REDACTED]@linkedin.com>
Sent: Thursday, September 10, 2020 4:27 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>
Subject: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: Next FITF Meetings

Hi Elvis,

Hope all is well. If the 22 September slot from 10-11 PDT is still available, we'll take it.

Thanks!

[REDACTED]

--

[REDACTED]

Advanced Threats

Trust & Safety

 The link

From: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>

Sent: Thursday, September 10, 2020 2:13 PM

To: [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@linkedin.com>

Subject: Next FITF Meetings

LinkedIn folks,

We wanted to hold our next round of FITF meetings the week of September 21st. I haven't nailed down the agenda yet, but thought it would be good to put something on the calendar.

Monday, September 21, 10-11 am or 1-2 pm PDT
Tuesday, September 22, 10-11 am or 1-2 pm PDT
Wednesday, September 23, 10-11 am or 1-2 pm PDT
Thursday, September 24, 1-2 pm PDT
Friday, September 25, 1-2 pm PDT

Pick a time slot and I'll send a calendar invitation to lock it in. I'm tentatively penciling in the week of October 12th for our last set of meetings before the elections. Let me know what you think.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 38

Subject: FITF Meeting with Verizon Media
Location: [REDACTED], passcode [REDACTED]
Start: Thu, 24 Sep 2020 8:00:00 PM
End: Thu, 24 Sep 2020 9:00:00 PM
Organizer: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>
Optional Attendees: [REDACTED]@verizonmedia.com;
Attachments: <unknown>;

Forward to whomever you deem appropriate.

- * Russia influence update - [REDACTED]
- * China influence update (Dehmlow)
- * Iran influence update [REDACTED]
- * [REDACTED] Post Indictment Discussion [REDACTED]
- * Iran briefing on [REDACTED] intrusion set [REDACTED]
- * Election logistics (Chan/All)

From: [REDACTED] >
Sent: Monday, September 14, 2020 2:26 PM
To: Chan, Elvis M. (SF) (FBI) >
Cc: [REDACTED] >; [REDACTED]@verizonmedia.com) >
Subject: [EXTERNAL EMAIL] - Re: [E] Next FITF Meeting

Let's do the 24th at 1 PDT.

On Mon, Sep 14, 2020 at 5:21 PM Chan, Elvis M. (SF) (FBI) > wrote:

Paranoids,

Just touching base to see when you can meet for our next touch point. We will have a threat briefing on the Iranian intrusion set known as [REDACTED] or [REDACTED] I know we have one Russian-backed media site to share with you as well. The rest

is TBD. Please pick one of the remaining dates/times below. We'll only need an hour of your time. Thanks!

September 21, 10 am or 1 pm PDT

September 23, 10 am PDT

September 24, 1 pm PDT

September 25, 1 pm PDT

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

--
[Image removed by sender.]

[REDACTED]

Senior Manager
Paranoids - Advanced Cyber Threats Team

M [REDACTED]

Washington, DC 20006

Exhibit 39

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 9/29/2020 10:31:02 PM
To: [REDACTED] [REDACTED]@google.com]; [REDACTED] [REDACTED]@google.com) [REDACTED]@google.com]; [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov]; Dehmlow, Laura E. (CD) (FBI) [REDACTED]@fbi.gov]; [REDACTED] r. (M) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (CID)(FBI) [REDACTED]@fbi.gov]; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]
Subject: FITF Meeting with Google
Location: [REDACTED]
Start: 9/29/2020 10:30:00 PM
End: 9/29/2020 11:00:00 PM
Show Time As: Tentative

Recurrence: (none)

Please forward to whomever you deem appropriate. Agenda TBD.

From: [REDACTED] <[REDACTED]@google.com>
Sent: Tuesday, September 29, 2020 1:50 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] ([REDACTED]@google.com) <[REDACTED]@google.com>
Subject: [EXTERNAL EMAIL] - Re: Last FITF Meetings before Election

Hi Elvis,

If Wednesday, October 14 at 1pm pst is still available, that works for us. Thank you.

On Tue, Sep 29, 2020 at 11:04 AM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Hi [REDACTED],

Per our prior discussion, I want to put a meeting on the calendar for our last bilateral sync ahead of the election. Please let me know which of these works best for you (one hour slot). Thanks!

Monday, Oct. 12, 10 am or 1 pm PDT
 Tuesday, Oct. 13, 10 am, 12 pm, or 2 pm PDT
 Wednesday, Oct. 14, 10 am or 1 pm PDT
 Thursday, Oct. 15, 10 am PDT
 Friday, Oct. 16, 10 am or 1 pm PDT

Regards,
 Elvis

Elvis M. Chan
 Supervisory Special Agent
 Squad CY-1, National Security
 FBI San Francisco

Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Confidential - Not For Public Release

Exhibit 40

Appointment

From: Chan, Elvis M. (SF) (FBI) [redacted]@fbi.gov
To: [redacted] (CID) (FBI) [redacted]@fbi.gov; [redacted] (SF) (FBI) [redacted]@fbi.gov; [redacted] CD (FBI) [redacted]@fbi.gov; [redacted] (SF) (FBI) [redacted]@fbi.gov; [redacted] (OGC) (FBI) [redacted]@fbi.gov; [redacted] (MH) (FBI) [redacted]@fbi.gov; Dehmlow, Laura E. (CD) (FBI) [redacted]@fbi.gov; [redacted]@google.com; [redacted]@google.com; [redacted]@google.com

Subject: FITF Meeting with Google

Location: [redacted]

Start: 10/14/2020 8:00:00 PM

End: 10/14/2020 9:00:00 PM

Show Time As: Tentative

Recurrence: (none)

Please forward to whomever you deem appropriate. Agenda TBD.

From: [redacted] <[redacted]@google.com>
Sent: Tuesday, September 29, 2020 1:50 PM
To: Chan, Elvis M. (SF) (FBI) [redacted]@fbi.gov
Cc: [redacted] ([redacted]@google.com); [redacted] ([redacted]@google.com); [redacted] ([redacted]@google.com)
Subject: [EXTERNAL EMAIL] - Re: Last FITF Meetings before Election

Hi Elvis,

If Wednesday, October 14 at 1pm pst is still available, that works for us. Thank you.

On Tue, Sep 29, 2020 at 11:04 AM Chan, Elvis M. (SF) (FBI) <[redacted]@fbi.gov> wrote:
Hi [redacted],

Per our prior discussion, I want to put a meeting on the calendar for our last bilateral sync ahead of the election. Please let me know which of these works best for you (one hour slot). Thanks!

- Monday, Oct. 12, 10 am or 1 pm PDT
Tuesday, Oct. 13, 10 am, 12 pm, or 2 pm PDT
Wednesday, Oct. 14, 10 am or 1 pm PDT
Thursday, Oct. 15, 10 am PDT
Friday, Oct. 16, 10 am or 1 pm PDT

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco
Work: [redacted]
Cell: [redacted]
Email: [redacted]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Please do not edit this section of the description.

View your event at



Confidential - Not For Public Release

Exhibit 41

Appointment

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 9/29/2020 11:39:59 AM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d6915d479cd74fc99079271b15f73467 [REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b48d6f5efa9640af9d49ecb0f63fdd91 [REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7e0acc320c214954b766d69d2fd89f1e [REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4c318ea7472445b8a022fbd1355c9430 [REDACTED]]; [REDACTED] (CD) (FBI) [REDACTED]@fbi.gov; Dehmlow, Laura E. (CD) (FBI) [REDACTED]@fbi.gov; [REDACTED] (MH) (FBI) [REDACTED]@fbi.gov; [REDACTED] (OGC) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov; [REDACTED] (CID) (FBI) [REDACTED]@fbi.gov]
CC: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c7d2d77006a842be9b0761ed156a4f8d [REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=498942253314459abf7dc97533c54ab4 [REDACTED]]; [REDACTED] (TD) (FBI) [REDACTED]@FBI.GOV; [REDACTED] (CYD) (FBI) [REDACTED]@fbi.gov; [REDACTED] (SF) (FBI) [REDACTED]@fbi.gov]
Subject: FITF Meeting with LinkedIn
Location: [REDACTED] PIN [REDACTED]
Start: 10/13/2020 2:00:00 PM
End: 10/13/2020 3:00:00 PM
Show Time As: Busy
Recurrence: (none)

Please forward this invitation to whomever you deem appropriate. Agenda below:

Russia Briefing (FITF-Russia and OGA)
 China Update (FITF-China)
 Iran Briefing (FITF-Global)
 Election Command Post Status Update

From: [REDACTED] <[REDACTED]@linkedin.com>
Sent: Tuesday, September 29, 2020 11:17 AM
To: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov>
Subject: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: Last FITF Meeting before Elections

2 pm PDT Tuesday Oct 13th works for me!

[REDACTED]
 Director of Threat Prevention
 LinkedIn Trust & Safety

From: "Chan, Elvis M. (SF) (FBI)" <[REDACTED]@fbi.gov>
Date: Tuesday, September 29, 2020 at 2:08 PM
To: [REDACTED] <[REDACTED]@linkedin.com>, [REDACTED] <[REDACTED]@linkedin.com>, [REDACTED]

<[REDACTED]@linkedin.com>, [REDACTED] <[REDACTED]@linkedin.com>

Subject: Last FITF Meeting before Elections

LinkedIn folks,

Per our prior discussion, I want to put a meeting on the calendar for our last bilateral sync ahead of the election. Please let me know which of these works best for you (one hourslot). Thanks!

Monday, Oct. 12, 10 am or 1 pm PDT

Tuesday, Oct. 13, 10 am, 12 pm, or 2 pm PDT

Wednesday, Oct. 14, 10 am or 1 pm PDT

Thursday, Oct. 15, 10 am PDT

Friday, Oct. 16, 10 am or 1 pm PDT

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 42

From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting
To: [redacted] (FBI); [redacted]
Sent: October 5, 2020 9:46 PM (UTC-04:00)

[redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[redacted]

FACEBOOK

From: [redacted]
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted] [redacted] 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.

[redacted]

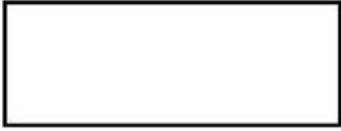
Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,
[redacted]

[redacted]



From: [redacted] (FBI)
Subject: RE: Tipper & Next FITF Meeting
To: [redacted]
Sent: October 5, 2020 10:12 PM (UTC-04:00)

From: [redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [redacted] (FBI) [redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[redacted]

For the next FITF meeting in order of preference we'd like to meet:

- 1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
- 2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
- 3. Friday Oct 16 11 am PDT / 2 pm EDT
- 4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[redacted]

FACEBOOK

From: [redacted]
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted] 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.

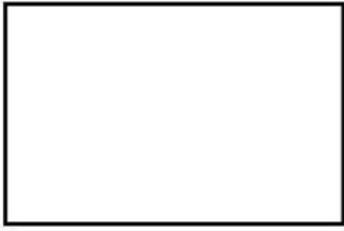
[redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,



[Redacted]

FACEBOOK

From: [Redacted]

Date: Sunday, October 4, 2020 at 2:31 PM

To: [Redacted]

Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [Redacted] 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.

[Redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,

[Redacted]

[Redacted]

[Redacted] (FBI)

Subject: RE: Tipper & Next FITF Meeting

Start: Tuesday, October 6, 2020 12:00 AM

End: Tuesday, October 6, 2020 12:30 AM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)

Required Attendees: [Redacted]

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

- 1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
- 2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
- 3. Friday Oct 16 11 am PDT / 2 pm EDT
- 4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

[Redacted]

From: [Redacted]

Date: Sunday, October 4, 2020 at 2:31 PM

To: [Redacted]

Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted]
[redacted] 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.

[redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT

Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT

Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,

[redacted]

[redacted]

[Redacted] (FBI)

Subject: FITF Meeting with Facebook
Location: [Redacted]
Start: Wednesday, October 14, 2020 1:00 PM
End: Wednesday, October 14, 2020 2:00 PM
Recurrence: (none)
Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)
Required Attendees: [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 (FBI); [Redacted] (FBI); [Redacted] (FBI)
Optional Attendees: [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI); [Redacted] (FBI);
 [Redacted]
 [Redacted] (FBI); [Redacted]
 (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [Redacted] (FBI); [Redacted]
 [Redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted] (FBI)

Subject: FITF Meeting with Facebook
Location: [Redacted]
Start: Wednesday, October 14, 2020 1:00 PM
End: Wednesday, October 14, 2020 2:00 PM
Recurrence: (none)
Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)
Required Attendees: [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 (FBI); [Redacted] (FBI); [Redacted] (FBI)
Optional Attendees: [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [Redacted]
 [Redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

From: [redacted]
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
[redacted]
Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted]
[redacted] 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.

[redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT

Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT

Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,

[redacted]

[redacted]

[redacted] (FBI)

Subject: FITF Meeting with Facebook

Location: [redacted]

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [redacted] (FBI)

Required Attendees: [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI); [redacted]
(FBI)

Optional Attendees: [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [redacted] attend if they can get information approved for sharing.

From: [redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [redacted] (FBI) [redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[redacted]

FACEBOOK

[Redacted] (FBI)

Subject: FITF Meeting with Facebook

Location: [Redacted]

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)

Required Attendees:
[Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
(FBI); [Redacted] (FBI); [Redacted] (FBI)

Optional Attendees:
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted]

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted] (FBI); [Redacted]

[Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

From: [redacted]
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
[redacted]
Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted]
[redacted] 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.

[redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,

[redacted]

[redacted]

[Redacted] (FBI)

Subject: FITF Meeting with Facebook
Location: [Redacted]
Start: Wednesday, October 14, 2020 1:00 PM
End: Wednesday, October 14, 2020 2:00 PM
Recurrence: (none)
Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)
Required Attendees: [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 [Redacted] (FBI); [Redacted] (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [Redacted] (FBI) [Redacted]
 [Redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

From: [Redacted]

Date: Sunday, October 4, 2020 at 2:31 PM

To: [Redacted]
[Redacted]

Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [Redacted]
[Redacted] 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.

[Redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,
[Redacted]

[Redacted]

[Redacted] (FBI)

Subject: FITF Meeting with Facebook

Location: [Redacted]

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)

Required Attendees:
[Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
(FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted] (FBI) [Redacted]
[Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

From: [redacted]

Date: Sunday, October 4, 2020 at 2:31 PM

To: [redacted]
[redacted]

Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted]
[redacted] 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.

[redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT
- Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,

[redacted]

[redacted]

[Redacted] (FBI)

Subject: RE: Tipper & Next FITF Meeting

Start: Tuesday, October 6, 2020 12:00 AM

End: Tuesday, October 6, 2020 12:30 AM

Recurrence: (none)

Meeting Status: Meeting organizer

Organizer: [Redacted] (FBI)

Required Attendees: [Redacted]

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted] (FBI)

[Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

- 1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
- 2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
- 3. Friday Oct 16 11 am PDT / 2 pm EDT
- 4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

From: [Redacted]

Date: Sunday, October 4, 2020 at 2:31 PM

To: [Redacted]

[Redacted]

Subject: Tipper & Next FITF Meeting

Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,



[Redacted] (FBI)

Subject: FITF Meeting with Facebook
Location: [Redacted]
Start: Wednesday, October 14, 2020 1:00 PM
End: Wednesday, October 14, 2020 2:00 PM
Recurrence: (none)
Meeting Status: Accepted

Organizer: [Redacted] (FBI)
Required Attendees: [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 (FBI)
Optional Attendees: [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [Redacted] (FBI); [Redacted]
 [Redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

[Redacted] (FBI)

Subject: FITF Meeting with Facebook

Location: [Redacted]

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Recurrence: (none)

Meeting Status: Accepted

Organizer: [Redacted] (FBI)

Required Attendees:
[Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
(FBI); [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI)

Optional Attendees:
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted]
[Redacted]

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted] (FBI); [Redacted]

[Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

[Redacted] (FBI)

Subject: FITF Meeting with Facebook

Location: [Redacted]

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Show Time As: Tentatively accepted

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: [Redacted] (FBI)

Required Attendees: [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
(FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted] (FBI) [Redacted]

[Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

[Redacted] (FBI)

Subject: FITF Meeting with Facebook

Location: [Redacted]

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Show Time As: Tentatively accepted

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: [Redacted] (FBI)

Required Attendees: [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI); [Redacted] (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]

Sent: Tuesday, October 6, 2020 1:45:34 AM

To: [Redacted] (FBI); [Redacted]

[Redacted]

Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

[Redacted] (FBI)

Subject: FITF Meeting with Facebook
Location: [Redacted]
Start: Wednesday, October 14, 2020 1:00 PM
End: Wednesday, October 14, 2020 2:00 PM
Recurrence: (none)
Meeting Status: Accepted

Organizer: [Redacted] (FBI)
Required Attendees: [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 [Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
 [Redacted] (FBI); [Redacted] (FBI); [Redacted]
 (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [Redacted] attend if they can get information approved for sharing.

From: [Redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [Redacted] (FBI) [Redacted]
 [Redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[Redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[Redacted]

FACEBOOK

[redacted] (FBI)

Subject: FITF Meeting with Facebook
Location: [redacted]
Start: Wednesday, October 14, 2020 1:00 PM
End: Wednesday, October 14, 2020 2:00 PM
Recurrence: (none)
Meeting Status: Accepted

Organizer: [redacted] (FBI)
Required Attendees: [redacted]
 [redacted] (FBI); [redacted] (FBI); [redacted]
 [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
 [redacted] (FBI); [redacted] (FBI); [redacted]
 (FBI); [redacted] (FBI); [redacted] (FBI)
Optional Attendees: [redacted] (FBI); [redacted] (FBI); [redacted]
 [redacted] (FBI); [redacted] (FBI)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [redacted] attend if they can get information approved for sharing.

From: [redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [redacted] (FBI) [redacted]
 [redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[redacted]

For the next FITF meeting in order of preference we'd like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[redacted]

FACEBOOK

From: [redacted] (FBI)
Subject: Re: Tipper & Next FITF Meeting
To: [redacted]
Sent: October 5, 2020 10:15 PM (UTC-04:00)

[redacted] - just sent all of you a calendar invite with your first choice. I'll let you know ahead of time if we have [redacted] join. If they do, they will be briefing. Thanks.

Regards,
[redacted]



From: [redacted]
Sent: Monday, October 5, 2020 06:45 PM
To: [redacted] (FBI) [redacted]
[redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[redacted]

For the next FITF meeting in order of preference we'd like to meet:

- 1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
- 2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
- 3. Friday Oct 16 11 am PDT / 2 pm EDT
- 4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[redacted]

FACEBOOK

From: [redacted]
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
[redacted]
Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted]
[redacted] 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.

[Redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT

Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT

Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,

[Redacted]

[Redacted]

From: [redacted] (FBI)
Subject: FITF Meeting with Facebook
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Sent: October 5, 2020 10:17 PM (UTC-04:00)

Please forward this invite to whoever you deem appropriate. Agenda TBD, but we may have [redacted] attend if they can get information approved for sharing.

From: [redacted]
Sent: Tuesday, October 6, 2020 1:45:34 AM
To: [redacted] (FBI); [redacted]
[redacted]
Subject: [EXTERNAL EMAIL] - Re: Tipper & Next FITF Meeting

[redacted]

For the next FITF meeting in order of preference weâ€™d like to meet:

1. Wednesday, Oct. 14 10 am PDT / 1 pm EDT
2. Wednesday Oct. 14 12 pm PDT / 3 pm EDT
3. Friday Oct 16 11 am PDT / 2 pm EDT
4. Friday, Oct. 16 12 pm PDT / 3 pm EDT

[redacted]

FACEBOOK

From: [redacted]
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
[redacted]
Subject: Tipper & Next FITF Meeting

Facebook folks,

First, I got a tip from CISA that [redacted]
[redacted] 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.

[redacted]

Second, we still don't have you locked in with our next bilateral meeting with FITF yet. Here are the remaining dates/times which are available:

- Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT
- Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT

[Redacted] (FBI)

Subject: FITF Meeting with Facebook --- UNCLASSIFIED

Location: Unclassified Teleconference

Start: Wednesday, October 14, 2020 1:00 PM

End: Wednesday, October 14, 2020 2:00 PM

Recurrence: (none)

Meeting Status: Declined

Organizer: [Redacted] (FBI)

Required Attendees: [Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI)

Optional Attendees: [Redacted] (FBI)

Classification: UNCLASSIFIED

=====

=====

Classification: UNCLASSIFIED

Wednesday, Oct. 14, 10 am, 11 am, or 12 pm PDT

Thursday, Oct. 15, 10 am, 11 am, or 12 pm PDT

Friday, Oct. 16, 11 am or 12 pm PDT

No set agenda yet, but we wanted to put something on the calendar. Please let us know if any of these work for you. Thanks!

Regards,



From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up
To: [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Sent: October 26, 2020 11:10 PM (UTC-04:00)

Thanks [redacted]

If folks are available for a call tomorrow (or an alternative day this week), let me know a preferred time.

The goal for us is to go over the referrals we sent last week and the trends we are tracking and align on any context you are able to discuss (if any).

I can send out dial-in info if needed.

[redacted]

On Oct 26, 2020, at 8:58 PM, [redacted] (FBI) [redacted] wrote:

[redacted]

Facebook ([redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,
[redacted]

[redacted]

From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted]
Sent: October 27, 2020 8:49 AM (UTC-04:00)

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]
Facebook, Inc
[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted]
"[redacted] (FBI)" <[redacted]>, "[redacted] (FBI)"
[redacted]
Cc: [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Follow Up

[redacted]

Facebook ([redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[redacted]

[redacted]

From: [redacted] (FBI)
Subject: Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted]
Sent: October 27, 2020 11:32 AM (UTC-04:00)

I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]
Facebook, Inc
[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted], [redacted] (FBI)" [redacted] (FBI)"
Cc: [redacted] (FBI)" [redacted]
Subject: Follow Up

[Redacted]

Facebook ([Redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[Redacted]

[Redacted]

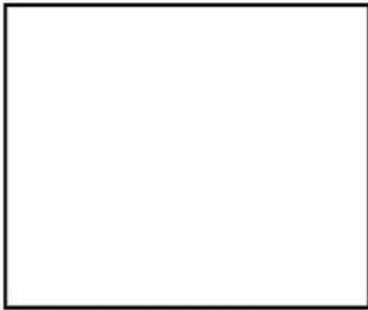
From: [redacted] (FBI)
Subject: Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI)
Sent: October 27, 2020 11:37 AM (UTC-04:00)
Alcon,

You guys can use my teleconference number whenever you want today: [redacted], pin [redacted] Thanks.

Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)

Subject: [EXTERNAL EMAIL] - Re: Follow Up
Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]

Facebook, Inc

[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[redacted] (FBI)" [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)

[Redacted]

Cc: [Redacted] (FBI)" [Redacted]

[Redacted] (FBI)" [Redacted]

Subject: Follow Up

[Redacted]

Facebook ([Redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[Redacted]

[Redacted]

From: [redacted] (FBI)
Subject: Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI)
Sent: October 27, 2020 11:37 AM (UTC-04:00)
Alcon,

You guys can use my teleconference number whenever you want today: [redacted], pin [redacted] Thanks.

Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]

Facebook, Inc
[redacted](cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted],
[redacted] (FBI)" [redacted] (FBI)"
[redacted]
Cc: [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Follow Up

[redacted],

Facebook ([redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,
[redacted]

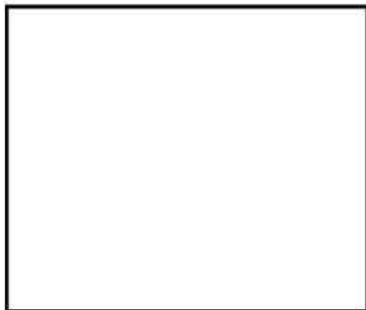
[redacted]

From: [redacted] (FBI)
Subject: Re: Follow Up
To: [redacted] (FBI)
Sent: October 27, 2020 11:37 AM (UTC-04:00)
[redacted] - use the host pin [redacted]

Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
[redacted]
Cc: [redacted] (FBI); [redacted] (FBI); [redacted]
[redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]
Facebook, Inc
[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]

Date: Monday, October 26, 2020 at 8:58 PM

To: "[redacted] (FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted] (FBI)"

Cc: [redacted] (FBI)" [redacted]

[redacted] (FBI)" [redacted]

Subject: Follow Up

[redacted],

Facebook ([redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[redacted]

[redacted]

From: [redacted] (FBI)
Subject: Re: Follow Up
To: [redacted] (FBI)
Sent: October 27, 2020 11:41 AM (UTC-04:00)

Thanks!



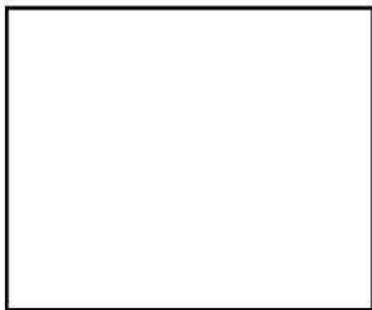
From: [redacted] (FBI) [redacted]
Sent: Tuesday, October 27, 2020 11:37 AM
To: [redacted] (FBI) [redacted]
Subject: Re: Follow Up

[redacted] - use the host pin [redacted]

Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI) [redacted] (FBI) [redacted] (FBI) [redacted] (FBI)
[redacted] (FBI) [redacted] (FBI) [redacted] (FBI)
Cc: [redacted] (FBI) [redacted] (FBI) [redacted]
[redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to cha as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]
Facebook, Inc
[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted] (FBI)"
[redacted]
Cc: [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Follow Up

[redacted]

Facebook ([redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[redacted]

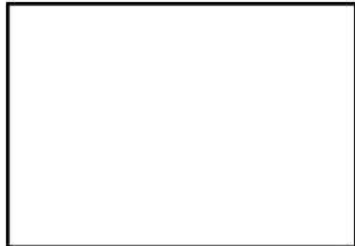
[redacted]

From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI)
Sent: October 27, 2020 11:50 AM (UTC-04:00)

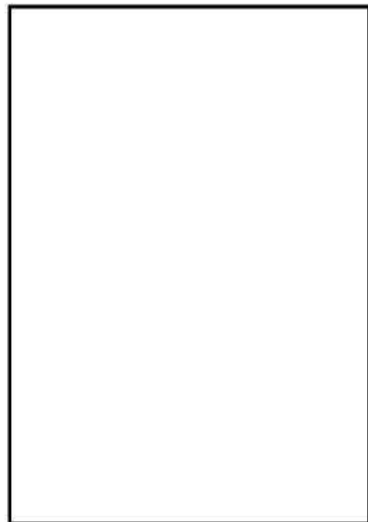
Thanks, [redacted]
[redacted] | Facebook
Associate General Counsel
575 7th St. NW, Washington, DC 20004
[redacted]

From: "[redacted] (FBI)" [redacted]
Date: Tuesday, October 27, 2020 at 11:36 AM
To: "[redacted] (FBI)" [redacted]
(FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Cc: [redacted]
[redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Re: Follow Up

Alcon,
You guys can use my teleconference number whenever you want today: [redacted] Thanks.
Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI) [redacted] (FBI) [redacted]
[redacted] (FBI) [redacted] (FBI) [redacted] (FBI)

[redacted]
Cc: [redacted] (FBI) [redacted] (FBI) [redacted]

[redacted]
[redacted]

Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]

Facebook, Inc

[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]

Date: Monday, October 26, 2020 at 8:58 PM

To: "[redacted] (FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted] (FBI)"

[redacted]

Cc: [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]

Subject: Follow Up

[redacted]

Facebook ([redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[redacted]



From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI)
Sent: October 27, 2020 11:50 AM (UTC-04:00)

Thanks, [redacted]

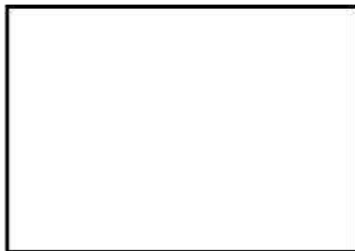
[redacted] | Facebook
Associate General Counsel
575 7th St. NW, Washington, DC 20004
[redacted]

From: "[redacted] (FBI)" [redacted]
Date: Tuesday, October 27, 2020 at 11:36 AM
To: "[redacted] (FBI)" [redacted]
(FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Cc: [redacted]
[redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Re: Follow Up

Alcon,

You guys can use my teleconference number whenever you want today: [redacted], pin [redacted]. Thanks.

Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...





From: [Redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [Redacted] (FBI) [Redacted] (FBI) [Redacted] (FBI) [Redacted] (FBI)
Cc: [Redacted] (FBI) [Redacted] (FBI) [Redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [Redacted] and I connected on the phone briefly this morning and thought it might be a good idea to cha as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [Redacted] prefers to set up the call.

Thanks,

[Redacted]

[Redacted]
 Facebook, Inc
 [Redacted] (cell/WhatsApp)

From: "[Redacted] (FBI)" [Redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[Redacted] (FBI)" [Redacted] (FBI)" [Redacted] (FBI)" [Redacted] (FBI)"
Cc: [Redacted] (FBI)" [Redacted]
Subject: Follow Up

[Redacted],

Facebook ([Redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[Redacted]





From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI)
Sent: October 27, 2020 11:54 AM (UTC-04:00)

Great, I'll send a calendar invite momentarily for those able to joint at 4 p.m. EST with [redacted] dial in info.

[redacted]

From: [redacted]
Date: Tuesday, October 27, 2020 at 11:49 AM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted] (FBI)" [redacted]
Cc: [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Re: Follow Up

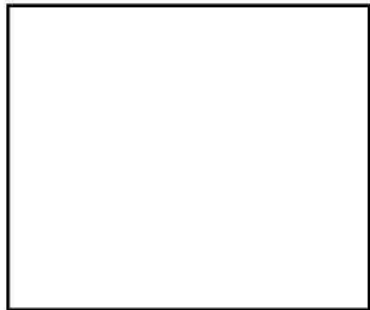
Thanks, [redacted].
[redacted] | Facebook
Associate General Counsel
575 7th St. NW, Washington, DC 20004
[redacted]

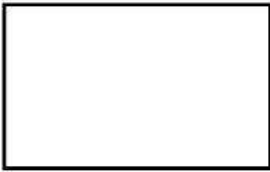
From: "[redacted] (FBI)" [redacted]
Date: Tuesday, October 27, 2020 at 11:36 AM
To: "[redacted] (FBI)" [redacted]
(FBI)" [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Cc: [redacted]
[redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]

Subject: Re: Follow Up
Alcon,
You guys can use my teleconference number whenever you want today: [redacted], pin [redacted]. Thanks.
Regards,



On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...





From: [Redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [Redacted] (FBI) [Redacted]
 [Redacted] (FBI) [Redacted] (FBI) [Redacted] (FBI)
Cc: [Redacted] (FBI) [Redacted] (FBI) [Redacted]

Subject: [EXTERNAL EMAIL] - Re: Follow Up
 Good morning all. [Redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [Redacted] prefers to set up the call.

Thanks,

[Redacted]

[Redacted]

Facebook, Inc

[Redacted] (cell/WhatsApp)

From: "[Redacted] (FBI)" [Redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[Redacted] (FBI)" [Redacted] (FBI)" [Redacted],
 [Redacted] (FBI)" [Redacted] (FBI)"
Cc: [Redacted] (FBI)" [Redacted]
 [Redacted] (FBI)" [Redacted]

Subject: Follow Up

[Redacted],

Facebook ([Redacted] cc'd above) would like to circle up with you to discuss the recent referrals provided regarding the threat you work. Please let them know your availability. Thanks!

Regards,

[Redacted]



From: [redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI);
[redacted] (FBI); [redacted] (FBI)
Cc: [redacted] (FBI); [redacted] (FBI)
Sent: October 27, 2020 11:54 AM (UTC-04:00)

Great, I'll send a calendar invite momentarily for those able to joint at 4 p.m. EST with [redacted] dial in info.

[redacted]

From: [redacted]
Date: Tuesday, October 27, 2020 at 11:49 AM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted] (FBI)"
[redacted] (FBI)" [redacted] (FBI)"
Cc: [redacted] (FBI)"
[redacted] (FBI)"
Subject: Re: Follow Up

Thanks, [redacted].

[redacted] | Facebook
Associate General Counsel
575 7th St. NW, Washington, DC 20004
[redacted]

From: "[redacted] (FBI)" [redacted]
Date: Tuesday, October 27, 2020 at 11:36 AM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted] (FBI)"
[redacted] (FBI)" [redacted] (FBI)"
Cc: [redacted] (FBI)" [redacted] (FBI)"
[redacted] (FBI)" [redacted] (FBI)"
Subject: Re: Follow Up

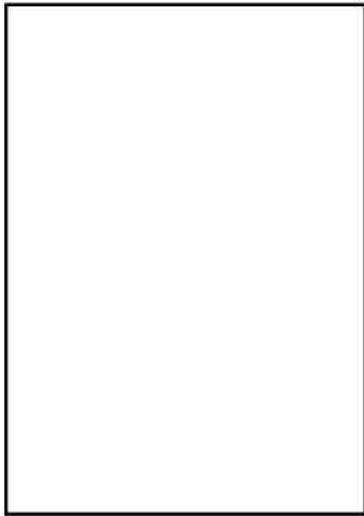
Alcon,

You guys can use my teleconference number whenever you want today: [redacted], pin [redacted]. Thanks.

Regards,

[redacted]

On Oct 27, 2020 8:32 AM, "[redacted] (FBI)" [redacted] wrote:
I think that works for most of us. I'll defer to [redacted] on the call in...



From: [redacted]
Sent: Tuesday, October 27, 2020 8:48 AM
To: [redacted] (FBI) [redacted] (FBI) [redacted] (FBI) [redacted] (FBI)
[redacted] (FBI) [redacted] (FBI) [redacted] (FBI)
Cc: [redacted] (FBI) [redacted] (FBI) [redacted]
[redacted]
Subject: [EXTERNAL EMAIL] - Re: Follow Up

Good morning all. [redacted] and I connected on the phone briefly this morning and thought it might be a good idea to chat as a group today if possible. Would 4 p.m. EST work for folks? Please feel free to let me know a different time, or let me know if today doesn't work. I can send out dial in information unless [redacted] prefers to set up the call.

Thanks,

[redacted]

[redacted]
Facebook, Inc
[redacted] (cell/WhatsApp)

From: "[redacted] (FBI)" [redacted]
Date: Monday, October 26, 2020 at 8:58 PM
To: "[redacted] (FBI)" [redacted] (FBI)" [redacted] (FBI)"
[redacted] (FBI)" [redacted] (FBI)"
Cc: [redacted] (FBI)" [redacted]
[redacted] (FBI)" [redacted]
Subject: Follow Up

[Redacted]

Subject: Sync on FB referrals
Start: Tuesday, October 27, 2020 4:00 PM
End: Tuesday, October 27, 2020 4:30 PM
Show Time As: Tentatively accepted

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: [Redacted]

Required Attendees: [Redacted]
[Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI)

Optional Attendees: [Redacted] (FBI)

Dial-in info:

[Redacted] pin [Redacted]

Ways to join

?? Computer or Mobile:

[Redacted]

?? Facebook Conference Room and Portal:

Use the touch panel to enter the join code [Redacted]

? Telephone:

Dial in on [Redacted] or find an alternative number then enter [Redacted]

Enabled by OneVC

[Redacted]

Subject: Sync on FB referrals
Start: Tuesday, October 27, 2020 4:00 PM
End: Tuesday, October 27, 2020 4:30 PM

Recurrence: (none)

Meeting Status: Accepted

Organizer: [Redacted]

Required Attendees:
[Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted]
[Redacted] (FBI); [Redacted] (FBI); [Redacted] (FBI);
[Redacted] (FBI)

Optional Attendees: [Redacted] (FBI)

Dial-in info:

[Redacted], pin [Redacted]

Ways to join

?? Computer or Mobile:

[Redacted]

?? Facebook Conference Room and Portal:

Use the touch panel to enter the join code [Redacted]

? Telephone:

Dial in on [Redacted] or find an alternative number then enter [Redacted]

Enabled by OneVC

Exhibit 43

>I called [REDACTED] about it this am, was the first he heard about it

[REDACTED] (10/14/2020 10:07:37 PDT):

>But we should ask.

[REDACTED] (10/14/2020 10:09:06 PDT):

>do they have any plans to proactively disclose this to the public?

[REDACTED] (10/14/2020 10:14:26 PDT):

>thanks for rephrasing more eloquently [REDACTED]

[REDACTED] (10/14/2020 10:15:30 PDT):

>[REDACTED] -- are we going to pass this in writing later?

[REDACTED] (10/14/2020 10:15:36 PDT):

>yes

[REDACTED] (10/14/2020 10:23:01 PDT):

>thanks [REDACTED]

[REDACTED] (10/14/2020 10:24:15 PDT):

>Was IR info this passed last night?

[REDACTED] (10/14/2020 10:25:59 PDT):

>This came in last week I think

[REDACTED] (10/14/2020 10:26:23 PDT):

>I'm just waiting for the #flyinmyhair intel

[REDACTED] (10/14/2020 10:27:20 PDT):

>The stuff that came in last night on IR was related to domains, correct [REDACTED]?

[REDACTED] (10/14/2020 10:27:29 PDT):

>Yep

[REDACTED] (10/14/2020 10:27:32 PDT):

>Plus some of this hashtag stuff

[REDACTED] (10/14/2020 10:27:39 PDT):

>Some of which were duplicates of previous domains?

[REDACTED] (10/14/2020 10:28:03 PDT):

>3/4 were dupes

[REDACTED] (10/14/2020 10:28:15 PDT):

>We should let them know

[REDACTED] (10/14/2020 10:31:48 PDT):

>[REDACTED] - do we want to go back to Sandworm and update on recent search patterns? And also ask if our recent share was helpful?

[REDACTED] (10/14/2020 10:33:39 PDT):

>probably not on search, ok with me if we want to ask if it was helpful

[REDACTED] (10/14/2020 10:34:57 PDT):

>[REDACTED] are you on and anything to add to this?

[REDACTED] (10/14/2020 10:35:07 PDT):

>re: referrals

[REDACTED] (10/14/2020 10:35:25 PDT):

>I'm not. [REDACTED] is handling this one for outreach.

[REDACTED] (10/14/2020 10:35:43 PDT):

>I can talk about it but its inside baseball

[REDACTED] (10/14/2020 10:40:57 PDT):

>Any issues anyone else wants to raise?

[REDACTED] (10/14/2020 10:47:59 PDT):

>Thanks all.

[REDACTED] (10/14/2020 10:49:21 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 10:56:09 PDT):
>FYSA it appears [REDACTED] at Bellingcat is able to see the name of the FBI agent working on the case through the awful redacting job of NYPost: [https://twitter.com/\[REDACTED\]/status/1316414276765208577?s=20](https://twitter.com/[REDACTED]/status/1316414276765208577?s=20)

[REDACTED] (10/14/2020 10:58:03 PDT):
>dumb question

[REDACTED] (10/14/2020 10:58:36 PDT):
>does that mean NYPost got this from FBI/DOJ?

[REDACTED] (10/14/2020 11:00:40 PDT):
>[REDACTED] (granted, not the most credible source but probably feeding the narrative) says Giuliani and Bannon turned it over to both the FBI and NY Post

[REDACTED] (10/14/2020 11:00:52 PDT):
>Not necessarily. You have to leave a copy of the warrant and a receipt for what is seized when executing a warrant

[REDACTED] (10/14/2020 11:01:13 PDT):
>could also be the reporter taking notes on the back of the doc before scanning it

[REDACTED] (10/14/2020 11:15:32 PDT):
>I have a call in to the Supervisor in the Wilmington RA to ask about this. I'll update here after I talk to him.

Exhibit 44

Filing and Security



Primary Case:

[Redacted]

Case Title:

[Redacted]

Serial Number: 9

Serialized: 08/27/2020

Category: Assessment

Initiated: 05/16/2018

Set to Expire: 08/14/2018

Additional Case:

[Redacted]

Case Title:

[Redacted]

Serial Number: 19

Serialized: 06/09/2021

Reference Documents:

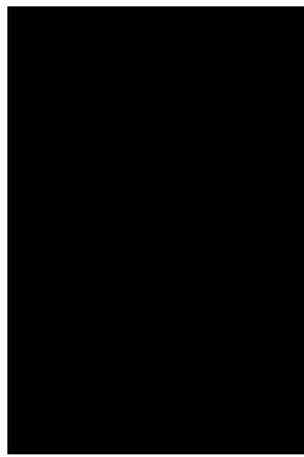
[Redacted]

[Redacted]

Referenced By:

[Redacted]

[Redacted]

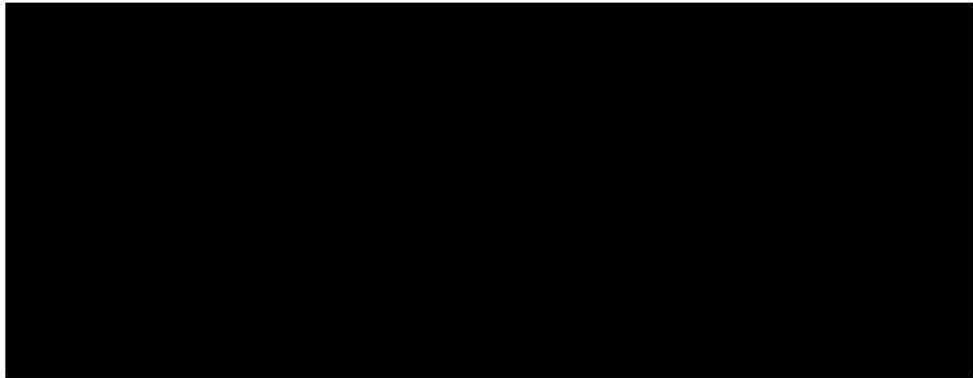


Details



Document Title: (U//FOUO) August 2020 Social Media and Technology Company Insights

Synopsis:



Administrative Notes: (U//FOUO) Warning: The private sector companies described in this document provided information to the FBI with the understanding that it would be shared with the USIC and with FVEY partners to further our collective understanding of the threat posed by malign foreign influence actors. Any further dissemination outside of intelligence channels, to include but not limited to dissemination for law enforcement purposes, must be made through the FITF at FBI Headquarters. Any reproduction, dissemination, or communication (including, but not limited to, oral briefings) of this information must be accompanied by a statement of these restrictions.

Details: (U//FOUO)

(U//FOUO) In August 2020, the FBI and National Security Agency conducted teleconference **meetings** with Facebook, LinkedIn, Google, Reddit, Verizon Media, and Twitter.

(U//FOUO) The attached Letterhead Memorandum was disseminated on or about 26 August 2020 to the Election Threats Executives within the US Intelligence Community, as follows:



[REDACTED]

Central Intelligence Agency

[REDACTED]

[REDACTED]

Department of Defense (OSD-P)

[REDACTED]

[REDACTED]

Department of Homeland Security (CISA)

[REDACTED]

[REDACTED]

Department of Homeland Security (I&A)

[REDACTED]

[REDACTED]

Department of Justice (NSD)

[REDACTED]

[REDACTED]

Department of State (INR)

[REDACTED]

[REDACTED]

Department of Treasury

[REDACTED]

[REDACTED]

National Security Agency

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

US CYBERCOM

[Redacted]

[Redacted]

[Redacted]



Package 1A7

Summary: (U//FOUO) August 2020 Social Media and Technology Company Insights
Acquired By: [Redacted]

Acquired On: 08/26/2020
Receipt Given: No

Attachments:

[Redacted]

[Redacted]



[Redacted]

[Redacted]



Intelligence Value: No Intelligence Value
Potential IIR/SIR? No
Sentinel Tags: No Sentinel Tags Selected

[Redacted]

[Redacted]

[Redacted]

Can you identify the source of this information? No

Routing



From: [Redacted]
Drafted By: [Redacted]
Approved By: [Redacted]
A/ASC Laura E Dehmlow [Redacted]

[Redacted]

UNCLASSIFIED//FOUO

Filing and Security



Primary Case: [Redacted]

Case Title: (U//FOUO) PCIU
Unrestricted Intelligence
Briefing and Liaison
Matters

Serial Number: [Redacted]
Serialized: [Redacted]
Initiated: [Redacted]

Additional Case: [Redacted]

Case Title: (U) DOCUMENT
CONTACTS MADE BY
SQUAD CY1
MAINTAINED BY CY-1

Serial Number: [Redacted]
Serialized: [Redacted]

Interaction (Assistance/Dissemination/Liaison)



Document Title: (U//FOUO) To document FBI CID PCCRIU portion of FITF meeting with Social Media Companies

Interaction Type: Liaison/Tripwire with Organization Outside the FBI
Responsible Division: CRIMINAL INVESTIGATIVE
Type of Contact: Telephone on 10/16/2020

Liaison Details: (U//FOUO) Between 13 October 2020 and 16 October 2020, FBI SF SSA [Redacted] hosted a series of teleconferences with representatives from San Francisco (SF), the Foreign Influence Task Force (FITF), FBI CID PCCRIU and representatives from Facebook, Google, LinkedIn, Reddit, Verizon Media, and Twitter. The purpose of the meetings was to provide an update on foreign influence and election related matters.

During the CID portion of the call, IA [Redacted] highlighted the recent Spanish FBI press release concerning election security. IA [Redacted] also emphasized the FBI's interest in any content relating to voter suppression. Particularly, content intended to frustrate a voters ability to vote by confusing them about the time, manner, or place of voting.

Liaison Event: Meeting
Event Role: (None Specified)
Audience Type: (None Specified)
Initiative Type: (None Specified)
Total Attendees: 14



Indexing



No Entities to display.

Intelligence



Intelligence Value: No Intelligence Value
Potential IIR/SIR? No
Sentinel Tags: *No Sentinel Tags Selected*

Can you identify the source of this information? No

Routing



Drafted By:
Approved By:



Filing and Security



Primary Case: [REDACTED]

Case Title: (U//FOUO) SUMMER SPACE; Malign Foreign Influence

Serial Number: [REDACTED]

Serialized: [REDACTED]

Category: [REDACTED]
Initiated: [REDACTED]

Additional Case: [REDACTED]

Case Title: [REDACTED]

Serial Number: [REDACTED]
Serialized: [REDACTED]

Legal Caveats: Trade Secrets and Other Confidential Proprietary Information

Details



Document Title: (U//FOUO) Meeting with Social Media and Tech Companies 02/10/2020 - 02/13/2020

Synopsis: (U//FOUO) To summarize meetings with social media and technology companies to discuss the foreign influence and election security matters.

Details: (U//FOUO)
(U) BACKGROUND

(U//FOUO) Beginning in around June 2014, the Internet Research Agency and subsequent companies known as Glavset LLC, MediaSintez LLC, MixInfo LLC, Azimut LLC, and NovInfo LLC conspired to defraud the U.S. by impairing, obstructing, and defeating the lawful functions of the Federal Election Commission, the



U.S. Department of Justice, and the U.S. Department of State in administering federal requirements for disclosure of foreign involvement in certain domestic activities. On February 16, 2018, a Federal Grand Jury in the District of Columbia granted an indictment on 13 Russian nationals and 3 companies, charging these entities and individuals with violation of multiple Federal Statutes.

(U//FOUO) On 02/10/2020, writer traveled to San Francisco AOR with members of the Foreign Influence Task Force (FITF)(UC [REDACTED], IA [REDACTED], IA [REDACTED], AGC [REDACTED] to meet with San Francisco Field Office (SSA E [REDACTED], IA [REDACTED], IA [REDACTED]) and engage with representatives from **social media** and technology companies. Writer's specific role was to provide an updated threat briefing on IRA activity. Talking points cleared by **FITF** are attached to this EC. DOJ Trial Attorney [REDACTED] also attended the **meetings** to provide a briefing regarding election crimes.

(U) MEETING SCHEDULE

(U//FOUO) Writer, along with aforementioned government representatives, met with the following companies:

1. Google (02/10/2020)
2. Twitter (02/11/2020)
3. Twilio (02/11/2020)
4. Linked In (02/11/2020)
5. Verizon **Media** (02/12/2020)
6. Reddit (02/12/2020)
7. Pinterest (02/12/2020)
8. OpenAI (02/13/2020)
9. Automatic (owners of WordPress and Tumblr) (02/13/2020)

(U//FOUO) Writer's portion of the meeting focused on four main points:

1. African organizations linked to IRA.

- a. Writer advised the FBI has high confidence leadership of Eliminating Barriers for the Liberation of Africa (EBLA), located in Ghana, is knowingly coordinating activity with IRA, to include advertising for a coordinator position in Charleston, SC on Linked In and other job advertising sites.
 - i. Verizon **Media** advised the Ghanaian connection is interesting because they saw some Ghanaian accounts and activity related to the 2016 election and provided that information to the Special Counsel's Office.
 - ii. Linked In thanked the FBI for the information since the ad was on its platform.

2. Concentration of IP infrastructure related to IRA - Africa activity.

3. Data Analysis of broader suspected IRA activity focused on IPs.

4. Purchasing of compromised social media accounts through websites.

- a. Twitter advised it is aware of the practice of compromised accounts sold by third party websites but mainly for criminal purposes or pornography.

Twitter also advised it is harder to detect compromised accounts versus inauthentic aged accounts IRA has used in the past. Twitter believes IRA continues to move away from aging accounts to develop a following and instead is using groups on platforms to push disinformation.

- b. Verizon Media is aware of compromised email accounts used to back stop disinformation campaigns and that purchased accounts makes sense when used for disinformation.


1A/1C Packages



Package 1A352

Summary: (U//FOUO) Cleared Talking Points
Acquired By: [REDACTED]

Acquired On: 02/10/2020
Receipt Given: No

Attachments:  **UNCLASSIFIED//FOUO**
 (U//FOUO) SF talking points.docx
 /LavenderService/resources/Documents/190688694/Attachments/54951633?
 fileName=SF%20talking%20points.docx (14 kb)
 (U//FOUO) Cleared talking points
 Legal Return: No
 Digital Record
[Show Attachment Preview '#'](#)

Indexing



No Entities to display.

Intelligence



Intelligence Value: Potential Intelligence Value
Potential IIR/SIR? Yes
Sentinel Tags: [REDACTED]

Can you identify the source of this information? No

[REDACTED] ID: [REDACTED]

Precedence: Routine
Assigned: Monday, March 16 2020 at 9:59 AM
Completed: Monday, March 16 2020 at 9:59 AM

Closure Codes: Reports - Contains Operation Information

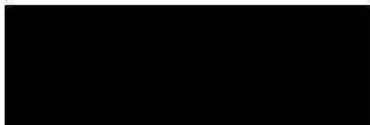
Final Report 1263

+ Show Activity Log

Routing



From:
Drafted By:
Approved By:



Filing and Security



Primary Case
Serial Number

Serialized
Category
Initiated

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title

Additional Case
Serial Number
Serialized

Case Title



Referenced By



Legal Caveats Trade Secrets and Other Confidential Proprietary Information

Details



Document Title (U//FOUO) FITF Meeting with Twitter on 10/14/2020

Synopsis (U//FOUO) To document FBI San Francisco and Foreign Influence Task Force meeting with Twitter on 10/14/2020.

Details

(U) BACKGROUND



(U//FOUO) Beginning in June 2014, the Internet Research Agency and subsequent companies known as Glavset LLC, MediaSintez LLC, MixInfo LLC, Azimut LLC, and NovInfo LLC conspired to defraud the U.S. by impairing, obstructing, and defeating the lawful functions of the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State in administering federal requirements for disclosure of foreign involvement in certain domestic activities. On February 16, 2018, a Federal Grand Jury in the District of Columbia granted an indictment on 13 Russian nationals and 3 companies, charging these entities and individuals with violation of multiple Federal Statutes. San Francisco is one of three FBI field offices, along with Washington Field and New York, to investigate the Internet Research Agency (IRA) and Project Lakhta.

(U) CURRENT SITUATION

(U//FOUO) San Francisco leads engagement with and has been the conduit to Silicon Valley technology companies for all other field offices, the Foreign Influence Task Force (FITF), and other U.S. Intelligence Community agencies pertaining to U.S. election protection, advanced persistent threats, and countering foreign influence activities.

(U) MEETING SUMMARY

(U//FOUO) On 10/14/2020, SSA [redacted] hosted a teleconference with representatives from San Francisco (SF), the Foreign Influence Task Force (FITF), Cyber Division (CyD), Criminal Investigative Division (CID), National Security Agency, and Twitter. Representatives from Twitter included [redacted] Director of Law Enforcement, Yoel Roth, Head of Site Integrity, [redacted] Security Counsel, [redacted] Threat Analyst, and [redacted], Global Legal Policy Director.

(U) The purpose of the meeting was a periodic information sharing touch point. The meeting summary follows:



(U//FOUO) [redacted] and [redacted] provided an overview of new information about the IRA. SSA [redacted] provided an update on Sandworm.

(U) Mr. Roth indicated the Sandworm accounts provided by the FBI were already suspended two months ago for terms of service violations (see referenced serial).

(U//FOUO) UC Laura Dehmlow provided a status update on Chinese influence activities, to include a discussion of Spamaflouge Dragon.

(U) Mr. Roth indicated the list of Chinese organizations provided by the FBI (see referenced serial) were reviewed, but their activities are not considered terms of service violations.

(U//FOUO) SSA [redacted] provided a status update on Iranian influence activities. SA [redacted] provided an overview of their recent seizure of over 90 Iran-affiliated websites.

(U) Mr. Roth said the recent account takedown mentioned in the recent Stanford Internet Observatory report was based on information previously provided by the FBI. They attributed these accounts to Charming Kitten because of their behavior, such as tweeting about social justice and racial issues like Black Lives Matters.

(U//FOUO) The group confirmed using the Signal platform for information sharing between the FBI and the social media companies. FBI San Francisco and Twitter will use pre-established channels for one-to-one communications.

Indexing

Display Name	Enterprise Role	Entity Role	Entity Type	US Person
[redacted]	ENTERPRISE INDEX	Reference	PERSON	Unknown
[redacted]	LIAISON	Reference	PERSON	Unknown
Yoel Roth	LIAISON	Reference	PERSON	Unknown
[redacted]	LIAISON	Reference	PERSON	Unknown
[redacted]	LIAISON	Reference	PERSON	Yes
[redacted]	ENTERPRISE INDEX	Reference	PERSON	Unknown
[redacted]	LIAISON	Reference	PERSON	Unknown

1 - 7 of 7 Entities

Accomplishments

Accomplishment Interview or requested information from the public or private entities

Claimant [redacted]

Date 10/14/2020

Interview Type Interview

Interviewees Liaison Partner

Location of Investigative Method United States (50 States and D.C.)

Task Force None

Intelligence

Intelligence Value Potential Intelligence Value

Potential IIR/SIR? Yes



Sentinel Tags [redacted]

Can you identify the source of this information? No

ID 10291947
Precedence Routine
Assigned Wednesday, October 21 2020 at 9:06 PM
Completed Wednesday, October 21 2020 at 9:07 PM
Closure Codes Tactical - Administrative information, Reports - Does not meet DETA LED threshold

[+ Show Activity Log](#)

Routing

From CYBER, DM-ECOU-2
Drafted By [Redacted] 
Approved By ASAC [Redacted] 
Distribution [Redacted]

Filing and Security

Primary Case

[Redacted]

Case Title

[Redacted]

Serial Number

Serialized

Category Initiated

[Redacted]

Reference Documents

[Redacted]

Details

Document Title (U//FOUO) October 12th 2020 Facebook Takedown

Synopsis (U//FOUO) To detail the September and October 2020 Facebook Takedown of GRU Unit 54777 Influence Operations

Details (U//FOUO)

(U) BACKGROUND

[Redacted]

(U//FOUO) Beginning in around June 2014, the Internet Research Agency and subsequent companies known as Glavset LLC, MediaSintez LLC, MixInfo LLC, Azimut LLC, and NovInfo LLC conspired to defraud the U.S. by impairing, obstructing, and defeating the lawful functions of the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State in administrating federal requirements for disclosure of foreign involvement in certain domestic activities. On February 16, 2018, a Federal Grand Jury in the District of Columbia granted an indictment on 13 Russian nationals and 3 companies, charging these entities and individuals with violation of multiple Federal Statutes.

(U) CURRENT SITUATION

(U//FOUO) San Francisco leads engagement with and has been the conduit to Silicon Valley technology companies for all RAVEN REIGN and Internet Research Agency designated offices, the Foreign Influence Task Force (FITF), and other U.S. Intelligence Community agencies pertaining to U.S. election protection and countering foreign influence activities.

(U//FOUO) As a result of ongoing FITF coordination through FBI San Francisco, between September 24th 2020 and October 12th 2020, Facebook identified and removed 224 Facebook users, 35 Pages, 18 Groups and 34 Instagram accounts for violating Facebook's policy against foreign or government interference which is coordinated inauthentic behavior on behalf of a foreign or government entity. Prior to action being taken, Facebook provided notice to FBI including the list of affected accounts, pages, and groups.

(U//FOUO) Attached in Digital 1A is an updated copy of Facebook's announcement of this action and a copy of the tipper information provided by Facebook on September 22nd 2020.

1A/1C Packages

Package 1A18

Summary (U//FOUO) Facebook Indicators and takedown notification

Acquired By

[Redacted]

Acquired On 10/12/2020
Receipt Given No

Attachments



UNCLASSIFIED//FOUO
(U//FOUO) 20200922_PX-PG_Facebook_Data.txt
/LavenderService/resources/Documents/195029628/Attachments/251836329?fileName=20200922_PX-PG_Facebook_Data.txt (8 kb)
(U//FOUO) Facebook Indicators and takedown notification
Legal Return: No
Digital Record
Show Attachment Preview #



UNCLASSIFIED//FOUO
(U//FOUO) Facebook_Takedown.pdf /LavenderService/resources/Documents/195029628/Attachments/251836237?fileName=Facebook_Takedown.pdf (257 kb)
(U//FOUO) Facebook Indicators and takedown notification
Legal Return: No
Digital Record
Show Attachment Preview #

Indexing

Display Name	Enterprise Role	Entity Role	Entity Type	US Person
72nd Special Service Center (Ts	ENTERPRISE INDEX	Main,Reference	ORGANIZATION	No

1 - 1 of 1 Entities

Accomplishments

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [Redacted]
 Claimant [Redacted]
 Date 10/12/2020
 Organization Name [Redacted]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [Redacted]
 Claimant [Redacted]
 Date 10/12/2020
 Organization Name [Redacted]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [Redacted]

Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]

Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [Redacted]
Claimant [Redacted]
Date 10/12/2020
Organization Name [Redacted]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [Redacted]
Claimant [Redacted]
Date 10/12/2020
Organization Name [Redacted]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [Redacted]
Claimant [Redacted]
Date 10/12/2020
Organization Name [Redacted]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [Redacted]
Claimant [Redacted]
Date 10/12/2020
Organization Name [Redacted]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [Redacted]
Claimant [Redacted]
Date 10/12/2020
Organization Name [Redacted]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]



Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International
 Organization Type Foreign Intelligence Service (FIS)
 Task Force PG PITTSBURGH CYBER TASK FORCE
 Technical Source Coverage No

Accomplishment *Disrupt*
 Agency or Country Designation FBI and Task Force
 Assists [REDACTED]
 Claimant [REDACTED]
 Date 10/12/2020
 Organization Name [REDACTED]
 Organization Scope International

Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]
Claimant [REDACTED]
Date 10/12/2020
Organization Name [REDACTED]
Organization Scope International
Organization Type Foreign Intelligence Service (FIS)
Task Force PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage No

Accomplishment *Disrupt*
Agency or Country Designation FBI and Task Force
Assists [REDACTED]

Claimant	[REDACTED]
Date	10/12/2020
Organization Name	[REDACTED]
Organization Scope	International
Organization Type	Foreign Intelligence Service (FIS)
Task Force	PG PITTSBURGH CYBER TASK FORCE
Technical Source Coverage	No

Intelligence



Intelligence Value	No Intelligence Value
Potential IIR/SIR?	No
Sentinel Tags	[REDACTED]

Can you identify the source of this information? No

Routing



From	PITTSBURGH, [REDACTED]
Drafted By	[REDACTED]
Approved By	[REDACTED]

Exhibit 45

Appointment

From: [Redacted - Privacy]@fb.com]

To: [Redacted - Privacy]@microsoft.com; [Redacted - Privacy]@microsoft.com]; [Redacted - Privacy]@fb.com];
 [Redacted - Privacy]@reddit.com; [Redacted - Privacy]@reddit.com]; [Redacted - Privacy]@yahooinc.com; [Redacted - Privacy]@linkedin.com
 [Redacted - Privacy]@linkedin.com]; [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@twitter.com; [Redacted - Privacy]@twitter.com];
 [Redacted - Privacy]@twitter.com; [Redacted - Privacy]@twitter.com]; [Redacted - Privacy]@yahooinc.com; [Redacted - Privacy]@
 [Redacted - Privacy]@microsoft.com]; [Redacted - Privacy]@reddit.com; [Redacted - Privacy]@reddit.com]; [Redacted - Privacy]@
 [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@reddit.com; [Redacted - Privacy]@reddit.com]; [Redacted - Privacy]@fb.com];
 [Redacted - Privacy]@wikimedia.org; [Redacted - Privacy]@wikimedia.org]; [Redacted - Privacy]@cisa.dhs.gov];
 [Redacted - Privacy]@twitter.com; [Redacted - Privacy]@twitter.com]; [Redacted - Privacy]@microsoft.com; [Redacted - Privacy]@microsoft.com];
 [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@google.com; [Redacted - Privacy]@google.com];
 [Redacted - Privacy]@microsoft.com; [Redacted - Privacy]@microsoft.com]; [Redacted - Privacy]@cisa.dhs.gov];
 hwc@google.com; [Redacted - Privacy]@twitter.com]; [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@
 [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@fb.com];
 [Redacted - Privacy]@cisa.dhs.gov]; [Redacted - Privacy]@twitter.com; [Redacted - Privacy]@twitter.com]; [Redacted - Privacy]@microsoft.com
 [Redacted - Privacy]@microsoft.com]; [Redacted - Privacy]@twitter.com; [Redacted - Privacy]@twitter.com]; [Redacted - Privacy]@google.com
 [Redacted - Privacy]@google.com]; [Redacted - Privacy]@pinterest.com; [Redacted - Privacy]@pinterest.com]; [Redacted - Privacy]@linkedin.com
 [Redacted - Privacy]@linkedin.com]; [Redacted - Privacy]@twitter.com; [Redacted - Privacy]@twitter.com]; [Redacted - Privacy]@pinterest.com
 [Redacted - Privacy]@pinterest.com]; [Redacted - Privacy]@microsoft.com; [Redacted - Privacy]@microsoft.com]; [Redacted - Privacy]@
 [Redacted - Privacy]@cisa.dhs.gov]; [Redacted - Privacy]@linkedin.com; [Redacted - Privacy]@fb.com];
 [Redacted - Privacy]@reddit.com; [Redacted - Privacy]@reddit.com]; [Redacted - Privacy]@google.com; [Redacted - Privacy]@linkedin.com];
 [Redacted - Privacy]@yahooinc.com]; [Redacted - Privacy]@pinterest.com; [Redacted - Privacy]@pinterest.com]; [Redacted - Privacy]@
 [Redacted - Privacy]@fb.com]; [Redacted - Privacy]@cisa.dhs.gov]; [Redacted - Privacy]@cisa.dhs.gov];
 [Redacted - Privacy]@linkedin.com; [Redacted - Privacy]@linkedin.com]; [Redacted - Privacy]@google.com]; [Redacted - Privacy]@
 [Redacted - Privacy]@yahooinc.com]

CC: [Redacted - Privacy]@fb.com]

Subject: USG | Industry Call (Monthly)

Location: [Redacted]

Start: 4/20/2022 6:00:00 PM
End: 4/20/2022 6:30:00 PM
Show Time As: Tentative

Recurrence: (none)

Updated invite to include USG and Industry partners on one invite + updated to monthly cadence

USG | Industry Mtg - occurs the 2nd Wednesday monthly

WAYS TO JOIN

Join Zoom Meeting



Meeting ID: [Redacted]

Passcode: [Redacted]



Dial by your location

toll: [REDACTED] (Washington DC US)

toll: [REDACTED] (Chicago US)

toll: [REDACTED] (Houston US)

toll: [REDACTED] (San Jose US)

toll: [REDACTED] (New York US)

toll: [REDACTED] (Tacoma US)

tollfree: [REDACTED] (US)

tollfree: [REDACTED] (US)

tollfree: [REDACTED] (US)

tollfree: [REDACTED] (US)

Meeting ID: [REDACTED]

Passcode: [REDACTED]

Confidential - Not For Public Release

Exhibit 46

From: Scully, Brian <[REDACTED]@cisa.dhs.gov>
To: [REDACTED]
CC: [REDACTED]; [REDACTED]
Sent: 5/12/2020 9:12:08 AM
Subject: RE: Cisco WebEx Invite

Hey [REDACTED],

Yes, just got off a call with the interagency. Think we're good. Here's the agenda I have:

- 2:00-2:10 - Dial In/Opening
- 2:10-3:10 - Deep Dive Topic (Industry/USG Moderated Discussion)
 - Changes to voting, campaigning, & threat landscape due to COVID-19 and migration online
 - Ensuring the public has reliable voting information (locations, dates, etc.)
- 3:10-3:20 - Highlights & Upcoming Watch Outs (Moderated)
- 3:20-3:30 - Foreshadow Next Agenda Topic & Wrap-Up

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Tuesday, May 12, 2020 12:09 PM
To: Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Cisco WebEx Invite

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.

Are we all set with the agenda? If so, we can circulate to industry.

Anything else we need to synch on before tomorrow?

Sent from my iPhone

On May 11, 2020, at 1:19 PM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED],

This should work for us. I'll send around to the interagency and let you know if there are any proposed changes.

Regards,
Brian

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Monday, May 11, 2020 11:15 AM
To: Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Cisco WebEx Invite

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 Brian,

Thank you for sharing the WebEx dial-in information -- will make sure that industry attendees receive it.

Wanted to also share the below proposed "run of show" (timeframes proposed are guideposts) that we discussed with industry in our meeting last week.

FYI that given our close-proximity to the prior meeting, we don't anticipate at this time any major "threat" updates, and would like to focus on the deep-dive topic in a discussion format to generate thinking and back-and-forth.

Thanks, and see you this week!

10 minutes: Dial In/Opening
 60 minutes: Deep Dive Topic (Industry/USG Moderated Discussion)
 Changes to voting, campaigning, & threat landscape due to COVID-19 and migration online
 Ensuring the public has reliable voting information (locations, dates, etc.)
 10 minutes: Highlights & Upcoming Watch Outs (Moderated)
 10 minutes: Foreshadow Next Agenda Topic & Wrap-Up

Sent from my iPhone

On May 11, 2020, at 10:33 AM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Sure. Haven't sent back to interagency yet.

Brian

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Monday, May 11, 2020 10:19 AM
To: Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>; N [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Cisco WebEx Invite

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.

Please hold for a few. We may have some minor tweaks based on our industry call.

We should be back in touch shortly

Sent from my iPhone

On May 11, 2020, at 10:13 AM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hey [REDACTED],

We're going to go with the agenda you proposed the other day. As we discussed on Friday, we'll make sure FBI and I&A keep the government threat update to 15 minutes total if you all could do the same with industry. The threat update makes the most sense up front, so I'll keep it there. Here's what I have for the agenda:

- **5 minutes:** Dial In/Opening
- **30 minutes:** Threat update: 15 minute each for Industry + USG
 - Industry (1 Speaker/Company. We can coord in advance to have one company highlight key trends) + USG (Speaker Line-Up Decided by DHS as USG Lead)
- **40 minutes:** Deep Dive Topic (Moderated Discussion -- DHS Lead)
 - Revised primary calendar
 - Changes to election administration for remaining primaries and general election
 - Threat Mitigation Activities – what actions have been taken so far, particularly around COVID-19 Disinformation and what actions are planned going forward.
 - Infrastructure risks due to the changing voting mechanics.
 - Operational Expectations
 - Operations Center coordination and information sharing
 - How to make sure the voting public has reliable information on voting (locations, dates, etc.)
 - USG/Industry Communication Strategies around election related mis/disinformation
- **10 Minutes:** Upcoming Watch-Outs & Highlights (Open Floor)
- **5 minutes:** Foreshadow Next Agenda Topic & Wrap-Up

From: [REDACTED]@fb.com>

Sent: Monday, May 11, 2020 9:30 AM

To: Scully, Brian <[REDACTED]@cisa.dhs.gov>

Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>

Subject: Re: Cisco WebEx Invite

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.

thanks, Brian.

Is the agenda included or will u send that separately?

Sent from my iPhone


On May 11, 2020, at 8:33 AM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Good morning,

I just sent the Cisco WebEx invite to you for Wednesday's meeting. Could you please forward to the appropriate industry folks?

Thanks,
Brian

Brian Scully

@cisa.dhs.gov

Produced to HJC

Exhibit 47

Appointment

From: [redacted] [redacted]@fb.com]
To: [redacted]@linkedin.com; [redacted]@verizonmedia.com; [redacted]@medium.com; [redacted]@verizonmedia.com; [redacted]@fb.com; [redacted]@medium.com; [redacted]@microsoft.com; [redacted]@pinterest.com; [redacted]@pinterest.com; [redacted]@fb.com; [redacted]@google.com; [redacted]@wikimedia.org; [redacted]@google.com; [redacted]@fb.com; [redacted]@fb.com; [redacted]@fb.com; [redacted]@google.com; [redacted]@fb.com; [redacted]@fb.com; [redacted]@reddit.com; [redacted]@reddit.com; [redacted]@fb.com; [redacted]@twitter.com; [redacted]@twitter.com; [redacted]@verizonmedia.com; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted]@microsoft.com

Subject: Monthly USG | Industry Call

Start: 5/13/2020 4:00:00 PM
End: 5/13/2020 5:30:00 PM
Show Time As: Tentative

Recurrence: (none)

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [redacted]@fb.com.

Ways to Join

Computer or Mobile:
 [redacted]

Facebook Meeting Room or Portal:
 Use the touch panel in your room or Portal to enter the join code [redacted]

Telephone:
 Dial in on [redacted] or find an alternative number [redacted] then enter [redacted]

 Please do not edit this section of the description.

View your event at [redacted]

Confidential

Exhibit 48

Message

From: [REDACTED]@fb.com]
Sent: 5/14/2020 11:31:15 AM
To: lobbyists [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]
Subject: USG-Industry Election Meeting

Sharing our HPM from yesterday's USG-Industry meeting on EI as several folks asked how it went. FWIW—it was one of the more substantive meetings we have had with USG.

United States: USG Election Integrity Meeting

- **What happened:** On Wednesday, May 13, U.S. Public Policy participated in a U.S. Government-Industry Election Integrity call to secure US2020. Along with Facebook, industry attendees included Google, Twitter, Microsoft, LinkedIn and others. On the USG side, attendees included senior officials from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DoJ's National Security Division, and the Office of the Director of National Intelligence (ODNI).
- **Why relevant:** Discussion focused on changes to the election landscape due to COVID-19, including how to respond to emerging threats and vulnerabilities due to an expected increase in mail-in voting and differences in approaches across 50 states that could create an information void filled by disinformation actors. Next steps include USG sharing with industry where they expect mail in voting to be predominant and discussion around what Facebook and other industry participants can do to boost signal on authoritative sources of voting information or other efforts. This was the fourth such convening to prepare for US2020 and further strengthened collaboration with industry and USG.
- **Next Steps:** We will continue to participate in these monthly calls with our tech peers & USG partners through the end of 2020.

Exhibit 49

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]69D>
To: [REDACTED]@twitter.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@linkedin.com; [REDACTED]@verizonmedia.com; [REDACTED]@google.com; [REDACTED]@wikimedia.org; [REDACTED]@pinterest.com; [REDACTED]@pinterest.com; [REDACTED]@medium.com; [REDACTED]@twitter.com; [REDACTED]@microsoft.com; [REDACTED]@twitter.com; [REDACTED]@google.com; [REDACTED]@microsoft.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@verizonmedia.com; [REDACTED]@reddit.com; [REDACTED]@google.com; [REDACTED]@verizonmedia.com; [REDACTED]@reddit.com; [REDACTED]@medium.com
CC: [REDACTED]
Sent: 6/9/2020 1:45:27 PM
Subject: Update, Agenda, Dial-In re 6/10/20 USG | Industry Call

Hello Everyone,

Two updates before tomorrow's monthly USG/Industry call:

- You should have earlier today from DHS received a WebEx dial-in information/invite for tomorrow's USG/Industry call from 2-3:30PM EST (let us know if you did not). The proposed run of show and WebEx information is below.
- We were notified of this development just today and wanted to make sure you had a timely heads up:
 - FYSA the GEC has requested to be added as a USG attendee to future meetings, but will not be attending tomorrow. A number of industry participants have reservations about this, and if the USG raises GEC attendance tomorrow, our plan is to tell USG that industry would need to confer further and we will take it offline so we can focus on current threats, and circle back as appropriate.

Thank you, and look forward to seeing you tomorrow!

Proposed Run of Show:

- 10 minutes: Dial In/Opening
- 30 minutes: Threat Updates
 - Threat update from USG (FBI, I&A)
 - Threat update from industry (FB, TW, GOOG)
- 30 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 - Discussion around lessons learned from the protests (ALL)
 - Election process update from DHS: New insights about voting by mail prevalence or other changes? (DHS)
 - Update on documents shared as part of mail-in balloting (DHS)
- 10 minutes: Highlights & Upcoming Watch Outs (Moderated)
- 10 minutes: Foreshadow Next Agenda Topic & Wrap-Up

WebEx Information:

2-3:30PM EST

[https://cisa.webex.com/\[REDACTED\]](https://cisa.webex.com/[REDACTED])

Meeting
number
(access
code):

Meeting password: [REDACTED]

Wednesday, June 10, 2020

Final Report 1291

2:00 pm | (UTC-04:00) Eastern Time (US & Canada) | 1 hr 30 mins

[Join meeting](#)

Join by phone

Tap to call in from a mobile device (attendees only)

[REDACTED] US Toll

[Global call-in numbers](#)

Join from a video system or application

Dial [REDACTED]

Join using Microsoft Lync or Microsoft Skype for Business

Dial [REDACTED]

Need help? Go to <http://help.webex.com>

Produced to HJC

Exhibit 50

Message

From: [REDACTED]@fb.com]
Sent: 6/9/2020 8:45:27 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=user52b849e3];
 [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group
 (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-55760- [REDACTED] [REDACTED]
 [/o=ExchangeLabs/ou=Exchange Administrative Group
 (FYDIBOHF23SPDLT)/cn=Recipients/cn=2caff8c994504311b32dda723f0bf28c- [REDACTED]
 [/o=ExchangeLabs/ou=Exchange Administrative Group
 (FYDIBOHF23SPDLT)/cn=Recipients/cn=5f516f6204ea4fdabee4078904481238- [REDACTED]
 [/o=ExchangeLabs/ou=Exchange Administrative Group
 (FYDIBOHF23SPDLT)/cn=Recipients/cn=7e0acc320c214954b766d69d2fd89f1e- [REDACTED]
 [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=user8cc572b5];
 nlipscomb [/o=ExchangeLabs/ou=Exchange Administrative Group
 [REDACTED]
 (FYDIBOHF23SPDLT)/cn=Recipients/cn=cb41ab97a72a43d69be84835781154f9- [REDACTED]
 [/o=ExchangeLabs/ou=Exchange Administrative Group
 [REDACTED]
 [REDACTED]
CC: [REDACTED]
Subject: [EXTERNAL] Update, Agenda, Dial-In re 6/10/20 USG | Industry Call

Hello Everyone,

Two updates before tomorrow's monthly USG/Industry call:

- You should have earlier today from DHS received a WebEx dial-in information/invite for tomorrow's USG/Industry call from 2-3:30PM EST (let us know if you did not). The proposed run of show and WebEx information is below.
- We were notified of this development just today and wanted to make sure you had a timely heads up:
 - FYSA the GEC has requested to be added as a USG attendee to future meetings, but will not be attending tomorrow. A number of industry participants have reservations about this, and if the USG raises GEC attendance tomorrow, our plan is to tell USG that industry would need to confer further and we will take it offline so we can focus on current threats, and circle back as appropriate.

Thank you, and look forward to seeing you tomorrow!

Proposed Run of Show:

- 10 minutes: Dial In/Opening
- 30 minutes: Threat Updates
 - Threat update from USG (FBI, I&A)
 - Threat update from industry (FB, TW, GOOG)
- 30 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 - Discussion around lessons learned from the protests (ALL)
 - Election process update from DHS: New insights about voting by mail prevalence or other changes? (DHS)
 - Update on documents shared as part of mail-in balloting (DHS)
- 10 minutes: Highlights & Upcoming Watch Outs (Moderated)
- 10 minutes: Foreshadow Next Agenda Topic & Wrap-Up

WebEx Information:

2-3:30PM EST



Meeting number (access code): [REDACTED]

Meeting password: [REDACTED]

Need help? Go to <http://help.webex.com>

Wednesday, June 10, 2020

2:00 pm | (UTC-04:00) Eastern Time (US & Canada) | 1 hr 30 mins

[Join meeting](#)

Join by phone

Tap to call in from a mobile device (attendees only)

[REDACTED] US Toll

[Global call-in numbers](#)

Join from a video system or application

Dial [REDACTED]

Join using Microsoft Lync or Microsoft Skype for Business

Dial [REDACTED]

Exhibit 51

Appointment

From: [redacted] [redacted]@google.com]
To: [redacted] [redacted]@fb.com]; [redacted] [redacted]@google.com]

Subject: Monthly USG | Industry Call

Start: 6/10/2020 6:00:00 PM

End: 6/10/2020 7:30:00 PM

Show Time As: Busy

Recurrence: (none)

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [redacted].

Ways to Join

Computer or Mobile:

Facebook Meeting Room or Portal:

Use the touch panel in your room or Portal to enter the join code [redacted]

Telephone:

Dial in on [redacted] or find an alternative number [redacted] then enter [redacted]

Confidential - Not For Public Release

Exhibit 52

Message

From: [REDACTED]@fb.com]
 Sent: 6/30/2020 3:45:24 PM
 To: [REDACTED]@fb.com; [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]
 Subject: Message summary [{"otherUserFbId":null,"threadFbId": [REDACTED]}

[REDACTED] (6/30/2020 03:31:33 PDT):
 > [REDACTED], just confirming here that Twitter, MSFT, and Google have all indicated that July 15 will work for the next USG/Industry meeting ([REDACTED] is double checking with [REDACTED] and will confirm otherwise by EOD). Maybe tomorrow we could let DHS know and could also, if you think a good idea, shoot to schedule the CIS demo? If there is any way to be more helpful here, just give the word.

[REDACTED] (6/30/2020 03:41:46 PDT):
 > [REDACTED] does this look good as a potential agenda to share with DHS? Also, just to double confirm, I believe we landed on "no" on the GEC b/c could open the door to other participants, but nobody felt particularly strongly? Will need to relay GEC preference when we go to DHS on the 7/15 (TBC) date, so wanted to make sure. Thank you so much.

[REDACTED] (6/30/2020 04:51:47 PDT):
 >Related to above, here is draft agenda to share with DHS for July meeting and will also need to share GEC preference -- [REDACTED]

[REDACTED] (6/30/2020 09:01:58 PDT):
 [REDACTED] Confirming here that Industry has confirmed July 15 works for pushing out the date of the next USG/Industry meeting. [REDACTED] so we can go to DHS, is the above slide/agenda draft OK and wanted to confirm we are saying no on the GEC? Thank you so much.

[REDACTED] (6/30/2020 09:08:39 PDT):
 >I sent a text to DHS that we may slip it a week and I would follow up later today or tomorrow with more info

[REDACTED] (6/30/2020 09:14:30 PDT):
 >DHS response: Good. We can make that happen. [REDACTED] --let's aim to send an email by COB today to DHS so they can alert their partners.

[REDACTED] (6/30/2020 09:36:12 PDT):
 >OK -- would just need signal on the above agenda and the GEC to be clear or what we can say to DHS in the note?

[REDACTED] (6/30/2020 09:39:44 PDT):
 >Agenda (at least). I prefer not to put GEC in an email.

[REDACTED] (6/30/2020 10:00:10 PDT):
 >Here is the draft agenda in the slide ([REDACTED]) -- 10 minutes: Dial In/Opening
 >30 minutes: Threat Updates
 >Threat update from USG (FBI, I&A)
 >Threat update from industry (FB, TW, GOOG) -- ANYONE ELSE?
 >40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 >Election process update from DHS/USG
 >Discussion around Voting-by-Mail & Timing on General Election Results
 >Scenarios To Anticipate if Election Results Delayed
 >Foreign Interference Claims, Inauthentically Generated Domestic Unrest, Voter Suppression
 >Misinformation, Hack/Leak, QAnon & Disproving Falsity
 >Threats That could Be Spun, so Calibrate Carefully
 >[REDACTED] & Known TTPs
 >10 minutes: Highlights & Upcoming Watch Outs & wrap (Moderated)

[REDACTED] (6/30/2020 10:22:02 PDT):
 >Hey—I have a dinner tonight so I may not be able to join the call.

[REDACTED] (6/30/2020 10:40:50 PDT):
 >Totally OK -- will back-brief. :-)

[REDACTED] (6/30/2020 10:42:48 PDT):

>Separately, had a quick sync with [REDACTED] and for the DHS email back, we can just tell them that given that we are pushing out the meeting to 7/15 (if they agree), we will be sending them a proposed agenda next week -- will review with [REDACTED] the above at 1:1 this week. On the GEC aspect, I will momentarily share the draft DHS email that goes to that.

[REDACTED] (6/30/2020 12:58:18 PDT):

[REDACTED] how are you with this draft back to DHS --
<https://docs.google.com/document/d/1cAVB078wBn3HDMHceHHj95GNTcRHURI9FellyEyDc8k/edit#>

[REDACTED] (6/30/2020 12:58:21 PDT):

>Also pasting here:

>Hi [REDACTED] and [REDACTED],

>

>Thank you so much for the outreach on our next sync. Given the Fourth of July holiday and various schedules, we were wondering if we could move our next meeting to wednesday, July 15 -- if this works, we can send along a draft agenda next week for consideration?

>

>Separately, on the GEC, we talked it over with our colleagues in industry and the feedback we received was that it has taken some time to build trust and we are advancing rapidly on US2020, where adding a new participant could cause potential disruption, so there is consensus around not expanding participation around our trusted group. As an additional and important point, we are primarily focused on defensive postures against threats, and the public diplomacy aspects of the GEC seems a bit removed and outside of the scope we are protecting against.

>

>Thank you for the chance to consult on this and will circle back with the agenda once we have that together.

>

>Talk soon --

[REDACTED]

[REDACTED] (6/30/2020 15:39:14 PDT):

>Just signal boosting the above [REDACTED] (think [REDACTED] wanted to send out tonight or early tomorrow. . .)

[REDACTED] (6/30/2020 15:40:24 PDT):

>You ok with this [REDACTED]?

[REDACTED] (6/30/2020 15:42:04 PDT):

>I'd just be very careful about the defensive v public diplomacy language since it's the trickiest piece here.

[REDACTED] (6/30/2020 15:42:17 PDT):

>I think we should say it, but would love your read on how to land it right w/our gov't partners, [REDACTED]

[REDACTED] (6/30/2020 15:44:27 PDT):

>We could just strike that sentence?

[REDACTED] (6/30/2020 15:45:24 PDT):

>Let me play with it

Exhibit 53

Message

From: [REDACTED]@fb.com]
Sent: 6/11/2020 8:35:04 AM
To: lobbyists@[REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]
Subject: 6/10/20 USG-Industry Election Meeting HPM

Team,

Sharing our HPM from yesterday's USG-Industry meeting on election integrity.

Let me know if you have any questions!

United States: USG-Industry Election Integrity Meeting

- **What happened:** On Wednesday, June 10th, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our threat intelligence team participated in our second monthly U.S. Government-Industry Election Integrity call to secure US2020. In addition to Facebook, industry attendees included Google, Twitter, Microsoft, LinkedIn and others. USG attendees included senior officials from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DoJ's National Security Division, and the Office of the Director of National Intelligence (ODNI).
- **Why relevant:** The discussion focused on changes to the election landscape due to COVID-19, including how to respond to emerging threats and vulnerabilities due to an expected increase by "mail-in voting" and differences in approaches across 50 states that could create an information void filled by disinformation and other actors. USG committed to sharing information with industry where they expect mail in voting to be predominant, which led to a discussion around what Facebook and other industry participants can do to boost signal on authoritative sources of voting information or other efforts. This was the fourth such convening to prepare for US2020, the second call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- **Next Steps:** We will continue to participate in these monthly calls with our tech peers & USG partners through the end of 2020. Additionally, next steps include a discussion of strategic communications by both industry and USG to ensure accurate voter information is part of our collective election security efforts.

Exhibit 54

Message

From: [REDACTED]@fb.com]
 Sent: 7/1/2020 2:20:09 PM
 To: [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]
 Subject: Message summary [{"otherUserFbId":null,"threadFbId": [REDACTED]}

[REDACTED] (7/01/2020 12:45:06 PDT):
 >Hi there -- [REDACTED] is everything set with DHS re the above? Am in a 1:1 with [REDACTED] and just wanted to quickly check in. :-)

[REDACTED] (7/01/2020 12:51:31 PDT):
 >I have been slammed with other things. Hope to send them later today.

[REDACTED] (7/01/2020 13:14:05 PDT):
 -- that's actually a good thing! :-) Just updated the email to include the agenda -- here it is:

[REDACTED] (7/01/2020 13:14:07 PDT):
 >Hi [REDACTED] and [REDACTED],
 >
 >Thank you so much for the outreach on our next sync. Given the Fourth of July holiday and various schedules, we were wondering if we could move our next meeting to Wednesday, July 15. Below is a proposed agenda we'd love your input on:
 >10 minutes: Dial In/Opening
 >30 minutes: Threat Updates
 >Threat update from USG (FBI, I&A)
 >Threat update from industry (FB, TW, GOOG)
 >40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 >Election process update from USG
 >Hack/Leak and USG Attribution Speed/Process
 >Vote-by-mail: How do we deal with the gap between Nov 3 and results?
 >10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)?
 >
 >Separately, on the GEC, we talked it over with our colleagues in industry and the feedback we received was that it has taken some time to build trust and we are advancing rapidly on US2020, where adding a new participant could cause potential disruption, so there is consensus around not expanding participation around our trusted group. As an additional and important point, we are primarily focused on defensive postures against threats, and the public diplomacy aspects of the GEC seems a bit removed and outside of the scope we are protecting against.
 >
 >Thank you for the chance to consult on this and will circle back with the agenda once we have that together.
 >
 >Talk soon --

[REDACTED] (7/01/2020 13:39:29 PDT):
 >Can you resend the CIS note as well. Hope to get them both sent tonight. Have several more calls today but will ship them. Thanks!

[REDACTED] (7/01/2020 13:52:50 PDT):
 >Absolutely [REDACTED] just boosted! Should be in your inbox now!

[REDACTED] (7/01/2020 14:03:17 PDT):
 >Sent them both. Done.

[REDACTED] (7/01/2020 14:18:02 PDT):
 >Best news! Thank you so much. Hopefully DHS/CISA/FBI will be good with the friendly no on GEC and so grateful to the adroit management of that relationship.

[REDACTED] (7/01/2020 14:20:09 PDT):
 >On GEC-I just mentioned our industry partners preferred not to add new participants.

Exhibit 55

Message

From: [REDACTED]@fb.com]
 Sent: 7/10/2020 7:28:55 AM
 To: [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]
 Subject: Message summary [{"otherUserFbId":null,"threadFbId": [REDACTED]}]

[REDACTED] (7/10/2020 02:12:58 PDT):
 >Hi everyone -- I am on PTO today and will try and dial in for bi-weekly industry sync if internet connectivity allows, but here is gameplan for discussion (as reviewed with [REDACTED] at our 1:1 today -- will also put in our notes for these discussions) -- [REDACTED] had reached out to DHS to see if they had any inputs on the agenda but I hadn't seen anything yet, so she can maybe share here if she gets any inbound? Thanks so much and here is framing:

>
 >***Agenda for bi-weekly industry sync***
 >*Prep for the USG meeting
 >*GEC and other participants may come up
 >* US2020 & Ask of USG
 >* Unstable and hard to predict next few months > for a certain set of threats, let us know what you know around attribution so we can act appropriately and swiftly (e.g., Hack/Leak threat)
 >*Driven by a foreign power
 >*Capacity to do detection
 >*If you see or are aware something is coming, helping us come to attribution quickly so that we can enforce
 >*Get it to us quickly
 >*Ask at prep meeting
 >*Vote by Mail
 >Prep for USG meeting on 7/15
 >*Threat Brief
 >*USG may have updates
 >*May be a lighter meeting
 >*Comms not ready yet
 >*Keep the pattern going
 >*Inbound on GEC and other entities
 >
 >All notes and the above here: [REDACTED]

[REDACTED] (7/10/2020 03:14:44 PDT):
 >Enjoy your PTO, [REDACTED]!

[REDACTED] (7/10/2020 07:28:55 PDT):
 ><https://www.cyberscoop.com/biden-campaign-ciso-chris-derusha/>

Exhibit 56

██████████@s.whatsapp.net/██████████@s.whatsapp.net/System

Message chatroom: chat transcript

Chat description: none provided

Chat type WhatsApp
 Private chat no
 Transcript timezone (UTC-08:00) Pacific Time (US & Canada)
 Transcript start 2020-10-14 06:05:00
 Transcript end 2020-10-14 16:46:00
 Transcript participants 3
 Initial participants ██████████@s.whatsapp.net); ██████████@s.whatsapp.net); System Message

Timestamp	Sender	Recipients	Message text
2020-10-14 06:05:00	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	██████████ -- looking at the calendar today, I see the FITF meeting. I don't recall whether I forwarded the invite to the rest of the group. Did you?
2020-10-14 06:40:20	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	I did not. I'll be able to dial in on the phone, but balancing a couple things today. Do we have an agenda for today?
2020-10-14 06:40:59	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	The agenda is TBD. They may have OGA at the meeting, but not yet certain.
2020-10-14 06:41:57	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	Think we want to get more info on the email leak in the NY Post from today and also on China based on the DNI's statement that they are much more prolific at IOs now than Russia

Timestamp	Sender	Recipients	Message text
2020-10-14 06:42:29	██████████ (whatsapp.net)	@s. ██████████ ██████████ @s.whatsa pp.net); Sy stem Mess age; ██████████ ██████████ @s.whatsa pp.net)	I just forwarded the invite to Security Policy, ██████████ and ██████████. Realize I forgot to forward to ██████████ as I type tyis
2020-10-14 06:42:37	██████████ (app.net)	@s.whatsa pp.net); Sy stem Mess age; ██████████ ██████████ @s.whatsa pp.net)	That makes sense.
2020-10-14 06:43:05	██████████ (app.net)	@s.whatsa pp.net); Sy stem Mess age; ██████████ ██████████ @s.whatsa pp.net)	I'm actually with ██████████ and ██████████ today - we have an all day mgr offsite. So I will likely be the one dialing in today
2020-10-14 06:43:26	██████████ (whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; ██████████ ██████████ @s.whatsa pp.net)	Wow, in person?
2020-10-14 06:43:39	██████████ (app.net)	@s.whatsa pp.net); Sy stem Mess age; ██████████ ██████████ @s.whatsa pp.net)	But we should invite ██████████ as well - do you want to forward her the invite?
2020-10-14 06:43:52	██████████ (app.net)	@s.whatsa pp.net); Sy stem Mess age; ██████████ ██████████ @s.whatsa pp.net)	Yes outside in ██████████'s backyard

Timestamp	Sender	Recipients	Message text
2020-10-14 06:44:13	[REDACTED] (whatsapp.net)	@s. [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	I will. Who else should I invite? [REDACTED], [REDACTED], [REDACTED], [REDACTED]?
2020-10-14 06:44:56	[REDACTED] (whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Awesome! I hope you got swag.
2020-10-14 06:45:28	[REDACTED] (whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Are we talking about the Mexico lead? If so, we should invite [REDACTED].
2020-10-14 06:46:04	[REDACTED] (whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Based on his investigation, think it makes sense
2020-10-14 06:46:07	[REDACTED] (whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Also [REDACTED] since they sent IR leads yesterday
2020-10-14 06:49:08	[REDACTED] (whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Ah, that answers another question I had. Did Elvis send the leads to you? I d idn't see them

Timestamp	Sender	Recipients	Message text
2020-10-14 06:49:22	[REDACTED] (whatsapp.net)	[REDACTED] @s. [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	And are the leads documented anywhere?
2020-10-14 06:51:23	[REDACTED] (whatsapp.net)	[REDACTED] @s. whats app.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	I think Elvis sends it to a random selection of people each time :) looks like h e sent it yesterday to me, [REDACTED], [REDACTED], [REDACTED] and [REDACTED].
2020-10-14 06:52:37	[REDACTED] (whatsapp.net)	[REDACTED] @s. whats app.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	[REDACTED] is having [REDACTED] document the IR leads in Cases now, looks like a fe w are duplicates of previous leads. [REDACTED] will dedupe them and document the m in Cases.
2020-10-14 06:55:26	[REDACTED] (whatsapp.net)	[REDACTED] @s. [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Thanks
2020-10-14 15:50:56	[REDACTED] (whatsapp.net)	[REDACTED] @s. [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	[REDACTED] -- I just heard from Elvis that the Sandworm indictment will be unsealed on the 19th, not the 20th.
2020-10-14 15:51:04	[REDACTED] (whatsapp.net)	[REDACTED] @s. [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] [REDACTED] @s.whatsa pp.net)	Elvis got that date from the USAO

Timestamp	Sender	Recipients	Message text
2020-10-14 16:46:00	[REDACTED]@s.whatsapp.net)	[REDACTED] @s.whatsapp.net); System Message; [REDACTED] @s.whatsapp.net)	Got it. Thanks [REDACTED].

Nickname	Name	Surname	E-mail	Source PID	Type
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	@s.whatsapp.net b2f828a0-c73c-49ca-bd7d-7ccccc1f1e4	User
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	@s.whatsapp.net 4ec312b0-6d8b-444b-ad9f-f2d30001ae90	User
System Message	System Message			5e5ae362-2735-4311-8329-fe4e67f70f72	User

Produced to HJC

Exhibit 57

Appointment

From: [redacted]@google.com
To: [redacted]@fb.com; [redacted]@google.com

Subject: Monthly USG | Industry Call

Start: 7/15/2020 6:00:00 PM

End: 7/15/2020 7:30:00 PM

Show Time As: Tentative

Recurrence: (none)

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [redacted].

Ways to join

Computer or Mobile:

Facebook Conference Room and Portal:

Use the touch panel to enter the join code [redacted]

Telephone:

Dial in on [redacted] or find an alternative number [redacted] then enter [redacted]

Enabled by oneVC

Confidential - Not For Public Release

Exhibit 58

Message

From: [REDACTED]@fb.com]
Sent: 7/17/2020 7:17:35 AM
To: [REDACTED]@fb.com]
Subject: USG-Industry Monthly Election Meeting (July)

Team,

Sharing our HPM from this week's USG-Industry meeting on election integrity.

Let me know if you have any questions!

[REDACTED]

United States: USG-Industry Monthly Election Integrity Meeting (July)

- **What happened:** On Wednesday, July 15th, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our threat intelligence and threat discovery teams participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. In addition to Facebook, industry attendees included Google, Twitter, Microsoft, LinkedIn and others. USG attendees included senior officials from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the fifth such convening to prepare for US2020, the third call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- **Why relevant:** The discussion focused on changes to the election landscape due to COVID-19, including how to respond to emerging threats and vulnerabilities due to an expected increase by "mail-in voting" and differences in approaches across 50 states that could create an information void filled by disinformation and other actors. The discussion also focused on cross-sector IO and cyber threat updates from state and non-state actors and expected information environment challenges in the lead up and aftermath to the election due to mail-in-voting, expected poll worker shortages, and lower volumes of registered voters, as well as the importance of communicating accurate voter information.
- **Next Steps:** We will continue to participate in these monthly calls with our tech peers & USG partners through the end of 2020. The next convening will occur in mid-August before the national party conventions.

Exhibit 59

Appointment

From: [REDACTED] [REDACTED]@google.com]
To: [REDACTED] [REDACTED]@fb.com]; [REDACTED] [REDACTED]@google.com]

Subject: Monthly USG | Industry Call
Location: [REDACTED]

Start: 8/12/2020 6:00:00 PM
End: 8/12/2020 7:30:00 PM
Show Time As: Tentative

Recurrence: (none)

To join the meeting on a computer or mobile phone: [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? [REDACTED] Recurrence will be second wednesday
from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this
invitation. If you feel someone should be added, please contact [REDACTED]@fb.com.

Confidential - Not For Public Release

Exhibit 60

TL;DR: Today, Facebook participated in one of our regular industry and USG coordination meetings on election preparedness and security focused on US 2020. We used this meeting as an opportunity to signal publicly the ongoing collaboration on emerging threats ahead of the election. Facebook, Google, Twitter (and others) issued a statement and background updates on our security work to date with press.

RESULTS:

- Media coverage has been low with overall sentiment trending straightforward to positive.
- We started as number 7 story on Techmeme.
- Coverage focused on these meetings being part of the ongoing series signaling strong collaboration among industry and USG ahead of November.
- Thanks to how this moment landed, we are now negotiating with tech platforms a drumbeat of these joint moments for Sept/Oct.

HIGHLIGHTS:

- Coverage can be best summed up by [Politico](#) highlighting Silicon Valley's ongoing efforts ahead of the election despite companies' differences.
 - *"Their individual rules and decision-making still apply, but they close coordination allows them to share both lessons learned and ID threats coming down the pike. That's key because one of the critical lessons learned in recent years is that problematic content often spreads across platforms, so combining forces helps the companies amplify their efforts."*
- [The New York Times](#) included a reference to Facebook's efforts in warding off election mishaps:
 - *"Facebook, for instance, has monitored election behavior in Brazil, Mexico, Germany and France. Last year, the social network said it was strengthening how it verified which groups and people placed political advertising on its site."*
- [NBC](#) highlighted that the uncertainty around the election results will be playing out as much in traditional media as it will on social platforms:
 - *"The traditional news media has long been scrutinized for how and when it reports election results because those decisions can have wide implications for how Americans and the world interpret an election."*
- A number of stories including [USA Today](#) pointed out companies' updates to strengthen platform integrity ahead of the election:
 - *"Facebook said in October it was strengthening how it verified groups and people who place political advertising on its site. Twitter has recently been strengthening its moderation on misinformation on the site."*
- A new narrative to watch includes questions about why TikTok and other companies are not a part of these meetings.
 - [Donie O'Sullivan](#), CNN: No @tiktok_us?
 - [Alex Stamos](#): I'm glad these meetings have continued. Important but missing names: TikTok Nextdoor Discord Amazon
- There are no worst stories at this time.

BEST/STRAIGHTFORWARD STORIES:

- [Big Tech met with govt to discuss how to handle election results](#), NBC, David Ingram, Kevin Collier, and Ken Dilanian
- [Google, Facebook and Others Broaden Group to Secure U.S. Election](#), New York Times, Mike Isaac and Kate Conger
- [Silicon Valley game plans for election night](#), Politico, Nancy Scola
- [Tech giants, including Facebook and Twitter, unite looking to secure the upcoming election](#), USA Today, Josh Rivera

WORST STORIES:

- N/A

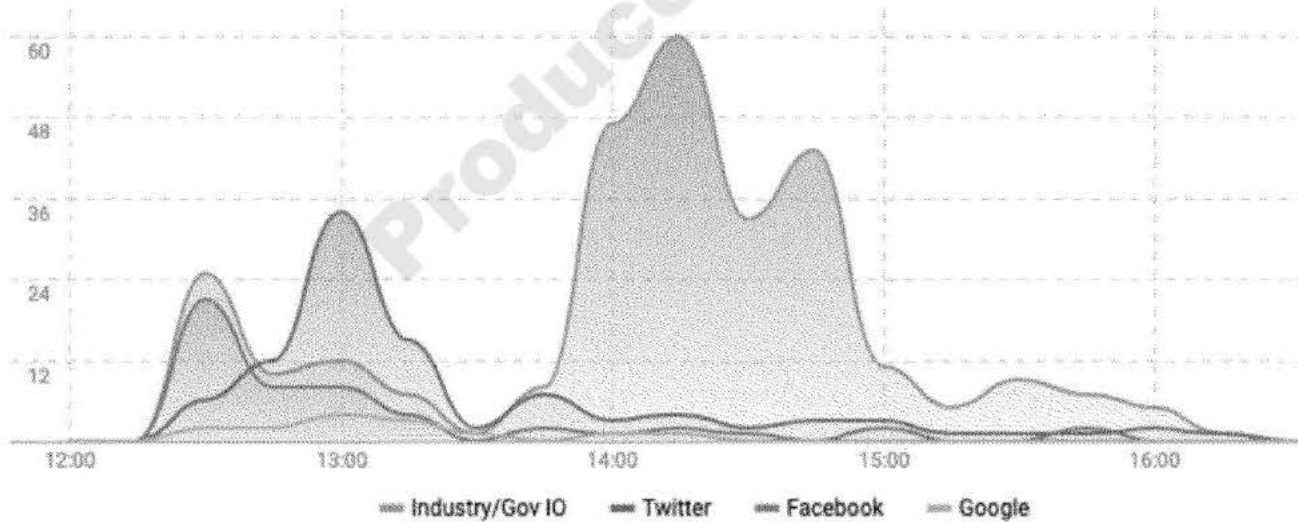
NOTABLE QUOTES:

- *“Tech companies and social media platforms have been working to curb the spread of misinformation during the lead up to the 2020 election, including by putting voting information labels on posts by Trump and Biden, flagging misleading posts by the candidates, tracking and exposing disinformation, publicly tracking political ads, labelling government and state-affiliated media accounts, unearthing deepfakes and curbing news pages that have political affiliations. Some are also giving their own employees paid time off to vote on Nov. 3.” (CNET)*
- *“Why the statement is eye-catching: The document is unusual because the tech companies are often extraordinarily competitive with each other. In some cases, the executives simply don't like each other. And the companies have taken different approaches to what to allow on their platforms. Their individual rules and decision-making still apply, but they close coordination allows them to share both lessons learned and ID threats coming down the pike. That's key because one of the critical lessons learned in recent years is that problematic content often spreads across platforms, so combining forces helps the companies amplify their efforts.” (Politico)*
- *“Absent from the meeting was the popular social media upstart TikTok, which Trump has threatened to ban and was recently the subject of an executive order because he says its Chinese ownership makes it a security threat. The company has previously said it plans to fight election misinformation on its platform.” (NBC News)*
- *“Facebook, for instance, is looking at updating policies related to the time between voting and when results are announced, one of the people said. It is also examining potential product updates through its Voting Information Center and additional labels added to posts from politicians, the person said. Matthew Morgan, general counsel for the Trump campaign, said that Democrats were ‘trafficking in conspiracy theories and hypotheticals’ and that Mr. Trump’s concerns stemmed from states with little experience in mail balloting rushing to adopt the method.’ (Wall Street Journal)*

ALL COVERAGE

SOCIAL MEDIA: Social conversation is low, with under 500 mentions. Sentiment is trending straightforward to positive. See below for timeline tracking statement tweets by industry partners, and overall conversation.

TIMELINE:



- [Donie O'Sullivan, CNN: No @tiktok_us?](#)
- [Mike Isaac, NYT: Big Tech meets with Big Government before Big Election/ @kateconger nytimes.com/2020/08/12/tec...](#)
- [Paul Beckett, WSJ: Facebook, Google and Twitter are girding for election misinformation risks as President Trump sounds the alarm on the voting process - super if sobering piece from @EmilyGlazer & @dustinvolz](#) [Link](#)
- [Alexander Marquardt, CNN: Meeting today on election security between major tech companies - incl Google, Facebook, Twitter, Microsoft - and FBI, ODNI, CISA & DoJ. Below some of the influence threats Facebook says they anticipate.](#)
- [Carla Marinucci, Politico: Silicon Valley game plans for election night](#) [Link](#) via @politico
- [Josh Lederman, NBC: Twitter, Google, Microsoft, Facebook issue joint statement saying they met again today with the US government about 2020 election integrity](#)
- [Erik Brattberg: Google, Facebook and Others Form Tech Coalition to Secure U.S. Election - The New York Times](#)

ARTICLES:

1. [Big Tech met with govt to discuss how to handle election results](#), NBC, David Ingram, Kevin Collier, and Ken Dilanian
 - [Reposted by Yahoo News](#)
2. [Google, Facebook and Others Broaden Group to Secure U.S. Election](#), New York Times, Mike Isaac and Kate Conger
 - [International News Headline](#)
3. [Tech giants, including Facebook and Twitter, unite looking to secure the upcoming election](#), USA Today, Josh Rivera
4. [Facebook, Google, Twitter and others work on election security ahead of RNC and DNC](#), CNET, Corinne Reichert
 - [Reposted by Entertainment Overdose, Desoto Post](#)
5. [Tech Companies Including Facebook, Google Meet with Feds to Make 'Preparations' for Election, Promise to 'Stay Vigilant'](#), Mediate, Rudy Takala
6. [Google, Facebook and others form tech coalition to secure U.S. election](#), New York Times, Mike Isaac and Kate Conger
7. [Silicon Valley game plans for election night](#), Politico, Nancy Scola
 - [Reposted by Microsoft News](#)
8. [Facebook and other tech giants gird for chaotic election](#), Wall Street Journal, Dustin Volz and Emily Glazer (*full text below*)
9. [Facebook, Google, Microsoft, and Twitter team up to fight election interference](#), Digital Trends, Meira Gebel
 - [Reposted by Digital Market News, Yahoo Finance](#)

--

PAYWALL

[Facebook and other tech giants gird for chaotic election](#), Wall Street Journal, Dustin Volz and Emily Glazer

Facebook Inc., FB 1.47% Alphabet Inc.'s GOOG 1.78% Google and Twitter Inc. TWTR 0.43% have discussed with federal officials how the social-media platforms can prevent the spread of misinformation in the days before and after the election, after the U.S. intelligence community warned of foreign interference and President Trump called the vote's integrity into question.

The conversations are designed to address problems that may arise from across the political spectrum and have included the Federal Bureau of Investigation, the Department of Homeland Security and intelligence agencies, according to people familiar with the matter.

They have been shaped by the impact of the coronavirus pandemic, which is expected to result in far more people voting by mail than in previous elections, making it unclear how long it will take to have final election results.

The discussions have grown more urgent, the people said, as President Trump has repeated his warning of likely vote-by-mail fraud. In late July, for example, he tweeted to his nearly 85 million followers: “2020 will be the most INACCURATE & FRAUDULENT Election in history. It will be a great embarrassment to the USA. Delay the Election until people can properly, securely and safely vote???”

The U.S. intelligence community has assessed that Russia has undertaken a broad effort to damage Democrat Joe Biden’s bid for the presidency, while China prefers that President Trump not win re-election, a senior intelligence official said recently.

The concern among officials and social-media companies is that any delay in declaring a result or widespread problems with mail-in voting could trigger the spreading of false stories about how the votes are being counted.

The broader rollout of mail-in voting will test states’ abilities to count votes quickly and accurately. Studies show absentee-voter fraud has been rare in prior elections. But politicians in both parties have sometimes been emboldened by delays in certifying results in past elections to speculate about foul play.

Among the possibilities being discussed at Facebook and other tech platforms are putting in place procedures to act more quickly on misinformation, because false posts can sometimes exist online for hours before platforms take them down, said people familiar with the discussions.

Facebook, for instance, is looking at updating policies related to the time between voting and when results are announced, one of the people said. It is also examining potential product updates through its Voting Information Center and additional labels added to posts from politicians, the person said.

Matthew Morgan, general counsel for the Trump campaign, said that Democrats were “trafficking in conspiracy theories and hypotheticals” and that Mr. Trump’s concerns stemmed from states with little experience in mail balloting rushing to adopt the method.

“Democrats are trying to undermine the integrity of our election mere months before Election Day by hastily implementing chaos-ridden universal vote-by-mail schemes in states that have no experience or infrastructure to support these systems,” Mr. Morgan said.

The National Security Council said in a statement that the Trump administration doesn’t tolerate foreign election interference and that it was working with states, social-media firms and election vendors “to protect the integrity of the 2020 elections.”

Representatives for Facebook, Twitter and Google said they are working closely with election officials and industry peers to safeguard the process, including by strengthening policies and procedures that were put in place after the 2016 election.

Democratic Party officials have pressed Facebook on similar subjects, including in a late July meeting when representatives of campaign committees asked the company for assurances that it would intervene if Mr. Trump or others promoted misinformation about the outcome during the counting of votes, according to people familiar with the conversation.

Facebook Chief Executive Mark Zuckerberg has convened a series of high-level meetings over the past several months to discuss the company’s potential response to election-related misinformation, a person familiar with the matter said.

At an internal Facebook employee Q&A on Aug. 6, Mr. Zuckerberg said the company is “sort of in an unprecedented position” given that election results could be unknown for days or weeks, according to the person. BuzzFeed News earlier reported on the meeting.

Chief among the issues, said several current and former officials from different agencies, were Mr. Trump's repeated attacks on the security of voting by mail and his suggestions that election results could be tampered with because of the potential effect such messages could have on public confidence in the outcome. Some current officials working on election security said they consider such messaging from the president to be a more significant threat than efforts by foreign countries to undermine the election's integrity.

A Wall Street Journal review of Mr. Trump's tweets dating back to 2012 found more than 110 instances of the president claiming widespread illegal voting, asserting an election or primary was rigged, or that voting by mail would allow for rampant fraud. More than half of those tweets were from this year, with the most of them concerning mail balloting.

Experts in both election security and foreign disinformation said Moscow's efforts to sow division and undermine faith in U.S. democracy have continued and evolved since 2016, moving away from automated, spamlike content and toward more-refined efforts to seed disinformation content on websites presented as authentic.

Clint Watts, a former FBI official and a research fellow with the Foreign Policy Research Institute, said that Mr. Trump's direct attacks on the election's integrity represented a different problem.

"Rewind four years: The Russian could never have pushed this volume or intensity of disinformation into our election space that comes directly from the president," Mr. Watts said.

Trump administration officials at times have faced the dilemma of trying to shore up public confidence in the election process, including vote-by-mail balloting, without provoking a reaction from Mr. Trump that undermines the effort, according to current and former officials.

Chris Krebs, the top cybersecurity official at the Department of Homeland Security, urged last week in a speech at the Black Hat cybersecurity conference that the public be calm in expecting delayed reporting of results.

"The last measure of resilience in the 2020 election is going to be an informed, patient voter," Mr. Krebs said at the conference. "It's going to take time to count the vote, whether it's absentee ballots coming in, whether it's longer lines. Whatever it takes, it's going to take a little bit more time."

Exhibit 61

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]69D>
To: [REDACTED]
CC: [REDACTED]
Sent: 9/11/2020 12:40:54 PM
Subject: RE: Draft Agenda for 9/16 USG/Industry Meeting

Perfect! Will make sure you are on the agenda. 😊

From: [REDACTED] <[REDACTED]@microsoft.com>
Sent: Friday, September 11, 2020 3:39 PM
To: [REDACTED] <[REDACTED]@fb.com>
Subject: RE: Draft Agenda for 9/16 USG/Industry Meeting

I can do a short threat update from MSFT covering our recent blog

[REDACTED] || p: [REDACTED]

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Friday, September 11, 2020 12:34 PM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@twitter.com>; [REDACTED] <[REDACTED]@pinterest.com>; [REDACTED] <[REDACTED]@google.com>; [REDACTED] <[REDACTED]@google.com>; [REDACTED] <[REDACTED]@twitter.com>; [REDACTED] (CELA) <[REDACTED]@microsoft.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@verizonmedia.com>; [REDACTED] <[REDACTED]@google.com>; [REDACTED] (CELA) <[REDACTED]@microsoft.com>; [REDACTED] <[REDACTED]@reddit.com>; [REDACTED] <[REDACTED]@pinterest.com>; [REDACTED] <[REDACTED]@medium.com>; [REDACTED] <[REDACTED]@reddit.com>; [REDACTED] <[REDACTED]@twitter.com>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@medium.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@microsoft.com>; [REDACTED] <[REDACTED]@linkedin.com>; [REDACTED] <[REDACTED]@pinterest.com>; [REDACTED] <[REDACTED]@wikimedia.org>; [REDACTED] <[REDACTED]@verizonmedia.com>; [REDACTED] <[REDACTED]@verizonmedia.com>; [REDACTED] <[REDACTED]@microsoft.com>; [REDACTED] <[REDACTED]@pinterest.com>; [REDACTED] <[REDACTED]@pinterest.com>; [REDACTED] <[REDACTED]@verizonmedia.com>; [REDACTED] <ty [REDACTED]@reddit.com>; [REDACTED] <[REDACTED]@microsoft.com>; [REDACTED] <[REDACTED]@verizonmedia.com>

Subject: [EXTERNAL] Draft Agenda for 9/16 USG/Industry Meeting

Hello Everyone,

Below please find a proposed draft agenda for our bi-weekly industry sync coming up in about an hour – in addition, there is a plan to have another strategic comms release around the next USG/Industry meeting – a draft of that will be shared early next week and the various Comms leads from the industry participants that engaged last time are communicating on this right now.

Thanks very much for the continued collaboration, and see you shortly!

- **10 minutes: Dial In/Opening**
- **30 minutes: Threat Updates**
 - Threat update from USG -- Foreign Actor/Activity (INSERT)
 - UNCLASS Detailed DNI Threat Update Extracted From Intelligence Reports
 - Threat update from industry (TW, FB, GOOG + ANY OTHERS)
- **40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)**
 - USG Election Process Update & Virtual Election Day War Rooms

- Delegitimization Claims of Concern
 - Amplification of Accurate Voter & Campaign Security Info
 - Timely Threat Indicator Sharing & Readiness for Post-Election Period
- **10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)**

Produced to HJC

Exhibit 62



From: ██████████@fb.com
Subject: Draft Agenda for 9/16 USG/Industry Meeting
Date: September 11, 2020 at 1:00 PM
To: ██████████@fb.com, ██████████@twitter.com, ██████████@pinterest.com, ██████████@google.com, ██████████@google.com,
 ██████████@twitter.com, ██████████@microsoft.com, ██████████@fb.com, ██████████@fb.com,
 ██████████@verizonmedia.com, ██████████@google.com, ██████████@microsoft.com, ██████████@reddit.com,
 ██████████@pinterest.com, ██████████@medium.com, ██████████@reddit.com, ██████████@twitter.com, ██████████@linkedin.com,
 ██████████@medium.com, ██████████@fb.com, ██████████@microsoft.com, ██████████@linkedin.com, ██████████@pinterest.com,
 ██████████@wikimedia.org, ██████████@verizonmedia.com, ██████████@verizonmedia.com, ██████████@microsoft.com,
 ██████████@pinterest.com, ██████████@pinterest.com, ██████████@verizonmedia.com, ██████████@reddit.com,
 ██████████@microsoft.com, ██████████@verizonmedia.com

Hello Everyone,

Below please find a proposed draft agenda for our bi-weekly industry sync coming up in about an hour – in addition, there is a plan to have another strategic comms release around the next USG/Industry meeting – a draft of that will be shared early next week and the various Comms leads from the industry participants that engaged last time are communicating on this right now.

Thanks very much for the continued collaboration, and see you shortly!

- **10 minutes: Dial In/Opening**
- **30 minutes: Threat Updates**
 - Threat update from USG -- Foreign Actor/Activity (INSERT)
 - UNCLASS Detailed DNI Threat Update Extracted From Intelligence Reports
 - Threat update from industry (TW, FB, GOOG + ANY OTHERS)
- **40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)**
 - USG Election Process Update & Virtual Election Day War Rooms
 - Delegitimization Claims of Concern
 - Amplification of Accurate Voter & Campaign Security Info
 - Timely Threat Indicator Sharing & Readiness for Post-Election Period
- **10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)**

Exhibit 63

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]E6D>
To: Scully, Brian; [REDACTED]
CC: [REDACTED]; [REDACTED]
Sent: 9/15/2020 8:06:03 AM
Subject: Re: Sep USG-Industry Meeting

Good morning, Gents!

I wanted to check-in and ask if you had any additions to the agenda or preferences on a weekly cadence of meetings in October.

Additionally, based on your comment below, it looks like USG will provide a more fulsome threat briefing tomorrow. Is that on track?

Looking forward to our discussion tomorrow!

Best,
[REDACTED]

Sent from my iPhone

On Sep 11, 2020, at 3:09 PM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Great. I just pushed the draft out to the interagency and will let you know if there are any additional proposed changes. I've also asked ODNI, FBI and DHS I&A to be prepared for a detailed threat update.

Brian

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Friday, September 11, 2020 3:08 PM
To: Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Sep USG-Industry Meeting

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.

+ [REDACTED] to provide BJJ for next week's meeting.

I think fine on virtual rooms but will share with industry and hope to revert by COB ([REDACTED] can help me with that)

Sent from my iPhone

On Sep 11, 2020, at 3:05 PM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Thanks [REDACTED]. We'll have at least one additional agenda item for the deep dive – Election Day Virtual Rooms – where CISA folks will walk through how the virtual rooms will work. I have not received any feedback from interagency on weekly, so will follow-up. Finally, do you have the BlueJeans info yet?

Have a great weekend.

Brian

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Friday, September 11, 2020 12:13 PM
To: [REDACTED] <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Sep USG-Industry Meeting

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.

Gents,

Below is the proposed draft agenda for our Sep 16th meeting. Would appreciate any feedback and wanted to call out the request for an "unclass" briefing from DNI/other parts of USG on any election related threats or possible threats that might be on radar.

Also, have you received any signal on whether there is a desire to have a weekly cadence of quick check-in meetings in October/November?

Thank you for the ongoing collaboration and look forward to "seeing" you next week!

Best,

[REDACTED]

Draft Agenda:

- **10 minutes: Dial In/Opening**
- **30 minutes: Threat Updates**
 - Threat update from USG -- Foreign Actor/Activity (INSERT)
 - UNCLASS Detailed DNI Threat Update Extracted From Intelligence Reports
 - Threat update from industry (TW, FB, GOOG + ANY OTHERS)
- **40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)**
 - USG Election Process Update
 - Delegitimization Claims of Concern
 - Amplification of Accurate Voter & Campaign Security Info
 - Timely Threat Indicator Sharing & Readiness for Post-Election Period
- **10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)**

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Friday, September 4, 2020 8:37:49 AM
To: Scully, Brian <[REDACTED]@cisa.dhs.gov>

Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Sep USG-Industry Meeting

Many thanks, Brian!

Sent from my iPhone

On Sep 4, 2020, at 8:15 AM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

[REDACTED],

Meeting on the 16th is good. I sent a hold out to government partners for that date/time. We will check on the weekly meetings and intel sharing and get back. May also be a good topic for the call.

Brian

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Friday, September 4, 2020 8:05 AM
To: [REDACTED] <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Re: Sep USG-Industry Meeting

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.

Good morning!

Following up on this before I head out for the weekend. Any thoughts about the questions below?

If we decide to move the next synch from the 9th to the 16th, I think it would be helpful for our partners to know that by COB today. Let us know what we can do to help.

Thanks—and best for a great long weekend!

[REDACTED]

From: [REDACTED] <[REDACTED]@fb.com>
Date: Tuesday, September 1, 2020 at 8:15 PM
To: "[REDACTED]@cisa.dhs.gov" <[REDACTED]@cisa.dhs.gov>, Brian Scully <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>
Subject: Sep USG-Industry Meeting

Gents,

Hope you are keeping well! Sorry for the late evening email but I am on PTO and trying to lock in a few issues for next week.

That said, with Labor day weekend approaching, we wanted to flag a few issues:

1. Would USG participants consider moving our next meeting from September 9th to September 16th in light of the coming Labor Day weekend and related schedules?

1. Would USG consider doing weekly meetings starting the week of October 14, 21, 28 (and maybe weekly meetings into November if needed)?

Final Report 1336

1. The September agenda is still a WIP—we hope to have a draft to share soon and will seek your input.
2. Additionally, would it be possible for USG to consider providing industry with the unclass version of the written briefings that DNI will provide Congress? The New York Times had a good piece on this earlier this week that made a good case why more detailed information sharing in an unclass form would be valuable (relevant excerpt below).

Thanks so much,

Shift on Election Briefings Could Create an Information Gap for Voters, New York Times, [REDACTED] and [REDACTED]

1. “The decision by the nation’s top intelligence official to halt classified, in-person briefings to Congress about foreign interference in a presidential election that is just nine weeks away exposes the fundamental tension about who needs to know this information: just the president, or the voters whose election infrastructure, and minds, are the target of the hacking?”
2. “One of the bitter lessons of the last election is that intelligence about hacking into voter registration systems and the spreading of disinformation must be handled in a very different way. Those defending against misinformation include state and city election officials; Facebook, Twitter and Google; and voters themselves, who need to know who is generating or amplifying the messages they see running across their screens.”
3. “And if they do not understand the threat assessments, they will enter the most critical phase of the election — those vulnerable weeks when everything counts and adversaries have a brief window to take their best shot — without understanding the battle space.”

Produced Pursuant to

Exhibit 64

Appointment

From: [redacted] [redacted]@google.com]
To: [redacted] [redacted]@fb.com]; [redacted] [redacted]@google.com]

Subject: Monthly USG | Industry Call
Location: [redacted]

Start: 9/16/2020 6:00:00 PM
End: 9/16/2020 7:30:00 PM
Show Time As: Tentative

Recurrence: (none)

To join the meeting on a computer or mobile phone: [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?
[redacted] Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm
PT/2pm - 330pm ET. Please do not forward or share this invitation.

If you feel someone should be added, please contact

[redacted].

Confidential - Not For Public Release

Exhibit 65

9/16/20 USG/Industry Meeting

- Als for next meeting
 - Als are (1) this virtual "war room"; (2) confirming early Oct; (3) getting elections data from DHS as promised; (4) states being afraid about our ads limitations
- I&A
 - Collection and analysis
 - Foreign actor on voter registration, systems, voter suppression -- time, place, manner
 - Monitoring Russia using over and covert exploitation by vote by mail
 - Russian state media and PROXIES (websites IDed by GEC's pillars of disinfo product)
 - Promote claims ineligible voters receiving ballots, tampered votes, overburdened USPS and states being overwhelmed
 - Consistent with US2020 primary elections where state media amplified public narratives around uncertainty around the vote
 - Get more clear cut information out there
 - How are the foreign actors messaging on CIVIL UNREST and violence
- FBI/DOJ (Brad Benavides - he's the Section Chief in charge of all FITF units)
 - Most of industry partners are tracking the same threats
 - No new TTPs or threat vectors that have not already been discussed
 - Disinfo from foreign actors making its way through social media
 - DoD looking at policy and response to synthetic content -- deepfakes -- FBI and colleagues are looking to try and better understand
 - Civil Unrest
 - Domestic and international terrorism
 - Militia groups
 - Discuss any threats to polling stations, civil workers, police, locals
 - What is the posture re PHYSICAL THREATS to the election but not otherwise tracking anything
 - Growing concerns by state and locals given the agitated climate -- physical security of election offices
 - FITF also concerned about USPERs who may want to engage in violent acts
- DHS
 - Voter registration
 - Perception and availability and online voter registration and voter lookup tools
 - TTPs around ransomware going after infrastructure
 - Director will make reference to social media collaboration
- FB
 - No shifts or trends
 - Regular public announcements and speaking to USG regularly
 - Broadly looking at 3 types of goals
 - Foreign/Russian actors
 - Hack/Leak operation - Ukraine/Biden
 - Post-election delegitimization of results
 - Efforts to what FBI said to drive or spur violence

- Google
 - Continuing enforcement against [REDACTED]
 - Damning indictment on American food and cuisine
 - Hacking threat actors being monitored, including [REDACTED]
 - State media and proxy organizations
 - OFAC-related terminations that could have election related connections
- MSFT
 - 3 primary actors -- [REDACTED]
 - More than 200 diff orgs -- campaigns, advocacy, pol parties and consultants
 - Similar to 2016 tactics against credential theft -- using obfuscation tactics and automation to enable credential theft
 - Targeted consultants serving parties and think tanks and individuals around campaigns
 - Targeted at ENTERPRISE/CORPORATE accounts
 - Not exclusively going after political actors, but also espionage targets of the [REDACTED] targets
 - [REDACTED] -- Web Bugs/Beacons
 - To determine if valid account
 - Test lures to test effectiveness of lures
 - Block web bugs and beacons to prevent compromise
 - Target Biden campaign to those directly connected or affiliated with campaign
 - [REDACTED] (Iran)
 - Espionage
 - US Political Space
 - Credential harvesting
 - Using personal email accounts
- Dates of Note / DHS Presentation
 - 11/3 -- election day
 - 12/14 -- Electoral College verifies
 - State Examples of Note
 - FL recognize that it has tight timeframes
 - PA cannot begging processing absentee ballots until election day -- lack of processing times
 - DHS will share data after validating with the states
 - Ohio State has a presidential election litigation tracker
 - Google concerned about dates shifting on deadlines
 - Russian proxies have highlighted the Iowa caucus difficulties
 - Saturday, Military and Overseas voter days, 9/19
 - Monday, 9/21, National Voter Registration Day
 - [REDACTED] CISA Mission Manager, Operational Support to the Election Community
 - Ops Centers, working with the Interagency
 - Cannot set up Slack but can join a created
 - No direct participation in federal room
 - [REDACTED] Elvis, Industry to sync separately
 - Classified and unclassified war room in Virginia -- trying to see about offering a virtual room -- need situational awareness in real time -- Slack, MSFT Teams, etc -- working through interagency and ISACs -- and bring private sector into

- analytics discussion for cyber work to be successful -- Federal and State/Local classified and unclassified chatroom
 - o MSFT Chat Rooms Maybe. . .
 - o DHS
 - Have a plan
 - Understand your options
- FB
 - o Delegitimizaition of Results
 - Know what specific claims will be
 - Govt partners to share specific claims that are anticipated so that platforms can put out accurate counter-messages
 - o What should cadence of conversation be the post-election period?
 - Can discuss next month
 - Will have more accelerated conversations in the weeks leading up
 - o Weekly sync and also through 12/14 electoral college (and tracking otherwise through inauguration)
 - o "What are the aspects of the election pre- and post- that are most ripe for foreign actors to mislead the public about so that we can amplify authentic information about the election proactively?"
 - o SDN
 - FB Approaches
 - Providing services is not an issue. They cannot spend on our platform, so we make sure they can't do that. (or make money)
 - o DHS relayed Election Officials Concerns
 - Platform restrict ad content around election will make it hard to engage with voters - We have Voting Alerts

Exhibit 66

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 9/29/2020 11:41:42 AM
To: [REDACTED] [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: [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?
- [REDACTED]

Exhibit 67

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]E6D>
To: Scully, Brian
CC: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Sent: 10/5/2020 6:41:21 AM
Subject: Re: October 2020 USG/Industry Meeting (Draft Agenda)

Great! Many thanks!

Sent from my iPhone

On Oct 5, 2020, at 9:40 AM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

[REDACTED]

Just added a bullet on election official reporting, so we can walk through the current process. Otherwise, we're good with the agenda.

Thanks,
 Brian

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Monday, October 5, 2020 7:21 AM
To: [REDACTED] <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@fb.com>
Subject: Re: October 2020 USG/Industry Meeting (Draft Agenda)

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.

Good morning!

Wanted to follow-up to see if you were ok with the schedule as noted below. If so, we will circulate —as final—with industry today.

Thanks!

Sent from my iPhone

On Sep 29, 2020, at 2:41 PM, [REDACTED] <[REDACTED]@fb.com> wrote:

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!

*******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
 - Election Official Reporting
- **10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)**

Meeting Dial-In Information:

- To join the meeting on a computer or mobile phone: [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?
- [REDACTED]

Produced to HJC

Exhibit 68

Exhibit 69

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov
Subject: RE: [EXTERNAL EMAIL] - Re: Last FITF Meeting before Elections
Date: September 29, 2020 at 1:04 PM
To: [REDACTED] [REDACTED]@reddit.com
Cc: [REDACTED] [REDACTED]@reddit.com, [REDACTED] [REDACTED]@reddit.com, [REDACTED]@reddit.com

Perfect! Just sent you all a calendar invite to lock it in. Thanks.

Regards,
 Elvis

Elvis M. Chan
 Supervisory Special Agent
 Squad CY-1, National Security
 FBI San Francisco
 Work: [REDACTED]
 Cell: [REDACTED]
 Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

From: [REDACTED] [REDACTED]@reddit.com>
Sent: Tuesday, September 29, 2020 12:47 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] <[REDACTED]@reddit.com>; [REDACTED] <[REDACTED]@reddit.com>; [REDACTED]@reddit.com
Subject: [EXTERNAL EMAIL] - Re: Last FITF Meeting before Elections

Hi Elvis,

Let's shoot for Friday, Oct. 16, at 10am.

Thanks!

On Tue, Sep 29, 2020 at 11:10 AM Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov> wrote:

Reddit folks,

Per our prior discussion, I want to put a meeting on the calendar for our last bilateral sync ahead of the election. Please let me know which of these works best for you (one hour slot). Thanks!

Monday, Oct. 12, 10 am or 1 pm PDT
 Tuesday, Oct. 13, 10 am, 12 pm, or 2 pm PDT
 Wednesday, Oct. 14, 10 am or 1 pm PDT
 Thursday, Oct. 15, 10 am PDT
 Friday, Oct. 16, 10 am or 1 pm PDT

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco

Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

--

[REDACTED]
Legal at Reddit, Inc.
(c) [REDACTED]

Exhibit 70

From: [redacted]@verizonmedia.com
To: "Chan, Elvis M. (SF) (FBI)" <[redacted]@fbi.gov >
Subject: Tentatively Accepted: FITF Meeting with Verizon Media @ Fri Oct 16,2020 1pm - 2pm (PDT) (Chan, Elvis M. (SF) (FBI))
Date: Mon, 12 Oct 2020 16:27:29 +0000
Message-ID: <[redacted]@google.com >
Attachments: invite.ics

[redacted]@verizonmedia.com has replied "Maybe" to this invitation.

FITF Meeting with Verizon Media

When Fri Oct 16, 2020 1pm – 2pm Pacific Time - Los Angeles

Where [redacted] ([map](#))

Calendar Chan, Elvis M. (SF) (FBI)

- Who**
- Chan, Elvis M. (SF) (FBI) - organizer
 - [redacted]@verizonmedia.com - creator
 - [redacted] (CID) (FBI)
 - [redacted] (SF) (FBI)
 - [redacted] ([redacted]@verizonmedia.com)
 - [redacted] (CD) (FBI)
 - [redacted]
 - [redacted] (SF) (FBI)
 - [redacted] OGC (FBI)
 - [redacted] (MH) (FBI)
 - Dehmlow, Laura E. (CD) (FBI)
 - [redacted]
 - [redacted] (CID) (FBI)
 - [redacted] (CID) (FBI)
 - [redacted] SF) (FBI)
 - [redacted] (CYD) (FBI) - optional
 - [redacted] (SF) (FBI) - optional
 - [redacted] (TD) (FBI) - optional

Attachments [~WRD0004.jpg](#)

Please forward to whomever you deem appropriate. Agenda TBD.

From: [redacted] >
Sent: Tuesday, September 29, 2020 1:18 PM
To: [redacted] >
Cc: [redacted] ([redacted]@verizonmedia.com) >; Chan, Elvis M. (SF) (FBI) >; [redacted] >
Subject: [EXTERNAL EMAIL] - Re: [E] Last FITF Meeting before Election

Let try for the 16th @ 1pm PT.

On Tue, Sep 29, 2020 at 4:15 PM [redacted] > wrote:

The 14th or 16th at 1pm seems to work best for me. The 12th is Indigineous Peoples Day and my kids are off, so that will be slightly harder.

On Tue, Sep 29, 2020 at 11:09 AM Chan, Elvis M. (SF) (FBI) > wrote:

Paranoids,

Per our prior discussion, I want to put a meeting on the calendar for our last bilateral sync ahead of the election. Please let me know which of these works best for you (one hour slot). Thanks!

Monday, Oct. 12, 10 am or 1 pm PDT

Tuesday, Oct. 13, 10 am, 12 pm, or 2 pm PDT

Wednesday, Oct. 14, 10 am or 1 pm PDT

Thursday, Oct. 15, 10 am PDT

Friday, Oct. 16, 10 am or 1 pm PDT

Regards,

Elvis

Elvis M. Chan

Supervisory Special Agent

Squad CY-1, National Security

FBI San Francisco

Work: [REDACTED]

Cell: [REDACTED]

Email: [REDACTED]@fbi.gov

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

--

[Image removed by sender.]

[Redacted]

CISO & Chief Paranoid
The Paranoids

M [Redacted]
@TheParanoids

[Redacted]
San Francisco, CA [Redacted]

--

[Image removed by sender.]

[Redacted]

Senior Manager
Paranoids - Advanced Cyber Threats Team

M [Redacted]
[Redacted]

Washington, DC [Redacted]

Invitation from [Google Calendar](#)

You are receiving this courtesy email at the account [Redacted]@fbi.gov because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at <https://www.google.com/calendar/> and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. [Learn More](#)

Exhibit 71

Appointment

From: [redacted] [redacted]@google.com]
To: [redacted] [redacted]@fb.com]; [redacted] [redacted]@google.com]

Subject: Monthly USG | Industry Call

Start: 7/8/2020 6:00:00 PM

End: 7/8/2020 7:30:00 PM

Show Time As: Busy

Recurrence: (none)

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [redacted].

Ways to Join

Computer or Mobile:

Facebook Meeting Room or Portal:

Use the touch panel in your room or Portal to enter the join code [redacted]

Telephone:

Dial in on [redacted] or find an alternative number [redacted] then enter [redacted]

Confidential - Not For Public Release

Exhibit 72

- [REDACTED]
- [REDACTED]
- [REDACTED]@reddit.com
- [REDACTED]@reddit.com
- [REDACTED]
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@twitter.com
- [REDACTED]
- [REDACTED]
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@twitter.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED] - optional
- [REDACTED] - optional

more details »

Changed: To join the meeting on a computer or mobile phone:

One-Touch: [REDACTED] Meeting ID: [REDACTED]
 Participant Passcode: [REDACTED] To join via phone: () Dial: [REDACTED] (2) Enter Conference ID: [REDACTED]
 (3) Enter Participant Passcode: [REDACTED] Want to test your video connection? [REDACTED]

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [REDACTED]@fb.com.

Invitation from Google Calendar

You are receiving this email at the account [REDACTED]@google.com because you are subscribed for updated invitations on calendar [REDACTED]

To stop receiving these emails, please log in to <https://www.google.com/calendar/> and change your notification settings for this calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. [Learn More](#).

Confidential - Not For Public Release

Exhibit 73

Appointment

From: Google Calendar [redacted]@google.com]
on behalf of [redacted] [redacted]@google.com]
Sent: 10/12/2020 9:47:21 PM
To: [redacted] [redacted]@fb.com]

Subject: Weekly USG | Industry Call
Attachments: invite.ics
Location: [redacted]

Start: 10/21/2020 6:00:00 PM
End: 10/21/2020 6:30:00 PM
Show Time As: Tentative

Recurrence: (none)

[redacted] has accepted this invitation.

Weekly USG | Industry Call

When Wed Oct 21, 2020 11am - 11:30am Pacific Time - Los Angeles

Where [redacted] (map)

Calendar [redacted]

- Who
- organizer
- creator
n.com
@twitter.com
@verizonmedia.com
@medium.com
@reddit.com
@pinterest.com
@verizonmedia.com
ini
@microsoft.com
@pinterest.com
@twitter.com
@verizonmedia.com
@linkedin.com
@twitter.com
@wikimedia.org

- [REDACTED]
- [REDACTED]
- [REDACTED]@pinterest.com
- [REDACTED]@twitter.com
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]@reddit.com
- [REDACTED]
- [REDACTED]@reddit.com
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@microsoft.com
- [REDACTED]@twitter.com
- [REDACTED]@twitter.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@linkedin.com - optional
- [REDACTED]@twitter.com - optional
- [REDACTED] - optional

To join the meeting on a computer or mobile phone: [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?

[REDACTED]

Please do not forward or share this invitation. If you feel someone should be added, please contact [REDACTED]@fb.com.

Invitation from Google Calendar

You are receiving this courtesy email at the account [REDACTED]@fb.com because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at <https://www.google.com/calendar/> and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. [Learn More](#).

Confidential - Not For Public Release

Exhibit 74

Appointment

From: Google Calendar [redacted]@google.com]
 on behalf of [redacted] [redacted]@google.com]
Sent: 10/16/2020 5:06:04 PM
To: [redacted] [redacted]@google.com]; [redacted]@linkedin.com; [redacted]@twitter.com;
 [redacted]@verizonmedia.com; [redacted]@medium.com; [redacted]@reddit.com; [redacted]@pinterest.com; [redacted]
 [redacted]@fb.com]; [redacted] [redacted]@fb.com]; [redacted]@verizonmedia.com; [redacted]
 [redacted]@fb.com]; [redacted] [redacted]@fb.com]; [redacted]@microsoft.com; [redacted]@pinterest.com];
 [redacted] [redacted]@fb.com]; [redacted]@twitter.com; [redacted]@verizonmedia.com; [redacted]
 [redacted]@google.com]; [redacted]@linkedin.com; [redacted]@twitter.com; [redacted]@wikimedia.org;
 [redacted] [redacted]@fb.com]; [redacted] [redacted]@fb.com]; [redacted]@fb.com];
 [redacted]@pinterest.com; [redacted]@twitter.com; [redacted]@google.com]; [redacted]
 [redacted]@fb.com]; [redacted] [redacted]@fb.com]; [redacted]@fb.com]; [redacted]@reddit.com;
 [redacted] [redacted]@pinterest.com]; [redacted]@reddit.com; [redacted]@twitter.com; [redacted]@verizonmedia.com;
 [redacted]@verizonmedia.com; [redacted]@microsoft.com; [redacted]@twitter.com; [redacted]
CC: [redacted]@linkedin.com; [redacted]@twitter.com; [redacted]@fb.com]; [redacted]@twitter.com; [redacted]
 [redacted]@linkedin.com]

Subject: Weekly USG | Industry Call
Attachments: invite.ics
Location: [redacted]

Start: 10/28/2020 6:00:00 PM
End: 10/28/2020 6:30:00 PM
Show Time As: Tentative

Recurrence: (none)

This event has been changed.

Weekly USG | Industry Call
 When Wed Oct 28, 2020 11am – 11:30am Pacific Time - Los Angeles
 Where Changed: [redacted] (map)
 Calendar [redacted]
 Who

- [redacted]
- [redacted] cre
- [redacted]@linkedin.com
- [redacted]@twitter.com
- [redacted]@verizonmedia.com
- [redacted]@medium.com
- [redacted]@reddit.com
- [redacted]@pinterest.com
- [redacted]@verizonmedia.com

- [REDACTED]@microsoft.com
- [REDACTED]@pinterest.com
- [REDACTED]
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]
- [REDACTED]
- [REDACTED]@linkedin.com
- [REDACTED]@twitter.com
- [REDACTED]@wikimedia.org
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]@pinterest.com
- [REDACTED]@twitter.com
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]@reddit.com
- [REDACTED]
- [REDACTED]@reddit.com
- [REDACTED]@twitter.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@verizonmedia.com
- [REDACTED]@microsoft.com
- [REDACTED]@twitter.com
- [REDACTED]
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@microsoft.com
- [REDACTED]@linkedin.com - optional
- [REDACTED]@twitter.com - optional
- [REDACTED]
- [REDACTED]@twitter.com - optional
- [REDACTED]

Not For Public Release

[more details »](#)

Changed: Join Zoom Meeting

[REDACTED]

Meeting ID: [REDACTED]

Passcode: [REDACTED]

One tap mobile

[REDACTED] US (San Jose)

[REDACTED] US (Tacoma)

Dial by your location

[REDACTED] US (San Jose)

[REDACTED] US (Tacoma)

[REDACTED] (Houston)
[REDACTED] (Chicago)
[REDACTED] (New York)
[REDACTED] (Germantown)

US Toll-free
US Toll-free
US Toll-free
US Toll-free

Meeting ID: [REDACTED]

Passcode: [REDACTED]

Find your local number: [REDACTED]

For any questions regarding this invite, please reach out to [REDACTED] at [REDACTED]@fb.com

Invitation from [Google Calendar](#)

You are receiving this email at the account [REDACTED]@google.com because you are subscribed for updated invitations on calendar [REDACTED]

To stop receiving these emails, please log in to <https://www.google.com/calendar/> and change your notification settings for this calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. [Learn More.](#)

Confidential - Not For Public Release

Exhibit 75

Exhibit 76

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]69D>

To: [REDACTED]@google.com; [REDACTED]@google.com; [REDACTED]@twitter.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@linkedin.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com; [REDACTED]@google.com; [REDACTED]@reddit.com; [REDACTED]@pinterest.com; [REDACTED]@pinterest.com; [REDACTED]@medium.com; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]@microsoft.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]; [REDACTED]; [REDACTED]@wikimedia.org; [REDACTED]@reddit.com; [REDACTED]@medium.com; [REDACTED]@twitter.com; [REDACTED]@linkedin.com; [REDACTED]@linkedin.com; [REDACTED]; [REDACTED]@verizonmedia.com

CC: [REDACTED]; [REDACTED]

Sent: 7/14/2020 3:11:43 PM

Subject: Dial In Information: 7/15 Monthly USG | Industry Call

Hello Everyone,

Three quick updates before tomorrow:

- Below please find the WebEx dial-in information for the Wednesday, 7/15 USG/Industry call.
- Starting in August onwards, we will migrate to using a BJN for our calls, and that information will be forthcoming.
- Here is the planned agenda (as discussed at our bi-weekly last Friday):
 - 10 minutes: Dial In/Opening
 - 30 minutes: Threat Updates
 - Threat update from USG (FBI, I&A)
 - Threat update from industry (FB, TW, GOOG)
 - 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 - Election process update from USG
 - Hack/Leak and USG Attribution Speed/Process
 - Vote-by-mail: How do we deal with the gap between Nov 3 and results?
 - 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

Thank you for your engagement and commitment here, and look forward to seeing you tomorrow.

USG/Industry Webex meeting.

Meeting number (access code): [REDACTED]

Meeting password: [REDACTED]

Wednesday, July 15, 2020

2:00 pm | (UTC-04:00) Eastern Time (US & Canada) | 1 hr 30 mins

-----Original Appointment-----

From: [REDACTED]
Sent: Monday, July 6, 2020 8:32 PM
To: [REDACTED]; [REDACTED]@google.com; [REDACTED]@google.com; [REDACTED]@twitter.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@microsoft.com; [REDACTED]@linkedin.com; [REDACTED]@verizonmedia.com; [REDACTED]@verizonmedia.com;

[Join meeting](#)

Tap to join from a mobile device (attendees only)

[Redacted] US Toll

Join by phone

[Redacted] US Toll

[Global call-in numbers](#)

Join from a video system or application

Dial [Redacted]


Join using Microsoft Lync or Microsoft Skype for Business

Dial [Redacted]


Need help? Go to <http://help.webex.com>

should be added, please contact [Redacted]@fb.com.


Ways to join

 Computer or Mobile:

[Redacted]

 Facebook Conference Room and Portal:

Use the touch panel to enter the join code [Redacted]

 Telephone:

Dial in on [Redacted] or find [an alternative number](#) then enter [Redacted]

Enabled by **OneVC**

[Redacted]@verizonmedia.com;
[Redacted]@google.com;
[Redacted]@reddit.com;
[Redacted]@pinterest.com;
[Redacted]@pinterest.com; [Redacted]@medium.com;
[Redacted];
[Redacted];
[Redacted]@microsoft.com;
[Redacted]@twitter.com; [Redacted]@twitter.com;
[Redacted]; [Redacted];
[Redacted]@wikimedia.org;
[Redacted]@reddit.com; [Redacted]@medium.com;
[Redacted]@twitter.com
Cc: [Redacted]@twitter.com; [Redacted]@linkedin.com;
[Redacted]@linkedin.com; [Redacted]

Final Report 1375

Subject: Monthly USG | Industry Call
When: Wednesday, July 15, 2020 11:00 AM-12:30 PM (UTC-08:00) Pacific Time (US & Canada).
Where:

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone

Produced to [Redacted]

Exhibit 77

From: [REDACTED] /O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=90EE91676BAF4A1B858AB16C9585BD01-SWANTNERS>
To: [REDACTED]
Sent: 7/14/2020 6:53:50 PM
Subject: Fwd: Dial In Information: 7/15 Monthly USG | Industry Call

You good to go on this?

Top things to keep your ears peeled for are I3 or Security Policy talking about sharing protocols with gov't. We'll need to understand how we'll be involved.

[REDACTED]

Facebook Law Enforcement Outreach

[REDACTED]

Begin forwarded message:

From: [REDACTED]@fb.com>
Date: July 14, 2020 at 3:11:44 PM PDT
To: [REDACTED]@google.com>, [REDACTED]@google.com>, "voel@twitter.com" <voel@twitter.com>, [REDACTED]@microsoft.com>, [REDACTED]@microsoft.com>, [REDACTED]@microsoft.com>, [REDACTED]@linkedin.com", [REDACTED]@linkedin.com>, [REDACTED]@verizonmedia.com>, [REDACTED]@verizonmedia.com>, [REDACTED]@verizonmedia.com>, [REDACTED]@google.com>, [REDACTED]@reddit.com>, [REDACTED]@pinterest.com>, [REDACTED]@pinterest.com>, [REDACTED]@medium.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@microsoft.com", [REDACTED]@microsoft.com>, [REDACTED]@twitter.com>, [REDACTED]@twitter.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@wikimedia.org", [REDACTED]@wikimedia.org>, [REDACTED]@reddit.com>, [REDACTED]@medium.com>, [REDACTED]@twitter.com>, [REDACTED]@linkedin.com", [REDACTED]@linkedin.com>, [REDACTED]@linkedin.com>, [REDACTED]@linkedin.com>, [REDACTED]@verizonmedia.com", [REDACTED]@verizonmedia.com>
Cc: [REDACTED]@fb.com>, [REDACTED]@fb.com>
Subject: Dial In Information: 7/15 Monthly USG | Industry Call

Hello Everyone,

Three quick updates before tomorrow:

- Below please find the WebEx dial-in information for the Wednesday, 7/15 USG/Industry call.
- Starting in August onwards, we will migrate to using a BJN for our calls, and that information will be forthcoming.

- Here is the planned agenda (as discussed at our bi-weekly last Friday):
 - 10 minutes: Dial In/Opening
 - 30 minutes: Threat Updates
 - Threat update from USG (FBI, I&A)
 - Threat update from industry (FB, TW, GOOG)
 - 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
 - Election process update from USG
 - Hack/Leak and USG Attribution Speed/Process
 - Vote-by-mail: How do we deal with the gap between Nov 3 and results?
 - 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

Thank you for your engagement and commitment here, and look forward to seeing you tomorrow.

USG/Industry Webex meeting.

Meeting number (access code): [REDACTED]

Meeting password: [REDACTED]

Wednesday, July 15, 2020

2:00 pm | (UTC-04:00) Eastern Time (US & Canada) | 1 hr 30 mins

[Join meeting](#)

Tap to join from a mobile device (attendees only)

[REDACTED] US Toll

-----Original Appointment-----

From: [REDACTED]@fb.com>
Sent: Monday, July 6, 2020 8:32 PM
To: [REDACTED]@google.com;
 [REDACTED]@google.com; yoel@twitter.com;
 [REDACTED]@microsoft.com;
 [REDACTED]@microsoft.com;
 [REDACTED]@microsoft.com;
 [REDACTED]@microsoft.com;
 [REDACTED]@linkedin.com;
 [REDACTED]@verizonmedia.com;
 [REDACTED]@verizonmedia.com;
 [REDACTED]@verizonmedia.com;
 [REDACTED]@google.com;
 [REDACTED]@reddit.com;
 [REDACTED]@pinterest.com;
 [REDACTED]@pinterest.com;
 [REDACTED]@medium.com; [REDACTED]
 [REDACTED]
 [REDACTED]@microsoft.com;
 [REDACTED]@twitter.com; [REDACTED]@twitter.com;
 [REDACTED]
 [REDACTED]@wikimedia.org;
 [REDACTED]@reddit.com;
 [REDACTED]@medium.com; [REDACTED]@twitter.com
Cc: yoelr@twitter.com;

Join by phone

[Redacted] US Toll

[Global call-in numbers](#)

Join from a video system or application

Dial [Redacted]

Join using Microsoft Lync or Microsoft Skype for Business


Dial [Redacted]

Need help? Go to <http://help.webex.com>


Ways to join

 Computer or Mobile:

[Redacted]

 Facebook Conference Room and Portal:

Use the touch panel to enter the join code [Redacted]

 Telephone:

Dial in on [Redacted] or find [an alternative number](#) then enter [Redacted]

Enabled by OneVC

[Redacted]@linkedin.com [Redacted]@linkedin.com;
Final Report 1379

Subject: Monthly USG | Industry Call
When: Wednesday, July 15, 2020 11:00 AM-12:30 PM (UTC-08:00) Pacific Time (US & Canada).
Where:

Recurrence will be second Wednesday from May to December 2020, 11am - 1230pm PT/2pm - 330pm ET. Please do not forward or share this invitation. If you feel someone should be added, please contact [Redacted]@fb.com.

Produced for HJC

Exhibit 78

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 9/17/2020 12:55:58 PM
To: lobbyists [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]
Subject: HPM USG-Industry Monthly Election Integrity Meeting (September)

Team,

Sharing our HPM from this week's USG-Industry meeting on election integrity and the link to our successfully-landed Joint Industry Statement. Great XFN collaboration on this continues (many thanks to [REDACTED], [REDACTED], [REDACTED] & [REDACTED]).

Let us know if you have any questions.

United States: USG-Industry Monthly Election Integrity Meeting (September)

- What happened:** On Wednesday, September 16, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our i3 Threat Team participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. We again successfully landed a Joint Industry Statement regarding our long-standing and ongoing efforts to secure US2020 in collaboration with the USG entities charged with securing the election, available here: <https://twitter.com/fbnewsroom/status/1306314722082349056?s=20>. Co-signatories included Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia. USG attendees included senior officials from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the seventh such convening to prepare for US2020, the fifth call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- Why relevant:** The discussion focused on timely sharing accurate voting and election information, countering targeted attempts to undermine the election conversation, preparing for "hack and leak" operations attempting to use platforms and traditional media to amplify unauthorized information drops, and mitigation efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.
- Next Steps:** We will continue to participate in these calls with our tech peers & USG partners through the end of 2020. The next monthly convening will occur on October 7th. We will then transition to weekly calls to check-in & share information through the December 14th Electoral College meeting.

Exhibit 79

Message

From: [REDACTED]@fb.com]
Sent: 10/14/2020 9:57:57 AM
To: [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbId":null,"threadFbId": [REDACTED]}]

[REDACTED] (10/14/2020 09:51:46 PDT):
>hi both

[REDACTED] (10/14/2020 09:52:52 PDT):
>qq - we didn't get anything from the FBI this morning on the NY Post issue did we? we were reaching out reactively correct?

[REDACTED] (10/14/2020 09:55:01 PDT):
>That's right [REDACTED]

[REDACTED] (10/14/2020 09:55:18 PDT):
>Nothing from them, we are reaching out to find out more

[REDACTED] (10/14/2020 09:57:57 PDT):
>Hi - confirming from i3 side as I checked with [REDACTED] [REDACTED] ..and myself. 1/ No proactive outreach from anyone at FBI that we're aware of on i3 2/ [REDACTED] will be on a call with FITF/FBI here in 5min that [REDACTED] is also on.

Produced to HSC

Exhibit 80

Message

From: [REDACTED] [REDACTED]@fb.com]
Sent: 10/8/2020 10:24:28 AM
To: lobbyists [REDACTED]@fb.com]
CC: [REDACTED] [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]; [REDACTED] [REDACTED]@fb.com]; [REDACTED]
Subject: USG-Industry Monthly Election Integrity Meeting (October)

Team,

Sharing our HPM from this week's USG-Industry meeting on election integrity. Great XFN collaboration on this continues (many thanks to [REDACTED], [REDACTED], [REDACTED] & [REDACTED]).

Let us know if you have any questions.

[REDACTED]

United States: USG-Industry Monthly Election Integrity Meeting (October)

- What happened:** On Wednesday, October 7, U.S. Public Policy along with Security Policy, Cybersecurity Legal, Law Enforcement Outreach, and our i3 Threat Team participated in our monthly U.S. Government-Industry Election Integrity call to coordinate security efforts for the U.S. 2020 election. Participants included Facebook, Google, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, and Wikimedia. USG attendees included senior officials from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); the FBI Foreign Influence Task Force; DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI). This was the eighth such convening to prepare for US2020, the sixth call in our series of USG-Industry monthly calls leading up to the November election, and further strengthened and deepened our collaboration with industry and USG.
- Why relevant:** The discussion focused on efforts to identify and mitigate delegitimization claims against US2020 electoral outcomes, including potential hack/leak scenarios, operational readiness of states and localities for administering the vote, and timely election-related information sharing via elections operations.
- Next Steps:** We will continue to participate in these calls with our tech peers & USG partners through the end of 2020. The meetings will now shift to a weekly 30 minute cadence where we will share information through the December 14th Electoral College meeting.

Exhibit 81

Message

From: ██████████ [/O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=ZAIDAZAID87B]
Sent: 9/19/2020 12:30:19 PM
To: ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com; ██████████@fb.com
Subject: Message summary [{"otherUserFbId":null,"threadFbId":██████████}
Attachments: sticker.png; sticker.png; sticker.png

██████████ (9/19/2020 09:56:51 PDT):
 >Hey ██████████ - just wanted to make sure you all had visibility into this and some context. ██████████ and I were alerted to this last night and this morning. ██████████ flagged (and was asking some clarifying questions) for a review that's happening tomorrow (Sunday). He wrote this morning as a TLDR:

██████████ (9/19/2020 09:56:54 PDT):
 >██████████ asked to review our preparedness this Sunday for a scenario in which there are claims/allegations of an off-platform hack related to US 2020 election, and the content may be disseminated on-platform. We expect such a release of potentially hacked content in the near term (but we're not 100% sure.)
 >
 >In this scenario, we wanted to understand how news curation would address reports on the claimed/alleged hack. Specifically, hoping to understand whether this is something that can be dealt with under the existing curation guidelines, or whether we should consider specific guidelines for this.

██████████ (9/19/2020 09:57:37 PDT):
 >I understand the meeting is happening at 9am PT, if you aren't already invited

██████████ (9/19/2020 10:10:44 PDT):
 >Yep. We are on a similar meeting on a different topic now.

██████████ (9/19/2020 10:11:24 PDT):

shared: sticker.png

██████████ (9/19/2020 10:14:13 PDT):
 >Thanks ██████████

██████████ (9/19/2020 10:25:56 PDT):
 >do we have internal guidance on how we determine whether something is hack or a leak? is it right that we remove content that is the product of a hack but allow content that is the product of a leak

██████████ (9/19/2020 10:25:58 PDT):
 >?

██████████ (9/19/2020 10:35:24 PDT):
 >Yes - that is correct

██████████ (9/19/2020 10:35:26 PDT):
 >And yes we do

██████████ (9/19/2020 10:35:36 PDT):
 >Sorry - was taking care of something and just seeing

██████████ (9/19/2020 10:35:40 PDT):
 >Do you still need?

██████████ (9/19/2020 10:36:04 PDT):
 >Heck, I don't need this until 9am pt tomorrow.

██████████ (9/19/2020 10:36:14 PDT):
 >Ah perfect - will send in a bit

██████████ (9/19/2020 10:36:17 PDT):
 >But yes we do

██████████ (9/19/2020 10:36:48 PDT):
 >we also have some safety exceptions around leaks, right ██████████? Like the whistleblowers name?

██████████ (9/19/2020 10:37:36 PDT):

shared: sticker.png

[REDACTED] (9/19/2020 10:38:58 PDT):
>How would we respond to a proposal to allow us to remove leaks "when linked to a foreign interference operation for a government" ?

[REDACTED] (9/19/2020 10:39:10 PDT):
>I Anticipate getting that ask at our meeting tomorrow.

[REDACTED] (9/19/2020 10:39:36 PDT):
>It feels like we would often not have that evidence, and it's squishy as hell. But tbh, it could be useful as a simple signaling function and a tool of last resort if we want it.

[REDACTED] (9/19/2020 11:13:11 PDT):
>so - here is how we differentiate in our KQs:

[REDACTED] (9/19/2020 11:13:15 PDT):
>U. What is the definition of "hacked" and how is it different from "leaked"?
>Hacking is a criminal activity: when an individual intentionally accessed data through digital devices (phone, computer, tablet, cloud, etc.) without authorization, the material is hacked. We say things are "leaked" when content is shared with an unintended audience without permission. The leaker had valid access to the data.

>
>V. What is the definition of "claimed or confirmed to come from a hacked source"?
>The caption states the shared content are from a hacked source OR we know from a third party channel that the displayed content were hacked.

[REDACTED] (9/19/2020 11:13:55 PDT):
>and then is also a related (though not entirely relevant KQ) for reference):

[REDACTED] (9/19/2020 11:13:56 PDT):
>L. Do we allow content that coordinates hacking?
>No. We remove statements of intent, calls to actions, representation or support of hacking, as well as depicting, admitting to or speaking positively of acts committed by the poster or associates, when the intent is to gain unauthorized access to data, accounts, systems or computers, hijack a domain, corrupt or disrupt cyber systems or seek ransoms The following activities are not allowed in the platform (not-exhaustive):
>Offering/Requesting services to hack accounts - ex. Facebook, Whatsapp, Email accounts, ...
>Offering services to access unauthorized data - ex. phone/laptop camera or data, criminal/university records,
>Threats/ statements of intent to hack, including web defacements and denial of service attacks
>Giving instructions/ tutorials on how to hack in order to gain access to unauthorized data or accounts
>However, we allow coordination of ethical or 'white hat' hacking services, when it's clear by the context that the intent is not to gain unauthorized access to data, accounts or systems, and when the post does not include information that can be used in a malicious way, such as (not-exhaustive)
>Offering/ requesting services/ calls for action for hacking without malicious intent being established (ex. "I'm looking for an hacker") or in the context of cybersecurity - except if the post includes explicit instructions/tutorials that can be used for non-ethical hacking
>Coordinate hackathons with benign intent
>Discuss the legality of hacking

[REDACTED] (9/19/2020 11:14:07 PDT):
>for all of us to keep in mind

[REDACTED] (9/19/2020 11:14:16 PDT):
>we should be really diligent about our lexicon and language in these conversations

[REDACTED] (9/19/2020 11:14:29 PDT):
>and careful about using the words hack and leak interchangeably - since we have drawn the line in our policies

[REDACTED] (9/19/2020 11:14:49 PDT):
>so [REDACTED] - to that point - want to make sure you meant to use the word Leak above in your question?

[REDACTED] (9/19/2020 11:15:24 PDT):
>but fundamentally, when it comes to foreign interference, to your point i think it will be very hard for us to determine

[REDACTED] (9/19/2020 11:15:29 PDT):
>and not sure we have ever really run into this

[REDACTED] (9/19/2020 11:15:46 PDT):
>though some of the ukraine stuff 2-3 years ago (would have to dig up) came close

[REDACTED] (9/19/2020 11:15:53 PDT):
>[REDACTED] - does this help?

[REDACTED] (9/19/2020 11:18:07 PDT):
>I did intentionally mean to use leak

[REDACTED] (9/19/2020 11:18:25 PDT):
>Q is should we expand where it is a *leak* linked to a known foreign interference campaign.

[REDACTED] (9/19/2020 11:18:55 PDT):
>In the upcoming cycle, we're actually likely to be reasonably confident, but unable to prove publicly.

[REDACTED] (9/19/2020 11:19:03 PDT):
>So ther is a question of our confidence tolerance.

[REDACTED] (9/19/2020 11:19:15 PDT):
>But if Russian actors drop a Burisma leak in the next two weeks

[REDACTED] (9/19/2020 11:19:25 PDT):
>(Which is likely & we are actively prepping for it)

[REDACTED] (9/19/2020 11:19:32 PDT):
>I doubt we'll be able to prove it is hacked.

[REDACTED] (9/19/2020 11:20:34 PDT):
>It's Snowden versus Podesta, right? Snowden had lawful access to the materials. He unlawfully took them and shared with an unintended audience. Podesta never intentionally shared anything.

[REDACTED] (9/19/2020 11:22:23 PDT):
>So today we'd leave Snowden materials up but take Podesta materials down. Is that right?

[REDACTED] (9/19/2020 11:22:50 PDT):
>Or does Snowden's illegality play into our assessment?

[REDACTED] (9/19/2020 11:23:36 PDT):
>(Setting aside entirely the idea that we're going to know anything about any of this at the moment the materials appear on FB.)

[REDACTED] (9/19/2020 11:24:03 PDT):
>yeah fair question.

[REDACTED] (9/19/2020 11:24:41 PDT):
>1) i am not sure that Snowden had valid access to what he put out, or at least not all of it. so there would be that question

[REDACTED] (9/19/2020 11:25:09 PDT):
>2) obviously if there were confidential information, classified or PII would be removed

[REDACTED] (9/19/2020 11:25:49 PDT):
>3) but yes, there is a delicate balance of whether content leaked (by a whistleblower or otherwise) is allowed...

[REDACTED] (9/19/2020 11:26:45 PDT):
>Actually, It's Snowden + conclusive evidence that Snowden was in fact controlled by the Russians.

[REDACTED] (9/19/2020 11:26:54 PDT):
>And the Q is whether those two factors combined are sufficient for us to act.

[REDACTED] (9/19/2020 11:28:05 PDT):
>We are likely to have in the next few weeks a leak or series of leaks about Biden's supposed link to Burisma, where we won't be able to prove they were "hacked", but where we will have responsible USG players publicly saying this is part of a foreign influence operation, our own assessment will align that this is a Russian op, and we will hear from our trusted secret squirrel partners that this is a Russian op.

[REDACTED] (9/19/2020 11:28:24 PDT):
>I doubt we'll have a public smoking gun to prove that, but the circumstantial public evidence will be quite strong.

[REDACTED] (9/19/2020 11:29:04 PDT):
>The Q is whether in that case, we want to be empowered to take stronger action. I could see either (a) removal; or (b) position ourselves to put a label on the content.

[REDACTED] (9/19/2020 11:30:12 PDT):
>Obviously there are significant ops implications for finding all of this content, and we would have at best imperfect execution. That could be a reason not to do this as well. But right now we could be described as having a "policy gap," and I expect we'll get pressure there.

[REDACTED] (9/19/2020 11:31:49 PDT):
>i would think that we would default to consider that hacked material and remove it

[REDACTED] (9/19/2020 11:31:59 PDT):
>based ont he definitions i provided above

[REDACTED] (9/19/2020 11:32:09 PDT):
>and to your point until there is conclusive evidence or narrative in the public domain

[REDACTED] (9/19/2020 11:32:15 PDT):
>but I am simplistic on this stuff

[REDACTED] (9/19/2020 11:32:17 PDT):
shared: sticker.png

[REDACTED] (9/19/2020 11:32:19 PDT):
>so I might be missing hte obvious right now!

[REDACTED] (9/19/2020 11:32:31 PDT):
>we likely won't have any evidence of hacking

[REDACTED] (9/19/2020 11:32:41 PDT):
>right but we won't know who "leaked" it?

[REDACTED] (9/19/2020 11:32:48 PDT):
>so we should default to more protection

[REDACTED] (9/19/2020 11:32:49 PDT):
>So I'm not sure how we'd know

[REDACTED] (9/19/2020 11:32:52 PDT):
>assume it was hacked

[REDACTED] (9/19/2020 11:32:55 PDT):
>right

[REDACTED] (9/19/2020 11:33:02 PDT):
>so without evidence

[REDACTED] (9/19/2020 11:33:05 PDT):
>default to hacked and remove

[REDACTED] (9/19/2020 11:33:55 PDT):
>what if it is a person who claims to be a Burisma employee, who is blowing the whistle on all this horrible behavior based on their deep and abiding sense of conscience and fair play?

[REDACTED] (9/19/2020 11:34:22 PDT):
>And while there is dispute about how authentic this person is, we can't *prove* they are lying (and we'd have to basically judge the truth/falsity of their claims to do so)

[REDACTED] (9/19/2020 11:35:40 PDT):
>yeah super tricky

[REDACTED] (9/19/2020 11:35:41 PDT):
>right

[REDACTED] (9/19/2020 11:36:05 PDT):
>we have, int he past, and I think it makes sense make room for whistleblower content.

[REDACTED] (9/19/2020 11:36:08 PDT):
>hanging our hat on hacked v leaked means we have to get into that world, and we will get a bunch of external criticism for quibbling over hack/leak.

[REDACTED] (9/19/2020 11:36:12 PDT):
>e.g., what about the pentagon papers?

[REDACTED] (9/19/2020 11:36:22 PDT):
>yes

[REDACTED] (9/19/2020 11:36:23 PDT):
>esp. in comparison to other platforms, who will be able to move faster here.

[REDACTED] (9/19/2020 11:36:28 PDT):
>and always have in past scenarios

[REDACTED] (9/19/2020 11:36:44 PDT):
>For example:

[REDACTED] (9/19/2020 11:36:49 PDT):
>My suggestion of adding "leaked as part of a foreign influence campaign by a government" would avoid that problem.

[REDACTED] (9/19/2020 11:36:56 PDT):
 >Recent Examples of Hi-Profile Hacked Content Impacting the Platform
 >Importantly, we have dealt with at least three high profile allegations of hacked materials being spread virally on social media. We dealt with two of the three escalations below before our hacked content policy went live on December 13, 2017.
 >
 >First, in May 2017, Emmanuel Macron's emails were hacked and leaked. We geo-blocked the content under local law because French election law prohibits the dissemination of any electoral propaganda during the 48 hours leading up to an election. Legal and outside counsel advised [REDACTED].
 >
 >Second, during the German elections in 2017, German authorities worried that emails obtained by hackers in a 2015 cyber attack on the German parliament would be leaked before the September 24, 2017 election. Ultimately, the hacked materials did not materialize, but Organic Content Policy worked with an XFN team to prepare for the possible leak or usage of the hacked emails in the election.
 >
 >Third, in 2019, the Chilean police was hacked, and the leaked documents contained various types of information, including names, Tax ID numbers, and other personal information of police officers. The office of the President of Chile contacted us concerning a website that was using the PII to call for harmful actions against police officers. We removed the hacked materials for violation of our Privacy Violations policy, and we blackholed the websites that were disseminating the information.
 >
 >These examples provide precedent for how we would analyze the dissemination of materials that may result from a hack of Burisma.

[REDACTED] (9/19/2020 11:37:12 PDT):
 >i like that

[REDACTED] (9/19/2020 11:37:29 PDT):
 >i think we should have someone on your team and my team run on this on monday

[REDACTED] (9/19/2020 11:37:40 PDT):
 >and get it up to [REDACTED]/leadership for consideration

[REDACTED] (9/19/2020 11:37:45 PDT):
 >once we kick the tires on it a little

[REDACTED] (9/19/2020 11:37:53 PDT):
 >The worry with this is that explicit "hacking" are the ops we saw in 2016-2019, but the history of this type of operation has generally *not* been through explicit hacking. The next op we see will likely be not provably hacking.

[REDACTED] (9/19/2020 11:37:58 PDT):
 >let's not get caught up in the chaos right now

[REDACTED] (9/19/2020 11:38:08 PDT):
 >that is my only caution

[REDACTED] (9/19/2020 11:38:12 PDT):
 >I'm good with that -- but we will be talking about this with [REDACTED] (and they will ask) in our lovely Sunday call tomorrow.

[REDACTED] (9/19/2020 11:38:18 PDT):
 >feels like all of a sudden last night, people started jumping off the deep end

[REDACTED] (9/19/2020 11:38:21 PDT):
 >[REDACTED] and I will be on that.

[REDACTED] (9/19/2020 11:38:39 PDT):
 >[REDACTED] got freaked out that we aren't ready

[REDACTED] (9/19/2020 11:38:40 PDT):
 >yes totally get it

[REDACTED] (9/19/2020 11:38:43 PDT):
 >this goes beyond the IS

[REDACTED] (9/19/2020 11:38:46 PDT):
 >and so there is a lot of spinning happening right now.

[REDACTED] (9/19/2020 11:38:51 PDT):
 >this goes into much more coordinated territory

[REDACTED] (9/19/2020 11:38:53 PDT):
 >Mainly want to make sure we don't get caught in the gears :).

[REDACTED] (9/19/2020 11:39:13 PDT):

> [REDACTED] is *most* focused on hack/leak, where he thinks affirmatively we aren't ready.

[REDACTED] (9/19/2020 11:40:57 PDT):

>Would a reasonable answer when asked tomorrow be: "policy is actively working this, and we anticipate having a proposal for discussion by early this week" ?

[REDACTED] (9/19/2020 11:41:29 PDT):

>And also highlight that a *big* part of the challenge here is ops, not policy -- that staying ahead of something like this (even if we have policy authority) is massively costly and we need to be prepared for that.

[REDACTED] (9/19/2020 11:43:36 PDT):

>I like this.

>

>

>Here's my [REDACTED] suggestion:

>

>Materials from a leak or hack will be widely covered by the media. Could we assume everything is based on a hack or illegal sharing (maybe a slight expansion of [REDACTED] idea), which would result in removal, but we would allow media to report on the substance?

>

>

>I sure there are downsides to that idea as people wouldn't have access to the source material on Facebook, but I assume it will be available on other platforms.

[REDACTED] (9/19/2020 11:44:30 PDT):

>https://youtu.be/k0omu7x_LbU

[REDACTED] (9/19/2020 11:45:11 PDT):

>My pushback only is that may be broader than we need, and I could imagine it could be seen as sweeping in a lot of future leaks. If we retain a "part of a foreign influence campaign" constraint, it feels more narrowly tailored to the space -- and it's an area where we have enough credibility to have some room to maneuver.

[REDACTED] (9/19/2020 11:47:11 PDT):

>I'll pull out one piece of what you suggested, though [REDACTED] -- which is remove the content but allow media to report on substance. We obviously aren't going to take down a NYT story about this. One thing we *could* do, though, which I've discussed at length and even had proposed by some journalists in Chatham House settings, would be to *label* stories that cover the operation with one of our NITs that says something like "this story is reporting on information believed to be leaked as part of a foreign influence operation," and link to a credible assessment from an independent researcher.

[REDACTED] (9/19/2020 11:48:02 PDT):

>I actually think this is one of the few things we could really do about a coordinated leak campaign (since most of the amplification will be from NYT/WAPO/etc), and would be a big service. But the implications are not small. Several people on this thread have heard me propose this before, and I'd love to explore this.

[REDACTED] (9/19/2020 11:49:01 PDT):

>Oh it's meant to be broad and not necessarily something that I'd advocate as a permanent policy. In laymen's terms, it's the "I'm not dealing with your bullshit" option for US2020.

[REDACTED] (9/19/2020 11:49:36 PDT):

>I like the labeling idea.

[REDACTED] (9/19/2020 11:51:58 PDT):

>would the media outlets buy into the labeling idea? Could we build an opt in label for the publishers (that would be best, but no true incentive perhaps)?

[REDACTED] (9/19/2020 11:52:00 PDT):

>that's fair. I think just having a policy that says "foreign interference" somewhere might actually help us communicate a strong stance to the public, which is something we could use.

[REDACTED] (9/19/2020 11:54:29 PDT):

>This idea has come up on chatham-house calls w/reporters from the major outlets, and (surprisingly) the sentiment was "yes yes please do this!"

[REDACTED] (9/19/2020 11:54:56 PDT):

>I would avoid an opt-in, though, b/c then we'd end up with the label on the responsible players who probably provide that context in their stories anyway, but *not* the irresponsible players that don't.

[REDACTED] (9/19/2020 11:55:27 PDT):

>(I realize not having an opt-in makes it riskier, but it would substantially limit the actual value)

[REDACTED] (9/19/2020 11:57:47 PDT):

>One last timing note: it's impossible to predict whether or exactly when a hack/leak like this could happen, but there is some consensus in the security world that a reasonable time to target would be the first debate, which is sept 29th. So our time horizon to clarify ahead of that timeline is pretty short.

[REDACTED] (9/19/2020 12:01:54 PDT):
>Catching up.

[REDACTED] (9/19/2020 12:02:43 PDT):
>yup

[REDACTED] (9/19/2020 12:02:47 PDT):
>something will drop before the debate

[REDACTED] (9/19/2020 12:02:58 PDT):
>though i think we should all remember the rumor mill is running wild on all sides

[REDACTED] (9/19/2020 12:03:10 PDT):
>te latest today is that he will announce we are pulling out of the UN in the next week

[REDACTED] (9/19/2020 12:03:15 PDT):
>to ride into the debates...

[REDACTED] (9/19/2020 12:03:16 PDT):
>I like the idea that we default to allow unless there is evidence of (1) illegality in accessing the materials or (2) foreign intelligence. Defaulting to remove, I think, would be way too restrictive. E.g., yesterday's HHS emails: <https://www.nytimes.com/2020/09/18/us/politics/trump-cdc-coronavirus.html?searchResultPosition=1>

[REDACTED] (9/19/2020 12:04:29 PDT):
>(And I get we'd allow the article as news reporting under any policy, but if these emails first appeared on FB with a caption that just says "my friend just forwarded this to me. whoa! gov'm't at its worst!", I don't think we'd want to remove them.)

[REDACTED] (9/19/2020 12:05:20 PDT):
>NYT alert just popped that USSS intercepted ricin that was mailed to WH.

[REDACTED] (9/19/2020 12:09:34 PDT):
>2020's getting ready for the fourth quarter press!

[REDACTED] (9/19/2020 12:27:17 PDT):
>Agree. Fwiw, our assessments on timing and likelihood are based on both (a) our internal assessments -- we see circumstantial evidence of the operation already in execution; (b) credible warnings we're getting from IC partners; and (c) general consensus among experts.

[REDACTED] (9/19/2020 12:27:44 PDT):
>i prefer to be in denial.

[REDACTED] (9/19/2020 12:27:54 PDT):
>I agree with this framework. It would be really interesting to think about labels we can deploy when we keep up.

[REDACTED] (9/19/2020 12:27:55 PDT):
>stop being such a downer [REDACTED]

[REDACTED] (9/19/2020 12:28:00 PDT):
>truth hurts!

[REDACTED] (9/19/2020 12:29:13 PDT):
>Also, I should note that as [REDACTED] are tracking, we're anticipating we will make a significant off-cycle CIB announcement late this coming week (likely Thursday) designed to inoculate the public and press against the risk of a hack/leak op from a foreign op, and anchor a warning that this could be coming. <-- please obv keep this to this group.

[REDACTED] (9/19/2020 12:29:51 PDT):
>Assuming that lands, which I would put at 95% likelihood at this point, if we had a shift or statement about our policy to make on hack/leak, it would make a lot of sense to say it at the same time.

[REDACTED] (9/19/2020 12:30:19 PDT):
>(recognizing that is a very compressed time window, but if we take the risk of the debates as a credible one, we don't have much more time than that in any event)

Exhibit 82

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=92BCA91BE2DF4977A7D82AFF68A516A5>
To: [REDACTED]
Sent: 9/18/2020 2:36:03 PM
Subject: Message summary [{"otherUserFbld": "[REDACTED]", "threadFbld": null}]

[REDACTED] (9/18/2020 11:06:24 PDT):

>fyi -- team is readying an off-cycle CIB enforcement for late next week

[REDACTED] (9/18/2020 11:06:28 PDT):

>on the hack/leak

[REDACTED] (9/18/2020 11:06:43 PDT):

>Both to get some assets clear that could pivot, and to give us a vehicle to signal the hack/leak risk.

[REDACTED] (9/18/2020 11:06:52 PDT):

>It's in good shape and should be escalated on Monday

[REDACTED] (9/18/2020 11:08:13 PDT):

>Has anything been made public about it? Or is this stuff we're getting from USG

[REDACTED] (9/18/2020 11:08:30 PDT):

>A combination of stuff we've gotten from USG and our own cross-work.

[REDACTED] (9/18/2020 11:08:50 PDT):

>nothing that has been heavily active at this point, but things that we assess could pivot to support a hack/leak operation.

[REDACTED] (9/18/2020 11:10:24 PDT):

>Got it

[REDACTED] (9/18/2020 11:11:24 PDT):

>Timing matters b/c our assessment and external assessment is that if RU were to do a leak, Sept 29th (first debate) would be a reasonable time for them to drop. And our ability to have any impact drops *radically* once the drop has happened. If we get out first, we can inoculate a bit, and position the company as a leading voice here.

[REDACTED] (9/18/2020 11:18:03 PDT):

>1/ Do we need leadership update? Including MZSS given this.

>2/ Any more help needed ahead of takedown? Or seems under control?

[REDACTED] (9/18/2020 11:18:14 PDT):

>(#2 from an internal XFN coordination perspective)

[REDACTED] (9/18/2020 11:18:37 PDT):

>(1) Yes. Sets are getting finalized. leadership update is aimed for Monday; planning enforcement on Thursday

[REDACTED] (9/18/2020 11:20:42 PDT):

>(2) IO XFN is supportive and pushing hard. Two worries: (1) we continue to have DS problems -- we keep getting bumped around to different DS' and discovering gaps in our data, and worried that could make us miss our timeline; (2) since we're moving fast here, just want to make sure we don't lag at leadership review and approval, so would love your help making sure we can get to quick review if needed.

[REDACTED] (9/18/2020 11:21:33 PDT):

>Cool. I flagged to [REDACTED] and lmk if on Monday after you send the leadership update we need anything to move it along.

[REDACTED] (9/18/2020 11:21:40 PDT):

>Sounds good -- thank you.

[REDACTED] (9/18/2020 11:21:43 PDT):

>I've talked it through with [REDACTED].

[REDACTED] (9/19/2020 11:22:07 PDT):
>Perrfect

[REDACTED] (9/19/2020 11:22:39 PDT):
>yep. she is aware and supportive.

[REDACTED] (9/18/2020 11:27:42 PDT):
>purchased accounts is another good example of a fast-twitch threat.

[REDACTED] (9/18/2020 11:48:54 PDT):
>Do you know what precipitated this meeting?

[REDACTED] (9/19/2020 11:49:09 PDT):
>I'm curious about timing - should we have discussed this process months (or weeks) ago

[REDACTED] (9/19/2020 11:49:31 PDT):
>Which meeting? the hack/leak discussion?

[REDACTED] (9/18/2020 11:49:39 PDT):
>This one now

[REDACTED] (9/18/2020 11:49:53 PDT):
>I honestly don't know what precipitated this meeting -- I was told you had asked for it :).

[REDACTED] (9/19/2020 11:50:07 PDT):
>On hack leak, for example, the teams have been working that for some time.

[REDACTED] (9/19/2020 11:50:26 PDT):
>[REDACTED]'s team have been coordinating work directly on hack/leak and our preparation for a couple months.

[REDACTED] (9/18/2020 11:50:36 PDT):
>OK

[REDACTED] (9/19/2020 11:51:01 PDT):
>The only thing that has changed *recently* for me is that (a) we got signal from USG that reinforced our own assessment; and (b) we got these potential networks we could enforce against and use as a pre-leak moment.

[REDACTED] (9/18/2020 11:51:55 PDT):
>unfortunately, our ability to be effective against a hack/leak once it drops is *extremely* limited

[REDACTED] (9/18/2020 13:30:10 PDT):
>How are you feeling coming out of that prep meeting? We're jamming to make sure we're ready for the enforcement.

[REDACTED] (9/19/2020 14:06:59 PDT):
>1/ Worried about late scenario planning - debugging separately.
>2/ Disruption stuff - glad we're putting heads together, seems you guys are on it. Was just brainstorming with [REDACTED] and I agree with your approach to using our disruption to try to "inoculate". I wonder if we should consider prepping Stamos... mainstream media amplifying leaks is totally his thing. After we disrupt and publish, he needs to do a broadcast tour talking about mainstream media not amplifying RU leaked content.

[REDACTED] (9/18/2020 14:33:22 PDT):
>(2) Absolutely -- already planned. Tbh, Alex is good, but others are more important. As we develop comms this weekend, we are going to do a much more proactive comms prep with key partners so this message gets echoed in all the right places. We'll have the key expert voices, who would avoid hyperbolization, ready to go out with us to send the message.

[REDACTED] (9/19/2020 14:33:45 PDT):
>That's great

[REDACTED] (9/18/2020 14:33:46 PDT):
>Assuming we land it right, whether the Russians act or not, it should have the pleasant

[REDACTED] (9/19/2020 14:35:14 PDT):

>On (1), fwiw, I know [REDACTED] has pulled a lot of work on this. Part of the problem is that for some of the scenarios (eg, Hack Leak), our options are limited -- not b/c we haven't looked, but b/c we aren't the primary target and most of the manifestation on our platforms will be news stories that we can't act on easily. Also, we have the tabletop scenario runs planned for mon/tue, which will be the most effective way to identify any gaps.

[REDACTED] (9/19/2020 14:36:03 PDT):

>That said, doing a double-check can't hurt (especially given how critical all this is). But I suspect we will always be able to find spaces where we aren't as prepared as we like as we head into this one...

Exhibit 83

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=MDVILY237>
To: [REDACTED]
Sent: 9/21/2020 7:45:07 AM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}

[REDACTED] (9/21/2020 06:20:56 PDT):
>following up on the draft about Burisma evidentiary assessments

[REDACTED] (9/21/2020 06:21:24 PDT):
>Thank you both for pulling this together -- looking solid. I took a crack at the overview to make sure it explains what we're thinking to leadership.

[REDACTED] (9/21/2020 06:22:33 PDT):
>on the Burisma section: it describes low/med/high confidence scenarios around Burisma. Two specific questions:

[REDACTED] (9/21/2020 06:23:25 PDT):
>(1) can you describe our *current* assessment of the evidence we have? It seems like we're somewhere between low and medium right now?

[REDACTED] (9/21/2020 06:24:17 PDT):
>(2) At which of these thresholds would we recommend to leadership that we should treat such evidence as sufficient proof of an influence operation that we should act on it (e.g., removing source files, label reporting)? Medium? High?

[REDACTED] (9/21/2020 06:26:09 PDT):
>The current assessment is the first one. It is low. Because that low confidence scenario is essentially ALL we have, as discussed in the phone call yesterday

[REDACTED] (9/21/2020 06:27:10 PDT):
>We have reporting that is not credible from Area 1, disputed by crowd strike and fireye. And no other evidence. If a leak were to come out now with no further indicators and information, we would be at LOW confidence

[REDACTED] (9/21/2020 06:27:57 PDT):
>We have reporting of concern from our USG partners -- not as to timing or specifics, but shouldn't we be considering that?

[REDACTED] (9/21/2020 06:28:26 PDT):
>My sense from our conversations has been that while they certainly don't have specifics, the tone and context we've heard from them is more than pure speculation.

[REDACTED] (9/21/2020 06:28:46 PDT):
>That doesn't mean it's not still low, of course, but I didn't see that incorporated in the description of what we know...

[REDACTED] (9/21/2020 06:28:50 PDT):
>Mere "Concern" isn't enough to act on a specific piece of content if we cannot tie it back to anything or have any further indicators

[REDACTED] (9/21/2020 06:29:24 PDT):
>We are asking about evidentiary scenarios that allow us to take action on specific content items that go beyond evidence of a hack but are considered merely leaked

[REDACTED] (9/21/2020 06:30:02 PDT):
>Right now if there was a leak and NO further info, it would be a low confidence scenario unless we could actually evaluate who is disseminating that content, etc

[REDACTED] (9/21/2020 06:30:16 PDT):
>I'm not arguing that we should be above low likelihood here

[REDACTED] (9/21/2020 06:32:31 PDT):
>but I don't think the low assessment reflects that we've heard specific warnings *from USG partners* in two dimensions: (1) high-risk assessment that this will happen (we'll often be

operating in this zone of uncertainty, and the fact that they are concerned enough to tell us this is a signal); and (2) when they gave us the tip that helped w/some of the investigation into the assets we'd action this week, didn't they explicitly note that they are concerned these assets could pivot to support a leak?

[REDACTED] (9/21/2020 06:33:29 PDT):

>Both of those are indications of the seriousness w/which they are taking this, which may be important in the absence of clearer context. Again, I don't disagree that our assessment is low here -- I think that's right.

[REDACTED] (9/21/2020 06:33:41 PDT):

>But I'd think we'd want to call out that evidence to leadership as part of our assessment.

[REDACTED] (9/21/2020 06:34:40 PDT):

>Can also chat this through by voice/video if that's easier!

[REDACTED] (9/21/2020 06:35:48 PDT):

>For #2 we have our own investigations and indications that allow us to feel comfortable to take action under CIB policy this week. And specific tips helped us but didn't entirely shape our investigative works. Their "concern" helps us think about taking prophylactic action under something that ALREADY violates our policies on its own. What we are asking about here is an evidentiary standard for something that doesn't (a mere leaked piece of content)

[REDACTED] (9/21/2020 06:36:33 PDT):

>My point here is that if we provided the "low" assessment to leadership today, the first thing they would ask is "have you heard from our USG partners?"

[REDACTED] (9/21/2020 06:37:01 PDT):

>And we'd then have to explain "yes, we've heard from them, and they've given us *some* indication this could happen, and have shared some tips, but they haven't given us any specific evidence of time/place/risk."

[REDACTED] (9/21/2020 06:38:42 PDT):

>sorry catching up, in another meeting

[REDACTED] (9/21/2020 06:39:07 PDT):

>I agree with the assessment that our confidence is low, and I'm incorporating the USG signal into that assessment

[REDACTED] (9/21/2020 06:39:09 PDT):

>I would argue that the current things we have heard which are unspecific in nature and the low confidence assessment about burisma, without further evidence, would not allow us to act in content that decidedly does not violate our policies. UNLESS we can answer the questions [REDACTED] laid out. And with that, passing to [REDACTED]

[REDACTED] (9/21/2020 06:39:27 PDT):

>what's the specific question for me?

[REDACTED] (9/21/2020 06:39:54 PDT):

>I don't disagree. I think the assessment is correct -- but it seemed incomplete b/c it didn't highlight the USG inbound we've gotten.

[REDACTED] (9/21/2020 06:40:11 PDT):

>i.e. if we see a Burisma leak, can we assume with low confidence that it's possible RU is behind it?

[REDACTED] (9/21/2020 06:40:13 PDT):

>So adding it in makes sense to me!

[REDACTED] (9/21/2020 06:40:34 PDT):

>I think that's fair, with the appropriate caveat about the lack of concreteness or actionable signal

[REDACTED] (9/21/2020 06:42:20 PDT):

>The other point that I asked about is leadership will be looking to us for a recommendation on whether our evidence is clear enough that we should take action on specific content. Our answer now is obviously no. I assume in our high confidence scenario,

[REDACTED] (9/21/2020 06:42:32 PDT):

>I have added "from vendors and USG" under the low confidence scenario after the word speculation

[REDACTED] (9/21/2020 06:43:03 PDT):

>What's your take on where we would be in a medium confidence scenario? Is there a scenario where, absent on-platform technical indications, we would feel strong enough to recommend action?

[REDACTED] (9/21/2020 06:43:19 PDT):

>what would be the action? removing content?

[REDACTED] (9/21/2020 06:43:27 PDT):

>yep.

[REDACTED] (9/21/2020 06:43:34 PDT):

>yes, I think that's right

[REDACTED] (9/21/2020 06:43:47 PDT):

>if we have high confidence the leak is sponsored by RU, we would advocate for removal

[REDACTED] (9/21/2020 06:45:19 PDT):

>The key question leadership will ask is whether there is a scenario where we have less than technical certainty where we would still advocate for removal.

[REDACTED] (9/21/2020 06:45:29 PDT):

>[REDACTED] and I discussed yesterday that we've previously been able to act in a sort of medium confidence scenario as well, as in the 2019 midterms "resisters" tip which was not corroborated at first

[REDACTED] (9/21/2020 06:46:06 PDT):

>I actually think that medium conf is best we can hope for or at least should plan for

[REDACTED] (9/21/2020 06:46:13 PDT):

>I agree with that

[REDACTED] (9/21/2020 06:46:17 PDT):

>and yes, I would advocate that medium conf is enough to act

[REDACTED] (9/21/2020 06:46:29 PDT):

>Ah -- got it. That is good to understand.

[REDACTED] (9/21/2020 06:46:38 PDT):

>We should be clear to leadership where we would anticipate acting.

[REDACTED] (9/21/2020 06:52:06 PDT):

>OK, so path forward is 1. low conf (current state) = no action, 2. medium conf (as outlined in the doc) = we would recommend action, correct?

[REDACTED] (9/21/2020 06:55:05 PDT):

>That's right.

[REDACTED] (9/21/2020 06:56:19 PDT):

>I'm still struggling a bit b/c I think our current description of low conf undersells what we know right now, and I don't want to undersell our current certainty b/c I want to be clear to leadership what *isn't* enough to act.

[REDACTED] (9/21/2020 06:57:05 PDT):

>undersells which part, the USG stuff?

[REDACTED] (9/21/2020 06:58:04 PDT):

>yeah. "speculation" seems to suggest to me "it could happen." While I think what we've heard from USG is "we think it's likely to happen."

[REDACTED] (9/21/2020 07:00:30 PDT):

>I really think the context from USG was "it's a likely adversarial scenario", which we

already agree with. So I think it's helpful to separate likelihood from confidence - likelihood, we all agree is high among all of the adversarial scenarios. On the confidence, which is dictated by specific data points, it's low - there is no timeline, no sourcing, no actionable intel, and no warning points other than Area 1 reporting, which is low quality.

[REDACTED] (9/21/2020 07:01:19 PDT):

>Agree on the incredibly low value from Area 1.

[REDACTED] (9/21/2020 07:01:49 PDT):

>The way you are framing distinctions between likelihood and confidence is interesting and now how I would intuitively split those words, but I understand your point.

[REDACTED] (9/21/2020 07:02:23 PDT):

>I think prudent to say we're worried about this being a likely scenario, and we share that worry with USG. Current intel about it though is low confidence since we have no concrete data points. I am also worried some of the USG context is circular and comes from Area 1

[REDACTED] (9/21/2020 07:02:31 PDT):

>but I could be wrong about it

[REDACTED] (9/21/2020 07:07:32 PDT):

>that makes sense -- leadership will definitely care about the "likelihood" assessment we're getting from gov't.

[REDACTED] (9/21/2020 07:07:40 PDT):

>[REDACTED] - do you have a sec for a quick call? I think I can give some verbal context to help frame the context from USG

[REDACTED] (9/21/2020 07:07:59 PDT):

>So I think it's useful, important to be clear to them that high likelihood / no concrete evidence signal from gov't is something we translate to low confidence assessment

[REDACTED] (9/21/2020 07:07:59 PDT):

>That makes sense to me,

[REDACTED] (9/21/2020 07:09:04 PDT):

>but that's an important point for leadership

[REDACTED] (9/21/2020 07:09:05 PDT):

>at least from the meeting I was in

[REDACTED] (9/21/2020 07:09:10 PDT):

>nod -- makes sense

[REDACTED] (9/21/2020 07:09:03 PDT):

>on a call now, but potentially could chat at 1130

[REDACTED] (9/21/2020 07:09:13 PDT):

>Right, we can go further and explain why we think they estimate that likelihood to be high

[REDACTED] (9/21/2020 07:09:43 PDT):

>which essentially is an estimation of geopolitical drivers and risk/benefit assessment to the Kremlin

[REDACTED] (9/21/2020 07:10:12 PDT):

>which has value in intelligence analysis - it's a statement about intent and capability, which is what we got from USG

[REDACTED] (9/21/2020 07:11:21 PDT):

>Essentially "we estimate Putin does not want Biden and it is in the Kremlin interest to ensure a Biden victory doesn't happen, and the best levers they might have is a Ukraine/Burisma scenario" <-- which they've said publicly

[REDACTED] (9/21/2020 07:12:22 PDT):

>I think all of that is true, and is an accurate evaluation of intent, which, when combined with evaluation of risk calculus, makes the scenario likely since we have precedent for Kremlin's actions before.

[REDACTED] (9/21/2020 07:13:38 PDT):

>but when we asked them for specifics of whether, how, or by whom Burisma may have been targeted, there was no answer. Doesn't mean it didn't happen, just that there were no details available.

[REDACTED] (9/21/2020 07:24:45 PDT):

>Also - there may be additional context I'm missing, such as from conversations [REDACTED] or others may have had, so possible there is stronger wording somewhere I'm not privy too.

[REDACTED] (9/21/2020 07:37:22 PDT):

>Adding [REDACTED] here as well since he was in these meetings

[REDACTED] (9/21/2020 07:43:35 PDT):

>This makes sense -- it's how I'd understood them to have gone, so glad I've been tracking.

[REDACTED] (9/21/2020 07:44:24 PDT):

>Essentially, I would say we are hearing increasing estimates of *likelihood* from government, and various types of circumstantial evidence that would be consistent with an operation (eg, Derkach). But we have *no* specific/concrete evidence that this is happening/will happen.

[REDACTED] (9/21/2020 07:45:07 PDT):

>Given that, it makes sense that we see basis for a prophylactic step (gets ahead of increasing likelihood), but are only at low confidence for an actual event occurring.

Exhibit 84

Message

From: [REDACTED] [REDACTED]@dnc.org
Sent: 8/5/2020 9:57:56 PM
To: [REDACTED] [REDACTED]@google.com
CC: [REDACTED] [REDACTED]@google.com]; [REDACTED] [REDACTED]@dnc.org]; [REDACTED] [REDACTED]@dnc.org]; [REDACTED] [REDACTED]@dnc.org]; [REDACTED] [REDACTED]@google.com]; [REDACTED] [REDACTED]@google.com]; [REDACTED] [REDACTED]@google.com]; [REDACTED] [REDACTED]@google.com]
Subject: Re: High-Reach YT Takeover Account examples

Thanks [REDACTED]. You and your team's work to reduce the risk and impact of hack-and-dump operations is much appreciated.

On Wed, Aug 5, 2020 at 5:27 PM [REDACTED] <[REDACTED]@google.com> wrote:

Good afternoon All,

Many thanks again [REDACTED], [REDACTED], [REDACTED], [REDACTED] and [REDACTED], as well as the others who joined the meeting yesterday. I hope you found it insightful and informative as we enter the last few months before the election.

Thank you [REDACTED] for flagging the accounts below. We will review, and my colleague [REDACTED] and I will follow-up.

I wanted to flag for you two items we identified on the call.

1. **Enhanced Protection.** In addition to our APP programs, earlier this year, we announced an effort to further protect Google Accounts that are at a high risk of attacks during the U.S. election season. We are asking stakeholders to submit your Google Account email addresses for enhanced protection, including personal email accounts. Find form here: <https://services.google.com/fb/forms/enhanced-security/>

2. **Hacked Materials.** In September 2020, we announced a hacked political materials policy. This policy is specifically related to the distribution of hacked political material. <https://support.google.com/adspolicy/answer/9991623>

As always please let me know if you have any questions or concerns. And don't hesitate to reach out for any necessary follow-up.

All the best,
[REDACTED]

On Wed, Aug 5, 2020, 2:40 PM I [REDACTED] <[REDACTED]@dnc.org> wrote:

Hi [REDACTED]

Thank you for putting together yesterday's meeting with Google's Threat Analysis group. Here are some of the examples of channel takeovers that received significant reach after switching over to US political content. While we understand these takeovers are the work of unsophisticated, commercially-motivated spam groups, their effect on American voters may not be significantly different than an operation undertaken by a more sophisticated actor. As we mentioned on the call, we're concerned both with the **frequency** with which these takeovers are occurring, the **speed** at which they are remediated, and the **reach** (via YT's "Up Next" algorithm) they achieve despite having little or no PageRank authority for news content.

highfiverock (top video saw 72k views in 1 day):
<https://www.youtube.com/user/highfiverock/videos>



TRUMP BREAKING NEWS (top video saw 97k views in 2 days):
<https://www.youtube.com/c/mandoprod/videos>



House Republican (81k-806k views per video):
<https://www.youtube.com/user/iandipra/videos>



Thank you again for your consideration.



Confidential - Not For Public Release

Exhibit 85

From: [REDACTED] <[REDACTED]@dni.gov>
To: [REDACTED]
Sent: 9/24/2020 3:06:48 PM
Subject: Re: CIB Takedown (Sept 2020)

Great stuff [REDACTED]!

From: "[REDACTED]" <[REDACTED]f@fb.com>
Date: Thursday, September 24, 2020 at 4:16:35 PM
To: "[REDACTED]" <[REDACTED]@dni.gov>
Cc: "[REDACTED]" <[REDACTED]@dni.gov>, [REDACTED] <[REDACTED]@dni.gov>
Subject: CIB Takedown (Sept 2020)

Good afternoon, [REDACTED]!

I hope this finds you well!

As part of monthly CIB reports, I wanted to share that today we announced the removal of three separate networks for violating our policy against foreign or government interference which is coordinated inauthentic behavior (CIB) on behalf of a foreign or government entity. These networks originated in Russia and were linked by our expert investigative teams to several different Russian actors: (1) Russian military including military intelligence services, (2) individuals associated with past activity by the Russian Internet Research Agency (IRA); and (3) individuals in Russia, including those associated with Russian intelligence services.

In each case, the people behind this activity coordinated with one another and used fake accounts as a central part of their operations to mislead people about who they are and what they are doing, and that was the basis for our action. When we investigate and remove these operations, we focus on behavior rather than content, no matter who's behind them, what they post, or whether they're foreign or domestic.

Over the past three years, we've shared our findings about these networks of coordinated inauthentic behavior we detected and removed from our platforms. Earlier this year, we started publishing monthly CIB reports where we share information about the networks we take down to make it easier for people to see progress we're making in one place. In some cases, like today, we also share our findings soon after our enforcement. Today's takedowns will also be included in our September report. You can find more information about our previous CIB enforcement actions here.

The networks we're announcing today targeted many countries around the world and had very limited following globally at the time of disruption. Much of this activity focused on two things: 1) creating fictitious or seemingly independent media entities and personas to engage unwitting individuals to amplify their content and 2) driving people to other websites that these operations control. Similarly to the Russia-based network we removed in August, these operations worked across many internet services and attempted to hire contributors and seed their stories with news organizations.

We've seen deceptive campaigns target journalists and public figures in the past, including as part of hack-and-leak operations. Hack-and-leak — where a bad actor steals sensitive information, sometimes manipulates it, and then strategically releases it to influence public debate — is one of the threats we're particularly focused on and concerned about ahead of the November elections in the US. While we have not seen the networks we removed today engage in these efforts, or directly target

the US 2020 election, they are linked to actors associated with election interference in the US in the past, including those involved in “DC leaks” in 2016. We anticipate that operations like these may attempt to pivot at any time and we will keep vigilant to find and remove them. We will also continue to share our findings publicly to provide context for the adversarial trends we see.

These threats are a whole-of-society challenge, and we’re working with partners across industry to tackle them. We have shared information about our findings with law enforcement, policymakers and industry partners. We are making progress rooting out this abuse, but as we’ve said before, it’s an ongoing effort. We’re committed to continually improving to stay ahead.

Our full blog post will go live here at 3 pm ET: <https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/>

The independent external assessment from Graphika on the first network will be live at this link at 3 pm ET: graphika.com/GRUminions

The independent external assessment from The Atlantic Council’s DFRLab on the second network will be live at this link at 3 pm ET: <https://medium.com/dfrlab/disinformation-campaign-removed-by-facebook-linked-to-russias-internet-research-agency-3cbd88d0dad>

The independent external assessment from The Atlantic Council’s DFRLab on the second network will be live at this link at 3 pm ET: <https://medium.com/dfrlab/facebook-takes-down-assets-linked-to-russian-disinformation-outlet-acab0164e3d4>

Please let me know if you have any questions.

Best,

██████

Produced to HSG

Exhibit 86



Hack and Leak Roundtable June 25, 2020 1p -230p ET Agenda

Overview

With the general election less than five months away, Aspen Digital, a program of the Aspen Institute, is convening journalists, ethicists, First Amendment attorneys, and platform executives for a frank, off-the-record conversation about standards and ethics when it comes to publication and coverage in hack and leak scenarios.

Goals

We're not expecting unanimous agreement on a single standard. Rather, we want to share points of view, workshop ideas, surface where there may be alignment, and determine whether this is an area worth pursuing further. Discussion points may include:

- How do news organizations address provenance/motivation?
- How do news organizations verify attribution/where leak is coming from?
- Do platforms label hack/leaked material? What would a labeling solution look like?
- Where are we aligned? Where do we disagree?
- Merit /feasibility of coming up with shared principles among news orgs?
- Merit /feasibility of coming up with shared principles among platforms?

AGENDA

1. Welcome and introductions – [REDACTED] Aspen Institute
2. Short history of hack and leaks – [REDACTED] Aspen Institute
3. Summary of report on *Guidelines for Responsible Reporting*, [REDACTED] and [REDACTED]
[REDACTED] Stanford
4. Case study: Podesta files, [REDACTED] Washington Post
5. Discussion

Exhibit 87

To: [REDACTED] Redacted - PII
 Cc: [REDACTED] Redacted - PII
 From: [REDACTED] Redacted - PII
 Sent: Thur 7/2/2020 12:54:58 PM (UTC)
 Subject: Hack and Leak follow up

Friends,

Thank you for joining our call last week about Hack-and-Leaks for your wonderfully candid and provocative comments and questions. It was an exhilarating conversation, and it seems clear that there is much more to discuss—and quite possible areas of collaboration.

Here is a high-level summary of the some of the issues that we heard surface:

- Balancing reporting on substance of leaks vs provenance
- Conflicting motivations, interests, and perspective among reporters on different beats
- Effectiveness of disclosures
- How to disclose when leak provenance is unclear
- Preparedness for hack-and-leak that come from within the US (versus a hostile foreign actor)
- Role of the gov't to disclose or attribute provenance
- Preparedness of hack-and-leaks targeting news organizations (emails, Slack, documents, etc.)
- Preparedness for range of likely scenarios (“We’re good at post-mortems, but not at planning”)
- Challenges of falsified documents attributed to hack-and-leak operation
- Labeling conventions and content moderation policies of platforms

The one thing around which there seems to be consensus is that the risk of a major hack-and-leak in the run up to election day is real. To that end, we’re setting up TWO times for us to gather in the coming weeks (if we don’t end up needing the second one, we will drop it, but thought it might be easier to reserve time in advance):

- July 14: 12p – 130p
- July 28: 12p – 1:30p

We will send you calendar holds for those two days and develop an agenda between now and then and hope that you can join us to continue the conversation. Please do share any feedback or suggestions with [REDACTED] and me.

Lastly, someone of you asked that we share email contact information. Please let me know if you want to be left off. Otherwise, I’ll move the addresses out of bcc next time

Cheers,

[REDACTED]

--

[REDACTED]
 Executive Director, Aspen Digital
 The Aspen Institute

[REDACTED]
 [REDACTED]



Exhibit 88

We wanted to zero in on this topic — and draw a tight box around it, this is not a conversation about self-styled whistleblowers, like Snowden or Chelsea Manning. This is intended to be a conversation about adversarial thefts and leaks.

This is OFF THE RECORD.

As ██████ said, we're almost certain to see one between now and the fall election.

I'm dual-hatted here today, both in my Aspen role and as a journalist, former magazine editor at POLITICO, and current contributor to WIRED and CNN on national security issues. As many of you know, I co-wrote a book on cybersecurity with my Aspen colleague ██████ in which we examined in depth the Sony Pictures Entertainment attack in 2014.

It was a landmark attack, as it turns out, for reasons we didn't realize at the time.

When you talk to people in cyber, almost everyone points *not* to the Sands Casino attack in early 2014 as the first destructive cyberattack in the United States, they point instead to the attack on Sony. Why do people remember Sony? Sony was as destructive as Sands, but we don't remember it because of the malware that was used to wipe the company's computer drives. Sony involved the theft of intellectual property—millions of dollars' worth of intellectual property—but we don't remember it because of the stolen intellectual property. We don't even remember Sony as an attack on free speech and American democracy, which it was, just like Iran's attacks on Sands and Russia's attack on the 2016 election also were.

We remember Sony today because of how hackers hit the softest part of the system—emails—and weaponized that information through the use of social media. Then North Korea got the mainstream media to pick up on those leaks and do the hackers' bidding for them, causing reputational and financial damage to the company by airing their innermost secrets.

Unfortunately, that part of Sony's legacy—so obvious now in hindsight—didn't sink in with the government and the private sector. We learned the wrong lesson; we focused on deterring destructive attackers and hardening our network systems. Russia, meanwhile, watched the Sony hack and learned the power of stolen information to influence public opinion and undermine confidence in an organization. And Russia saw how American society had been quick to blame and isolate the victim, Sony, rather than unite against the perpetrator.

The Sony attack, as it turned out, represented the Rubicon: coupled with the experience of media and global reaction to WikiLeaks and Edward Snowden, North Korea knew that media organizations—some reputable, some not—would rush to cover the leaks, amplifying the thefts with little self-reflection. If North Korea simply sent a stolen spreadsheet of a company's executive salaries to reporters, they'd publish it quickly. Particularly in the sped-up news cycles of the digital age, the media had decided that the "newsworthiness" of purloined internal secrets outweighed any ethical dilemmas raised by how that material was obtained.

The tactics pioneered by the attack on Sony were exactly the same tactics that the Russians later used to influence our election in 2016. We saw these tactics build on one another. As Russia considered whether to weaponize the emails they'd stolen from the Democratic National Committee, they knew from the North Korea attack on Sony that the media would lap up—and publish without delay—purloined emails.

In the years since, we've seen Macron Leaks and other operations, by Russia and other adversaries, all with a shared goal of influencing their own strategic goals at a cost to western democracy.

What all of those cases have made clear as we've seen in the years since is that Hack-and-leaks are a particularly difficult and challenging cyber threat to address precisely because they exploit the seams of democracy, as well as the seams of the news media and news organizations themselves.

I think we all in this virtual room share a sense that we should be doing something better and more thoughtful to confront hack-and-leak and allowing adversaries to weaponize our news channels against our democracy, but it's a super complex issue and there aren't easy answers here even for the most responsible actors.

Our goal here today is open this conversation mostly to see where it leads — think of it has a highly structured and curated fishing expedition — to see if we can combine the smartest people we know to help address this really really thorny problem.

Along those lines, as a starting point today, I wanted to lay out three challenges and three opportunities around hack-and-leaks and the environment we face over the months ahead and then hand it over to [REDACTED], [REDACTED] and [REDACTED] to talk specifically about more various aspects of this.

The first challenge is simply that hack-and-leak operations, no matter the source, are hard to ignore. The documents often contain legitimate news and insights into key decisions or relationships, although we've certainly seen reporting that can stray from the newsworthy to the salacious, in places like Sony, or the silly, as all of us now can debate John Podesta's risotto recipe.

The second challenge is that even if you wish to ignore it, it's hard. Part of the opportunity that adversaries have seized with these operations is how the diversification and disintermediation of online media allows information to reach ever-wider audiences quickly and how sites like Wikileaks, RT, Sputnik, and less reliable fringe or partisan websites can publish material that forces more mainstream and reliable organizations to confront stories they'd normally argue don't rise to their standards. As we've seen from QAnon's Pizzagate to the President's own Twitter feed to the rumored-and-never-spotted giant Antifa bus during the protests in recent weeks, news organizations often now have to wrestle with the fringe-y, conspiratorial ideas in a way that they didn't have to before.

The third challenge is attribution — it's often impossible to fully understand the context and attribution of these leaks in real-time, forcing intelligence agencies and news organizations to speculate about the provenance of the documents (and thus the motives and desired outcomes of the attack) without necessarily being able to state plainly and publicly the goals of the perpetrators.

* * *

Three opportunities for a more mature response in this election and beyond.

First is that we've seen in both the Macron Leaks and the DNC/Podesta Leaks is that there are often warnings ahead of time. The DNC announced it had been attacked before the first documents began to circulate, and we've seen in the Mueller Report how Roger Stone and others appeared to have a strong understanding of the damaging information to come on Podesta and Hillary Clinton's campaign as the fall election unfolded, similarly in France and almost three months before the "Macron Leaks" appeared online, online researchers were warning of such an operation underway.

Moreover, many of these leaks don't happen in a vacuum; they're an additional pillar of a broader operation — as we now understand unfolded with the Internet Research Agency in 2016 and as part of a broader disinfo and misinfo campaign against Macron in 2017.

Given those warnings, how should news organizations and platforms begin mobilizing and thinking about these attacks and the resulting coverage when we suspect there's something coming?

Second opportunity is that these operations are less of a surprise; no one's first instinct in 2014 was North Korea, and in 2016 it took too long for us to realize our election was under attack from Russia. Part of what the Macron Leaks falter is that people were better able to recognize in real-time what was happening. So how do we do a better job—or even should we do a better job of saying reader beware?

The third opportunity is conversations like this — there's a level of willingness across platforms, news organizations, and threat researchers to share information and — perhaps not collaborate — but at least converse together around these topics in 2020 that never would have existed in 2014 or 2016. Today, of course, we have reporters, researchers, and researchers better primed to be wary and suspicious, to understand that we might be being played by an adversary with a specific agenda and purpose.

I'm really excited for this conversation and to see where this leads.

Exhibit 89

To: [Redacted - PII]
 Cc: [Redacted - PII]; [Redacted - PII]
 From: [Redacted - PII]
 Sent: Tue 7/14/2020 11:55:32 AM (UTC)
 Subject: Re: TOMORROW: Aspen H/L part deux

No worries. [Redacted]. We might have 3rd one you can join in a couple of weeks. – will keep you posted. Enjoy your holiday. Stop working! 😊

From: [Redacted] <[Redacted - PII]>
 Date: Tuesday, July 14, 2020 at 3:12 AM
 To: [Redacted] r <[Redacted - PII]>
 Cc: [Redacted] <[Redacted - PII]>, [Redacted] <[Redacted - PII]>
 Subject: Re: TOMORROW: Aspen H/L part deux

I am behind on so many work things while trying to be on holiday, [Redacted], so I won't be able to make it today - even though I know it will be fascinating. Hope it all goes well.... [Redacted]

On Mon, 13 Jul 2020 at 20:53, [Redacted] <[Redacted - PII]> wrote:
 Friends,

Looking forward to seeing you all tomorrow to continue the great conversation we had the other day about Hack/Leaks. The plan tomorrow is primarily focus this session on context, and on attribution – the so called ‘third paragraph’ question. For news organizations that means answering questions like:

- How should news organizations respond initially to events that are likely hack-and-leaks, e.g., a Wikileaks or DC Leaks dump, but whose provenance/attribution is unclear?
- What's the context that should be placed by news organizations around suspected hack-and-leaks?
- How should that context change if/when there's a suspected-but-not-confirmed provenance?
- How should that context change if/when there's a "confirmed" provenance from government intelligence

For UGC platforms, there is an additional question about labeling suspected hack-and-leaks.

We asked a few of you to speak very briefly about how you approach these questions. But this session will be much more about conversation. Reminder that we have one more meeting on July 28th. More on that tomorrow.

[Redacted]

--

[Redacted]
 Executive Director, Aspen Digital
 The Aspen Institute
 [Redacted - PII]
 @ [Redacted]



Exhibit 90



Exhibit 91

From: [REDACTED]@aspeninstitute.org>
To: [REDACTED]
CC: [REDACTED]
Sent: 5/19/2020 3:18:50 PM
Subject: Re: Connecting the two of you to talk about hacks and leaks!

Terrific! Thanks [REDACTED] (and Hi [REDACTED]). It's going to be a really good group. We'll send out a doodle next for mid-June. More soon! [REDACTED]

[REDACTED]

From: [REDACTED]@google.com>
Date: Tuesday, May 19, 2020 at 5:48 PM
To: [REDACTED]@aspeninstitute.org>
Cc: [REDACTED]@fb.com>, [REDACTED]@google.com>
Subject: Re: Connecting the two of you to talk about hacks and leaks!

[REDACTED]

Hi [REDACTED]

I hope that you had a nice weekend!

Pursuant to our conversation last week, I confirm that I'll be happy to attend the off-the-record gathering you told me about and look forward to hearing more from you about date/time/preparation, etc. Thank you for having me, it should be an interesting day!

I'm also adding in cc to this message my colleague [REDACTED] who oversees our broader work with Aspen, for her awareness.

Best,

[REDACTED]

On Wed, May 6, 2020 at 8:54 AM [REDACTED]@aspeninstitute.org> wrote:
Thanks [REDACTED] And Hi [REDACTED] I'd love to chat with you about this. You have time later this week or early next? [REDACTED]

From: [REDACTED]@fb.com>
Date: Wednesday, May 6, 2020 at 2:08 AM
To: [REDACTED]@aspeninstitute.org>, [REDACTED]@google.com", [REDACTED]@google.com>
Cc: [REDACTED]@fb.com>
Subject: Connecting the two of you to talk about hacks and leaks!

[REDACTED]

As I've mentioned to both of you, I wanted to connect you up! [REDACTED] is thinking through how to host a closed door conversation about dealing with hack/leak operations with attendees from both traditional media and the major platforms. [REDACTED] and I are planning to attend for Facebook, and I'm really hopeful that the effort could make progress on this hard problem. From our conversation [REDACTED] it sounded

like you'd be the right contact at Google!

Final Report 1425

I hope the two of you can connect, and that you can join the (virtual) conversation, [REDACTED]

[REDACTED]

--

Google

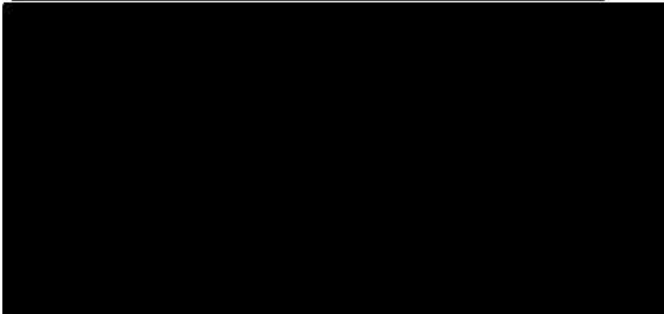


Produced to HJC

Exhibit 92

From: [REDACTED]@stanford.edu>
To: [REDACTED]
CC: [REDACTED]
Sent: 6/25/2020 9:52:46 AM
Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

Thanks guys - I have the key snippets from the report ready to share-screen (to coin a verb for our milieu).



From: [REDACTED]@aspeninstitute.org>
Sent: Thursday, June 25, 2020 7:08 AM
To: [REDACTED]@gmail.com>
Cc: [REDACTED]@aspeninstitute.org>; [REDACTED]@stanford.edu>; [REDACTED]@fb.com>; [REDACTED]@fb.com>
Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

yes

From: [REDACTED]@gmail.com>
Date: Thursday, June 25, 2020 at 10:03 AM
To: [REDACTED]@aspeninstitute.org>
Cc: [REDACTED]@aspeninstitute.org>, [REDACTED]@stanford.edu>, [REDACTED]@fb.com>, [REDACTED]@fb.com>
Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

So we will have screen sharing capabilities?

On Thu, Jun 25, 2020, 5:47 AM [REDACTED]@aspeninstitute.org> wrote:
Thanks both. Ten minutes please. I DO think it's helpful to put them up on the screen actually. Easier to follow along. We can put link to full report in chat as well. That work? And THANK YOU!!!!

From: [REDACTED]@gmail.com>
Date: Wednesday, June 24, 2020 at 1:32 PM
To: [REDACTED]@aspeninstitute.org>
Cc: [REDACTED]@aspeninstitute.org>, [REDACTED]@stanford.edu>, [REDACTED]@fb.com>, [REDACTED]@fb.com>
Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

Hi [REDACTED] and I spoke. He will go first and then I will go. Can you remind how long we have total?

Also, I thought maybe useful to put up our 10 suggested guidelines as I highlight some of them. [REDACTED] thought better to put a link in the chat that people can call up if they wish. I'm really fine either way.

On Wed, Jun 24, 2020 at 7:24 AM [REDACTED]@aspeninstitute.org> wrote:
Hi [REDACTED] and [REDACTED]

Just checking in on tomorrow. You all set? And will you have slides?

Thanks!

From: [REDACTED]@aspeninstitute.org>
Date: Tuesday, June 16, 2020 at 5:16 PM
To: [REDACTED]@gmail.com>, [REDACTED]@stanford.edu>
Cc: [REDACTED]@aspeninstitute.org>, [REDACTED]@fb.com>, [REDACTED]@fb.com>
Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

The goal going in is simply to define the problem and ethical challenges and examine where there might be interest or appetite for further conversation. This is basically a semi-structured and organized roundtable fishing exercise. We're very much not sure that there *is* a specific outcome or objective, because it might very well prove that there are too many different considerations and institutional constraints for there to be any concerted action.

We really just want to get a bunch of smart people together who care about this issue and have different perspectives, lay out the issue through a mix of presentations, case studies, and debate, define the problem, and see what follow-up action or activities or conversations might make sense. It's possible that something like what [REDACTED] is suggesting makes sense as a follow-on, but we don't want to drive toward a premature conclusion or goal before we've surfaced all the questions and concerns from various perspectives.

Our hope is that any definitive takeaways would actually come during a second follow-up conversation....

From: [REDACTED]@gmail.com>
Sent: Tuesday, June 16, 2020 4:26 PM
To: [REDACTED]@stanford.edu>
Cc: [REDACTED]@aspeninstitute.org>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@aspeninstitute.org>
Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

Sounds okay. I'm just not clear on what the objective is of this gathering or how to structure so you have a definitive takeaway. Maybe a consensus on what [REDACTED] was after re labeling or somesuch. Unsure we can get any meaningful commitments from this particular group re editorial decisions in newsrooms when the hack happens.

On Tue, Jun 16, 2020 at 10:10 AM [REDACTED]@stanford.edu> wrote:



I think that sounds about right - high level summary from us, punctuated with references to these objections.

[REDACTED] what do you think?

From: [REDACTED]@aspeninstitute.org>

Sent: Tuesday, June 16, 2020 8:48 AM

To: [REDACTED]@stanford.edu>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@aspeninstitute.org>; [REDACTED]@gmail.com
<[REDACTED]@gmail.com>

Subject: Re: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

Ha! This gave me a chuckle as I can literally hear reporters and editors speaking the objections you capture here.

That said, we were thinking you guys would go near the top of the meeting and this feels a bit, uh – hostile for a first time meeting of this group on this topic. And with the exception of the last question, does not address the role of the platform. Maybe you can reposition it as summary of your top recommendations and weave in some of the anticipated pushback but not make it the focus?

From: [REDACTED]@stanford.edu>

Date: Monday, June 15, 2020 at 8:06 PM

To: [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@aspeninstitute.org>; [REDACTED]@aspeninstitute.org>; [REDACTED]@gmail.com" [REDACTED]@gmail.com>

Subject: FOLLOW-UP -- Re: Hack and Leak Working Group - Agenda Discussion

Hey guys, [REDACTED] and I put together some bullet points to keep our planning discussion going, as requested. These are the objections we heard during our meetings, followed by our rebuttal. We went through some version of this back-and-forth before really getting into the substance of our recommendations in pretty much all of our meetings.

Should we connect again later this week?

Best.... [REDACTED]

- Objection: "We can't/won't/don't collaborate with other news organizations on breaking news."
 - Response: But you do share many common values and norms that result in like-minded reports and editors making similar decisions independently of one another. Example: Ukraine whistleblower's identity. And it's not like you never talk to your colleagues either....
- Objection: "You can't expect us to not cover newsworthy events, and disinformation, misinformation, hack-and-leaked documents, etc are often newsworthy."
 - Response: Of course, and that's not what we're saying. What we are saying is that you still have to cover newsworthy events in a responsible manner.
- Objection: "News moves too fast for us to impose a ton of structure along the lines of what you propose."
 - Response: You already have structure in the form of written standards, performance criteria, and so on. What we are arguing for is integrating norms and practices for responsible reporting on propaganda, hack-and-leak etc into these existing structures.
- Objection: "We're already on top of this. For example, we have experts give presentations and advice on this topic to our reporters."
 - Response: Didn't you just tell us that news moves too fast to be on top of this? And how do you ensure that your reporters take the advice, given the competitive dynamics of the profession that put a premium on being first to break a story? Is there are any follow-through from editors and senior management?
 - "We rely on them as professionals to do the right thing."
 - Response: Do you have any management guidance for your reporters so that they know what their leadership considers to be the right thing?
 - "If we produced written standards on this topic, we'd get chewed up by media watchdog groups. We know we're not perfect but there have been instances where the criticism is simply not helpful."
- Objection: "We don't get too caught up in the competitive dynamics with other news organizations. We take the time to get the story right."
 - [Later in the conversation]: "Our search engine optimization team is always pushing us to

- Objection: “The biggest problems are with the social media companies, who operate in a normative vacuum while making a ton of money in the process. You should do a project on them too.”



--

Stanford University
Cell: [REDACTED]

--

Stanford University
Cell: [REDACTED]

Produced to HJC

Exhibit 93

From: [REDACTED]@aspeninstitute.org>
To: [REDACTED]
Sent: 7/13/2020 12:44:57 PM
Subject: Re: Tomorrow's H/L meeting

Excellent! [REDACTED] just texted you. ([REDACTED] I always have a hard time convincing him to take my calls because he assumes any [REDACTED] phone call is just spam!)

From: [REDACTED]@fb.com>
Sent: Monday, July 13, 2020 3:39 PM
To: [REDACTED]@aspeninstitute.org>; [REDACTED]@fb.com>
Cc: [REDACTED]@aspeninstitute.org>
Subject: Re: Tomorrow's H/L meeting

This all makes sense to me. Two thoughts:

(1) I will likely have to drop about 2/3rds of the way through (I have to go see my family, and the latest I can get on a plane, which is super weird during a pandemic, means I need to leave for the airport at 10 am)

[sidebar, [REDACTED] this means I'll be in VT for a while... perhaps we can do socially distanced drinks!]

(2) I think focusing in on the "suspected/not confirmed" point is important. One of the hardest operational challenges here will be at what point we have enough data to cross over into labelling. We could label something as "suspected" linked to a foreign IO, but do people prefer injecting uncertainty into the label in return for being able to move much more quickly?

From: [REDACTED]@aspeninstitute.org>
Sent: Monday, July 13, 2020 12:34 PM
To: [REDACTED]@fb.com>; [REDACTED]@fb.com>
Cc: [REDACTED]@aspeninstitute.org>
Subject: Tomorrow's H/L meeting

Hi guys,

We've got pretty good rsvp for tomorrow's meeting. We thought we'd focus this session on attribution and context – the so called 'third paragraph' question. For next organizations that means answering questions like:

- How should news organizations respond initially to events that are likely hack-and-leaks, e.g., a Wikileaks or DC Leaks dump, but whose provenance/attribution is unclear?
- What's the context that should be placed by news organizations around suspected hack-and-leaks?
- How should that context change if/when there's a suspected-but-not-confirmed provenance?
- How should that context change if/when there's a "confirmed" provenance from government intelligence?

For Facebook (and others), it's some of the above certain, plus how should platforms label suspected
hack-and-leaks? Final Report 1434

We asked the [REDACTED] to talk about how two part of the same news organization approach
these issues. CNN may weigh in as well. I'm sure, [REDACTED] your provocation about labeling will make for robust
discussion as well.

Any questions? Concerns? Comments?

[REDACTED]

Produced to HJC

Exhibit 94

From: [REDACTED]@aspeninstitute.org>
To: [REDACTED]
CC: [REDACTED]
Sent: 9/28/2020 12:01:48 PM
Subject: Hack-and-leaks and contested elections
Attachments: Election.Coverage.Principles.final.docx; Hack.leak.response.final.docx

[REDACTED]

I wanted to pass along drafts that we've been working on to publish out of both the summer hack-and-leak series and the "Day After" contested election conversations. There's no reference to tech platforms or anyone's participation in either series (and actually the principles don't mention the existence of any series of meetings at all) but I did want to pass them both along in case you had any suggestions/edits/thoughts (or if, for whatever reason, you were interested in having Facebook's participation specifically mentioned).

Anyway, regardless thought you'd be interested. Our hope is that the hack-and-leak piece gets published as an oped somewhere, and once we add a short intro, we're going to try to publish the contested election principles somewhere too.

[REDACTED]

Produced to HJC

Exhibit 95



Hack and Leak Roundtable Participant List June 25, 2020

[REDACTED]
Director of Policy
Reddit

[REDACTED]
Director of Security
Wikimedia Foundation

[REDACTED]
Reporter
NBC News

[REDACTED]
EVP, News Standards and Practices
CNN

[REDACTED]
Head of Cybersecurity Policy
Facebook

[REDACTED]
Director Cybersecurity Initiatives
Aspen Institute

[REDACTED]
Director
Stanford Cyber Policy Center

[REDACTED]
Co-Founder and Editor
The Dispatch

[REDACTED]
Executive Editor
Lawfare

[REDACTED]
Director Public Policy Strategy
Twitter

[REDACTED]
Senior VP
Poynter Institute

[REDACTED]
VP and Deputy General Counsel
The New York Times

[REDACTED]
National Security Reporter
Washington Post

[REDACTED]
Staff writer
New Yorker

[REDACTED]
Reporter
CNN

[REDACTED]
Investigations Correspondent
NPR

[REDACTED]
Former Editor in Chief, Guardian
Member of Facebook Oversight Board

[REDACTED]
Chief Washington Correspondent
New York Times

[REDACTED]
Editor in Chief
The Daily Beast



[REDACTED]
Executive Director
Aspen Institute

[REDACTED]
Cybersecurity Correspondent
Reuters

[REDACTED]
Cofounder and Director
First Draft News

[REDACTED]
Global Public Policy Lead for
Information Integrity
Google

[REDACTED]
Visiting Lecturer,
Stanford

Exhibit 96

To: [Redacted - PII]
Cc: [Redacted - PII] [Redacted - PII]
From: [Redacted - PII]
Sent: Wed 8/12/2020 12:49:20 PM (UTC)
Subject: Hack and Leak "finale"

Hello Friends,

Thank you for your engagement in our discussion about hack and leaks. I hope you agree it's been a really fruitful conversation so far. Please join us for our third – and last – session on Wednesday, September 2 at 12p-2pET. In this meeting, we'll walk through a fictional scenario that [Redacted] has designed, and talk through our thought processes about disclosure, reporting, labeling and the like. It's not so much a table top as a "think out loud session" about a simulation. (let's just say that it gave me agita when I read it!)

This will be our last meeting of this series. We are looking to publish a document that supplements the good work of [Redacted] and [Redacted], with a focus on the interplay between what shows up in feed and on the 'pages' of the news media.

A calendar invite will follow shortly.

Cheers,

[Redacted]

--

[Redacted]

Executive Director, Aspen Digital

The Aspen Institute

[Redacted - PII]

@ [Redacted]



Exhibit 97

Message

From: [REDACTED]@fb.com]
Sent: 9/20/2020 8:49:16 PM
To: [REDACTED]@fb.com]; [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbId": [REDACTED], "threadFbId": null}]

[REDACTED] (9/20/2020 17:03:58 PDT):
>Hey, am rewriting the hack/leak tabletop scenario based on latest

[REDACTED] (9/20/2020 17:04:07 PDT):
>will send to you later for any feedback

[REDACTED] (9/20/2020 17:04:12 PDT):
>with apologies for short turn

[REDACTED] (9/20/2020 19:40:35 PDT):
>hi frined

[REDACTED] (9/20/2020 19:40:36 PDT):
>ok

[REDACTED] (9/20/2020 19:40:40 PDT):
>i am back online

[REDACTED] (9/20/2020 19:40:43 PDT):
>hello

[REDACTED] (9/20/2020 19:40:46 PDT):
>congrats on your pilot's license

[REDACTED] (9/20/2020 19:40:48 PDT):
>i briefly disappeared to do eating

[REDACTED] (9/20/2020 19:40:54 PDT):
>thank you!

[REDACTED] (9/20/2020 19:41:02 PDT):
>i now have a backup career if the election goes poorly

[REDACTED] (9/20/2020 19:41:04 PDT):
>i am doing this now

[REDACTED] (9/20/2020 19:41:07 PDT):
>not the best backup cuz... covid

[REDACTED] (9/20/2020 19:41:09 PDT):
>hire me

[REDACTED] (9/20/2020 19:41:28 PDT):
>honestly a [REDACTED] + [REDACTED] jet crew would be pretty great

[REDACTED] (9/20/2020 19:41:55 PDT):
>happy to review the scenario whenever tho! I'm gonna be up late working on this Russia takedown

[REDACTED] (9/20/2020 19:41:59 PDT):
>how was your day of many many meetings

[REDACTED] (9/20/2020 19:41:59 PDT):
>so there seems to be desire to tweak hack/leak scenario for table-top to be leak and not hack

[REDACTED] (9/20/2020 19:42:04 PDT):
>the worst

[REDACTED] (9/20/2020 19:42:07 PDT):
>just the worst

[REDACTED] (9/20/2020 19:42:13 PDT):
>i can only image. feel for y'all

[REDACTED] (9/20/2020 19:42:22 PDT):

>you were on there for my hideous on-the-spot attempt at foreign interference right?

[REDACTED] (9/20/2020 19:42:29 PDT):

>this kinda makes sense. it's definitely a harder policy question

[REDACTED] (9/20/2020 19:42:45 PDT):

>ha, i was, but if it was hideous it was because our M-team does not entirely understand how to define foreign itnerference

[REDACTED] (9/20/2020 19:43:34 PDT):

>no, it was because i was all about hack-leak this afternoon and had zero indication that after asking none of our team to present these topics over the weekend, she'd feel compelled to ask us to kick off foreign interference

[REDACTED] (9/20/2020 19:44:08 PDT):

>anyway, getting down to business on this scenario, will send shortly.

[REDACTED] (9/20/2020 19:45:06 PDT):

>roger dodger

[REDACTED] (9/20/2020 20:30:04 PDT):

>okay how's this --

[REDACTED] (9/20/2020 20:31:15 PDT):

>No major changes to the scene-setter; only changes are in bullet 1:

>

>*Scene-setter:* It's the morning of Monday, October 5. Widespread vote-by-mail and early in-person voting is about to begin (in some states, vote by mail and early in-person voting have already begun). In recent weeks, vote-by-mail has continued to be heavily criticized by some for its alleged susceptibility to fraud. Polls suggest that the presidential race in battleground states is tight. Media reports suggest that:

>

>-- Some commentators are circulating rumors that embarrassing confidential information is about to be leaked about one of the presidential candidates.

>-- QAnon supporters are reportedly expecting a major new 'drop' from 'Q' soon — possibly a heads-up on a coming indictment.

>-- Some partisan activists may be planning to disseminate false information about how to vote by mail and conditions at early voting locations, including health risks, in an effort to decrease turnout.

[REDACTED] (9/20/2020 20:31:58 PDT):

>*Inject #1: Monday October 5*

>

>Issue B: Comms flags to the Elections Comms XFN workchat thread that a foreign businessperson has just tweeted that they are 'blowing the whistle' on one of the presidential candidates by *releasing confidential information* about their company's business dealings with the candidate's family. The businessperson posted on Twitter images they describe as screenshots of documents reflecting a confidential business deal, and stated that they have disseminated other such screenshots to unnamed "partners" for further distribution. The screenshots posted on Twitter, taken at face value, appear to show that the presidential candidate was involved in an effort to trade future official actions in exchange for their family's business advantage in a country in Asia. Political junkies start discussing on Twitter, but as yet, no wire services or major broadcast/cable networks have run stories. The candidate's campaign immediately denies that the candidate or his family had any relationship with the businessperson and describes the documents as "fakes."

[REDACTED] (9/20/2020 20:32:34 PDT):

>*Inject #2: Wednesday October 7*

>

>Issue B: Shortly after the tweet, mainstream media began reporting on it. Some stories emphasize that the businessperson's story about his position checks out, and that the screenshots of the documents do not show any obvious signs of being forgeries. Other stories question the businessperson's credibility and the authenticity of the documents, and raise the possibility that a foreign state actor is behind this. Posts linking to the foreign businessman's tweet, and posts with the images in the tweet, appeared on our platform shortly after the tweet, gained substantial distribution, and look likely to go viral over the

next 24 hours. Analysis of the posters shows no significant signals of coordination between them or links to known foreign state actors. Law enforcement has told us they cannot definitively confirm or rule out the possibility of foreign government involvement in the matter. I3 identifies a URL that is hosting the images posted in the tweet, as well as a number of additional images that are described on the site as being additional screenshots of similar business records.

[REDACTED] (9/20/2020 20:32:52 PDT):

>*Inject #3: Friday October 9*

>

>Issue B: A meme with the words "Corrupt [Candidate]" superimposed over an image of one of the screenshots is posted by a number of users and looks likely to go viral over the next 24 hours.

[REDACTED] (9/20/2020 20:32:59 PDT):

>grateful for feedback

[REDACTED] (9/20/2020 20:33:42 PDT):

>these are good

[REDACTED] (9/20/2020 20:34:14 PDT):

>might be worthwhile to include IC or LE info that indicates that there *was* a foreign government involved in obtaining the documents, but nthing definitive

[REDACTED] (9/20/2020 20:34:19 PDT):

>its most similar to where we are at on Burisma

[REDACTED] (9/20/2020 20:34:36 PDT):

>but will make Mteam folks remember that in 2016 the public did not have conclusive evidence of GRU activity re: podesta

[REDACTED] (9/20/2020 20:37:52 PDT):

>Thanks - just to make sure I understand --

>

>LE or IC has told us that there was a foreign govt involved in obtaining the documents, but we don't view that as definitive because it's just LE/IC's word for it?

>

>Or the LE/IC info says there is some indication a foreign govt *may* have been involved in obtaining the docs, but isn't definitive on that?

[REDACTED] (9/20/2020 20:38:40 PDT):

>more like, they've told us at a classified level that they think a government was involved in obtaining info

[REDACTED] (9/20/2020 20:38:43 PDT):

>but not unclass

[REDACTED] (9/20/2020 20:38:47 PDT):

>idk how you include that ha

[REDACTED] (9/20/2020 20:38:51 PDT):

>but its not evidence we could *talk about*

[REDACTED] (9/20/2020 20:39:25 PDT):

>at an unclass level, they told us is *may* have been a government, and they dont have conclusive evidence tha tthe dissemination mechanism (hte leaker in your example) is controlled by a government

[REDACTED] (9/20/2020 20:45:13 PDT):

>okay, thanks - don't want to directly mirror stuff since this is supposed to be hypo, but is this better for the govt line?

>

>Law enforcement tells us they believe a specific foreign government is likely involved in the episode, but the investigation is ongoing and they cannot yet draw definitive conclusions or release any information publicly.

[REDACTED] (9/20/2020 20:46:02 PDT):

>i think so, yes

[REDACTED] (9/20/2020 20:47:24 PDT):

>okay thanks! looking fwd to the discussion. good luck with all your stuff that is actually work on real things instead of . . . fake things

[REDACTED] (9/20/2020 20:47:30 PDT):

>haha

[REDACTED] (9/20/2020 20:47:37 PDT):
>thanks for keeping us all on track mate

[REDACTED] (9/20/2020 20:47:41 PDT):
>hope you're holdin up ok

[REDACTED] (9/20/2020 20:47:47 PDT):
>are you still in PA?

[REDACTED] (9/20/2020 20:47:55 PDT):
>na, back in Cali

[REDACTED] (9/20/2020 20:47:57 PDT):
>otherwise id invite you to fly up to Shelter Cove one of these weekends

[REDACTED] (9/20/2020 20:47:59 PDT):
>ohhh

[REDACTED] (9/20/2020 20:48:08 PDT):
>needed to give justin and kate and kids some family time :)

[REDACTED] (9/20/2020 20:48:09 PDT):
>well then, lmk if you want to do a day trip up to shelter cove

[REDACTED] (9/20/2020 20:48:17 PDT):
>yeah for sure

[REDACTED] (9/20/2020 20:48:20 PDT):
>thatd be awesome

[REDACTED] (9/20/2020 20:48:36 PDT):
>with this damn license out of the way im gonna try and do some fun flights before starting instructor training lol

[REDACTED] (9/20/2020 20:48:45 PDT):
>how big's your plane? we could get [REDACTED] and his wife maybe?
>
>thats so cool

[REDACTED] (9/20/2020 20:48:57 PDT):
>we could I think! it seats 4 including me)

[REDACTED] (9/20/2020 20:49:03 PDT):
>oh wow aweomse

[REDACTED] (9/20/2020 20:49:04 PDT):
>so we could fit the four of us!

[REDACTED] (9/20/2020 20:49:07 PDT):
>do u want to ask him?

[REDACTED] (9/20/2020 20:49:13 PDT):
>yeah! ill start a fb chat

[REDACTED] (9/20/2020 20:49:16 PDT):
>sweet

Exhibit 98

From: [REDACTED]@gmail.com>
To: [REDACTED]@ceip.org; [REDACTED]@twitter.com;
CC: [REDACTED]
Sent: 8/7/2020 6:44:41 AM
Subject: Hack-and-leak brainstorm this morning
Attachments: Burisma.leak.docx

All,

Thanks for joining us this morning at 11 a.m. ET to help brainstorm the informal tabletop exercise we want to put our reporter/tech group through on a potential hack-and-leak for the fall election. The meeting/Zoom information should be in the calendar invite, but I've also posted it below.

I've attached the working scenario right now; we're hoping that among us at 11 ET, we can iterate this, refine it, complicate it, and polish a scenario that would help all of the group think through how they would respond to various twists and turns in a Burisma-focused leak incident this fall. Bring your most devious and cynical imaginations!

Please keep this document confidential to yourselves; for various reasons, we don't want this to circulate widely.

Join Zoom Meeting

[https://aspeninst.zoom.us/\[REDACTED\]](https://aspeninst.zoom.us/[REDACTED])

Meeting ID: [REDACTED]

Passcode: [REDACTED]

Dial by your location

One tap mobile

--

[REDACTED]
Director, Cyber Initiatives
The Aspen Institute

Exhibit 99

To: [Redacted - PII]
Cc: [Redacted - PII] [Redacted - PII]
From: [Redacted - PII]
Sent: Tue 9/1/2020 7:44:00 PM (UTC)
Subject: Re: Hack and Leak "finale"

Hi Everyone,

Last email before tomorrow's final installment of our informal summer working group on hack-and-leak operations.

As I mentioned, we're going to spend tomorrow's session working through collectively an exercise that [Redacted] has designed, with some outside input, about how a terrifyingly real hack-and-leak operation might unfold over ten days this fall. To help orient you, here's the basic outline of Day One of the scenario:

Day One: Monday, October 5th

- An anonymous website, BIDENCRIMES.info, and a Twitter account, @HUNTERLOLZ, begin posting documents that purport to be from Burisma, tied to Hunter Biden. Splashed across the top of the site, in English, is "Joe Biden betrayed america before for \$\$\$\$. He'll do it again." Initially, the documents, mostly in Ukrainian, appear to be minutes of various Burisma board meetings, internal emails, and financial records. There is initially no sign of a smoking gun. The website appears to have been first registered in 2016. No ownership information is public. The Twitter account was created in 2014, oddly just before Hunter joined the Burisma board. It has tweeted once and follows one person.

From there, using some of the most cynical and devious minds we could find, we've designed various inputs and developments and are going to ask all of you to help think through out loud how you'd respond in your own roles, what you'd think at various points, and game out how various tech platforms and news organizations would respond in real time as the story unfolded. This is not a traditional table-top so much as an opportunity to hear others' thinking in reaction to evolving pieces of evidence, campaign reactions, and more.

We're appreciative of all the thinking and conversation you've brought to this so far and are eager to hear the results of tomorrow.

See you on the Zoom!

[Redacted], [Redacted] and [Redacted]

From: [Redacted - PII] <[Redacted - PII]> on behalf of [Redacted]
<[Redacted - PII]>
Date: Wednesday, August 12, 2020 at 8:49 AM
To: [Redacted] <[Redacted - PII]>
Cc: [Redacted] <[Redacted - PII]>, [Redacted] <[Redacted - PII]>
Subject: Hack and Leak "finale"

Hello Friends,

Thank you for your engagement in our discussion about hack and leaks. I hope you agree it's been a really fruitful conversation so far. Please join us for our third – and last – session on Wednesday, September 2 at 12p-2pET. In this meeting, we'll walk through a fictional scenario that [Redacted] has designed, and talk through our thought processes about disclosure, reporting, labeling and the like. It's not so much a table top as a "think out loud session" about a simulation. (let's just say that it gave me agita when I read it!)

This will be our last meeting of this series. We are looking to publish a document that supplements the good work of [REDACTED] and [REDACTED], with a focus on the interplay between what shows up in feed and on the 'pages' of the news media.

A calendar invite will follow shortly.

Cheers,

[REDACTED]

--

[REDACTED]

Executive Director, Aspen Digital

The Aspen Institute

Redacted - PII

[REDACTED]



Exhibit 100

CONFIDENTIAL

Aspen Digital Hack-and-Dump Working Group — September 2020

EXERCISE :: The Burisma Leak

Day One: Monday, October 5th

- Anonymous website, BIDENCRIMES.info, and a Twitter account, @HUNTERLOLZ, begin posting documents that purport to be from Burisma, tied to Hunter Biden. Splashed across the top of the site, in English, is “Joe Biden betrayed america before for \$\$\$\$. He’ll do it again.” Initially, the documents, mostly in Ukrainian, appear to be minutes of various Burisma board meetings, internal emails, and financial records. There is initially no sign of a smoking gun.
 - NOTE: The website appears to have been first registered in 2016. No ownership information is public. The Twitter account was created in 2014, oddly just before Hunter joined the Burisma board. It has tweeted once and follows one person.

Day Two: Tuesday, October 6th

- The Drudge Report links to the anonymous website, BIDENCRIMES.info, and the site is quickly picked up by other fringe media and begins to spread on social media sites.

Day Three: Wednesday, October 7th

- *Fox & Friends* discusses BIDENCRIMES.info in its 7 a.m. block. @realDonaldTrump tweets six minutes later, “Is Joe Biden biggest criminal of all time? Check out @HUNTERLOLZ.”
- Three reporters (Dina Temple-Rason, Donie O’Sullivan, and Ellen Nakashima) are contacted by an anonymous ProtonMail account, BIDENCRIMES@protonmail.com, and each sent a different document. None of the documents have appeared on the public website. They are each told they are the only reporter receiving a specific document.
 - Dina’s document purports to be a ledger of payments showing that Hunter Biden was paid \$3 million over two months in 2015 by Burisma, far more than had been reported publicly before.
 - Donie’s document is a 2016 email, purportedly from Hunter to his father, dated the evening before the firing of prosecutor Viktor Shokin, simply titled “Burisma,” and the body of which reads: “I really need you to do this for me.”
 - Ellen’s document purports to be the board contract between Burisma and Hunter.
- In Ukraine, Burisma announces that it has no evidence of any hack of its servers, disavows all files as forgeries.

Day Four: Thursday, October 8th

- The Biden campaign, adopting the policy of Hillary Clinton's campaign in 2016 and the Macron campaign, says they will not confirm the veracity of any documents.
- CrowdStrike announces, without further detail, it has reason to believe that BIDENCRIMES.info is the work of Fancy Bear (APT 28).
- CNN's Jim Scuitto reports an anonymous Cloudflare executive who says that he doubts the CrowdStrike appraisal; Cloudflare believes that no foreign actor is involved and has evidence that BIDENLEAKS.info is being hosted and run by Americans.
- At 4 p.m., the *Washington Post* publishes a story by Ellen Nakashima confirming that the Burisma board contract given to her is legitimate; there is no wrongdoing evident or alleged in the document, but Burisma sources confirm the document is real.
- Cesar Conde, the chairman of NBC News, announces that because of the suspicion that the BIDENCRIMES.info leaks are coming from a foreign power with a goal of undermining America's free and fair elections, no aspect of NBC News or MSNBC will report on the allegations or use the materials as the basis for reporting. In his statement, carried live on the evening news with Lester Holt, he asks all other news organizations to follow NBC's leadership. The Guardian quickly announces it will follow the same principle, as does The Huffington Post.
- At Ohio Trump rally that night, crowd starts chanting "LOCK HIM UP." President Trump, at podium, pumps his fists as the crowd chants.

Day Five: Friday, October 9th

- In a statement released at 9 a.m. and signed only by him, Director of National Intelligence John Ratcliffe says he has no reason to believe the documents posted by BIDENCRIMES.info are forgeries, nor does the IC have reason to believe the website is a Russian operation.
- At 11 a.m., on the House floor, House Intelligence Chair Adam Schiff says that according to his briefings, the IC is not being forthright with the American people about the source and veracity of the leaks.
- Also at 11 a.m., Mandiant releases a short statement saying it has traced the source of BIDENLEAKS.info to infrastructure consistent with China's Ministry of State Security.

- At 2 p.m., @HUNTERLOLZ tweets a link out to a .zip file that appears to contain a new tranche of 20,000 documents, mostly in Ukrainian, stolen from Burisma and posted on BIDENCRIMES.info.
- All but simultaneously, at 2:01 p.m., @DonaldJTrumpJr, @TeamTrump, and @parscale all retweet the @HUNTERLOLZ post.
- By 3 p.m., Twitter determines that the hosting service for the .zip tweeted by @HUNTERLOLZ traces back to a server in Hong Kong.
- That afternoon, Facebook’s sources inside the IC tell Facebook to be wary about the DNI’s statement.
- At 5 p.m., Dina Temple-Raston airs an NPR story saying that she has confirmed the \$3 million payment document she received is fake.

Day Six: Saturday, October 10th

- Overnight, progressive blogger Josh Marshall notices and tweets out one document in the new tranche of .zip files that appears to be a confirmation of a wire transfer for \$1 million from Deutsche Bank to an off-shore account in the name of Hunter Biden, dated two days after the firing of the chief prosecutor, Shokin. Overnight, independent security researchers and news organizations find the majority of the .zip files are authentic, but some are manipulated. First Draft News tweets an hour after Josh’s tweet that his document appears to be an authentic Burisma document but has been edited—what was edited is unclear.
- At 10 a.m., the *New York Times* posts a story saying that two anonymous “senior Justice Department officials” in Washington say that the acting U.S. attorney in D.C. has empaneled a grand jury to investigate Joe Biden.

Day Seven: Sunday, October 11th

- On the Sunday shows, Biden campaign staff dismiss the entire hack-and-leak as dirty tricks by Vladimir Putin.
- After the morning shows air, *The Daily Beast* quotes two “former senior intelligence officials” that the directors of the CIA and NSA refused to sign onto Ratcliffe’s Friday statement, although sources differ why they did not sign it. David Sanger matches that reporting an hour later.
- Alex Berenson announces on Twitter that he’s conducted an interview, via DM, with the person behind @HUNTERLOLZ and that he believes the person is an American.

Day Eight: Monday, October 12th

- At 7:15 a.m., President Trump calls into *Fox & Friends* and says he hopes the FBI will investigate Joe Biden.
- At 9 a.m., Attorney General Bill Barr holds a press conference to say the American people deserve the truth and that he has instructed the FBI to verify the allegations of Joe Biden and Hunter Biden's corruption. He announces that the Justice Department is investigating wrongdoing by Hunter Biden and Joe Biden for money laundering, tax fraud, theft of honest services, and acting as an unregistered foreign agent. In response to a reporter's question, he volunteers that he believes Joe Biden should submit to an FBI interview within days.
- At 11 a.m., Senator Richard Blumenthal says the American people are being lied to and demands in a CNN interview, "Paul Nakasone, Gina Haspel, and Chris Wray owe Americans the truth. I can't say more than that."
- At 2 p.m., Jim Comey tweets "FBI agents tell me they are being silenced about the truth. Donald Trump is illegally coordinating with Putin. He must resign."
- At 7:30 p.m., Rudy Giuliani says on Fox News that he was right all along re: 2019 Ukraine pressure campaign.

Day Nine: Tuesday, October 13th

- @realDonaldTrump tweets at 6:15 a.m.: "See, Ukraine phone call was perfect — I knew Sleepy Joe was actually Crooked Joe! Tell FBI: LOCK HIM UP!"

Day Ten: Wednesday, October 14th

- Rep. Devin Nunes, Sen. Tom Cotton, and Secretary of State Mike Pompeo announce they will travel immediately to Kiev to get Burisma's cooperation with the unfolding investigation. They depart that night on an official US government jet.

Day Eleven: Thursday, October 15th

- The second presidential debate

Bidencrimes.info 17 letters,

Exhibit 101

From: Sender Unspecified
To: Joel Kaplan <[REDACTED]@s.whatsapp.net>; Nick Clegg <[REDACTED]@s.whatsapp.net>; System Message <>
Sent:
Subject: (No Subject)
Attachments: rsmf.zip

Nick Clegg <[REDACTED]@s.whatsapp.net>

Which team is responsible for checking how/whether this could be a false hack/leak?
<https://mobile.twitter.com/JuddLegum/status/1316376280103825409>

Nick Clegg <[REDACTED]@s.whatsapp.net>

Ignore - see it's shared on 2020 thread

Joel Kaplan <[REDACTED]@s.whatsapp.net>

I think it's actually kinda outrageous that we are all freaking out about a NY Post cover story, enqueing and demoting because liberals are tweeting about it, with no evidence whatsoever. We did not do this when the NYT dunoed an expose on Trump's tax returns citing leaked documents that they wouldn't even share.

Joel Kaplan <[REDACTED]@s.whatsapp.net>

Dumped.

System Message <SystemMessage>

Missed Voice Call

Nick Clegg <[REDACTED]@s.whatsapp.net>

Just on a call

Joel Kaplan <[REDACTED]@s.whatsapp.net>

We have to decide whether to undo this demotion. None of [REDACTED], [REDACTED], [REDACTED], [REDACTED], or I think this was appropriate/justified. But Unwinding will likely leak and be a story (conversely, doing things that might be perceived as anti-conservative, like demoting the content, never seem to leak).

Nick Clegg <[REDACTED]@s.whatsapp.net>

Yea I see - unwinding it now will unfortunately create more headaches than it's worth. Calling now

Joel Kaplan <[REDACTED]@s.whatsapp.net>

One thing to clarify-The difficult issue is that the demotion was NOT automatic (we manually demoted it). That's what makes it hard-if it were automatic, it would be sort of an easy call not to intervene.

Nick Clegg <[REDACTED]@s.whatsapp.net>

Yep will clarify

Joel Kaplan <[REDACTED]@s.whatsapp.net>

Fuck fuck fuck.

Joel Kaplan <[REDACTED]@s.whatsapp.net>

<https://twitter.com/trumpwarroom/status/1316398578995257344?s=21>

Joel Kaplan <[REDACTED]@s.whatsapp.net>

I took a call from the WH, which is extremely baffled and agitated, and asking all the questions one would expect them to ask about the process of soft demotion, how articles get selected to go to fact checkers, whether the Atlantic piece about Pres Trump calling soldiers stupid—which they flatly denied—was sent to 3 PFCs and demoted.

Nick Clegg <[REDACTED]@s.whatsapp.net>

Ugh - don't blame them at all - so sorry just don't feel I can decently jump off this call until 11

Nick Clegg <[REDACTED]@s.whatsapp.net>

free now - shall I call?

Nick Clegg <[REDACTED]@s.whatsapp.net>

Obviously, our calls on this could colour the way an incoming Biden administration views us more than almost anything else...

Nick Clegg <[REDACTED]@s.whatsapp.net>

should i call MZ and "inform" him of what we're doing?

Nick Clegg <[REDACTED]@s.whatsapp.net>

Sheryl adamant that we should NOT demote as she thinks we break into jail with the Dems.

Joel Kaplan <[REDACTED]@s.whatsapp.net>

You mean not not demote?

Joel Kaplan <[REDACTED]@s.whatsapp.net>

<https://twitter.com/realDonaldTrump/status/1316501350658707456>

Joel Kaplan <[REDACTED]@s.whatsapp.net>

So we just let it sit for 7 days? Even reporters who defended us today made clear it was to give fact checkers and chance to rate.

Nick Clegg <[REDACTED]@s.whatsapp.net>

She asks what Twitter is doing re virality? If we don't lift the demotion won't it just go massively viral, she asks?

Nick Clegg <[REDACTED]@s.whatsapp.net>

She's now called MZ who is saying we should do "what we normally do" on a demotion...

Joel Kaplan <[REDACTED]@s.whatsapp.net>

I give up.

Nick Clegg <[REDACTED]@s.whatsapp.net>

SS is pressing MZ v hard on this...

Nick Clegg <[REDACTED]@s.whatsapp.net>

MZ says ok to wait another 24 hours to see whether 3PFCs

Produced to HJC

Exhibit 102

(A/C PRIV) Five Factors — Hack/Leak Policy Assessment - Laptop 1

1. Do we believe that the actor responsible for the leak is directed by a foreign gov't? (we will presume that a US government actor does *not* meet this factor)

Current Assessment (10/20/2020):

We currently have low to medium confidence that these documents and story are part of a foreign government influence operation.

Previous Assessments:

- 10/19/2020 - Low to medium confidence
- 10/16/2020 — Low confidence

Policy Language: PRIVACY VIOLATIONS & IMAGE PRIVACY - On Escalation Only Policy:

a. Remove

- source material that purports to reveal nonpublic information about the US/2020 election shared as part of a foreign government influence operation (*determined by Cyber XFN*)
- reporting on such a leak by state-controlled media entities from the country behind the leak (*determined by Cyber XFN*)

OFF PLATFORM FACTORS

Low to Medium Confidence

	Source	Primary Sources	Intel	Relevant Links
1	The New York Times	United States intelligence analysts	intelligence analysts started contacting several people with knowledge of the GRU hack of Burisma, after picking up intelligence “chatter” that stolen Burisma emails would be leaked in a forthcoming “October surprise.”	https://www.nytimes.com/2020/10/14/us/politics/hunter-biden-ukraine-facebook-twitter.html
2	The Washington Post	four former officials familiar with the matter	U.S. intelligence agencies warned the White House last year that President Trump’s personal lawyer Rudolph W. Giuliani was the target of an influence operation by Russian intelligence	https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43158900-0ef5-11eb-b1e8-16b59b92b36d_story.html
3	The Washington Post	former officials familiar with the matter	national security adviser Robert O’Brien cautioned Trump in a private conversation that any information Giuliani brought back from Ukraine should be considered contaminated by Russia	https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43158900-0ef5-11eb-b1e8-16b59b92b36d_story.html
4	NBC News	two people familiar with the matter	Federal investigators are examining whether the emails allegedly describing activities by Joe Biden and his son Hunter and found on a laptop at a Delaware repair shop are linked to a foreign intelligence operation	https://www.nbcnews.com/politics/national-security/feds-examining-if-alleged-hunter-biden-emails-are-linked-foreign-n1243620
5	The Daily Beast	Rudy Giuliani	The U.S. Treasury Department may have declared one of his former associates—Ukrainian parliamentarian Andrii Derkach, who worked with Giuliani on his hunt for dirt on the Bidens—to be an “active Russian agent.” But that’s some Deep State talk, he	https://www.thedailybeast.com/rudy-giuliani-says-theres-only-5050-chance-i-worked-with-a-russian-spy-to-dig-dirt-on-bidens

Source	Primary Sources	Intel	Relevant Links
		added. "The chance that Derkach is a Russian spy is no better than 50/50."	

2. Do we believe that the leak is part of a foreign influence operation to manipulate the election? (with sufficiently strong consensus, this factor could necessitate action on a release from a US government actor)

Low to Medium Confidence

	Source	Primary Sources	Intel	Relevant Links
1	Business Insider Investigations Team	Repair shop owner; Andriy Derkach to Washington Post (in Dec. 2019)	The same month that the repair shop's owner was said to have given Giuliani's lawyer a copy of the hard drive, Giuliani <u>met with a Ukrainian national named Andriy Derkach</u> to discuss efforts to obtain damaging information on Joe Biden before the 2020 election.	https://www.businessinsider.com/new-york-post-hunter-joe-biden-giuliani-red-flags-disinformation-2020-10
2	The Daily Beast	Fox News research team	Fox News' own research team has warned colleagues not to trust some of the network's top commentators' claims about Ukraine. "Reading the timeline in its entirety—not a small task—makes clear the extensive role played by Rudy Giuliani and his associates, Lev Parnas and Igor Fruman, in spreading disinformation," Murphy writes.	https://www.thedailybeast.com/fox-news-internal-document-bashes-john-solomon-joe-digenova-and-rudy-giuliani-for-spreading-disinformation
3	The Washington Post	US intelligence officials	Earlier in 2019, U.S. intelligence also had warned in written materials sent to the White House that Giuliani, in his drive for information about the Bidens, was communicating with Russian assets.	https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43158900-0ef5-11eb-b1e8-16b59b92b36d_story.html
4	Active Measures by Thomas Rid (Operation Neptune)	Circumstantial	Knowledge that Russian influence activities have historically included a hack-forge-leak pattern and the dumping of documents at the bottom of a lake to be then "found" and seized by intelligence officials. While this is anecdotal, it shows a history of these types of techniques being employed by these actors	https://www.wired.com/story/uncovering-operation-neptun-the-cold-wars-most-daring-disinformation-campaign/
5	CNN	a US official and a congressional source briefed on the matter	US authorities are investigating whether recently published emails that purport to detail the business dealings of <u>Joe Biden's son in Ukraine</u> and China are connected to an ongoing Russian disinformation effort targeting the former vice president's campaign. The FBI is leading the investigation.	https://www.cnn.com/2020/10/16/politics/russian-disinformation-investigation/index.html
6	The Daily Beast	Video shared by Eelco Bosch van Rosenthal of Nieuwsuur	Steve Bannon boasted on Dutch TV weeks ago that he had Hunter Biden's hard drive. The clip was not used by the channel at the time, but the journalist shared it on Friday after the NYPost story had come out. Bannon had teased that he'd release the contents before the presidential debate	https://www.thedailybeast.com/steve-bannon-boasted-on-dutch-tv-weeks-ago-that-he-had-hunter-bidens-hard-drive
7	The Daily Beast	YouTube Channel	The YouTube Channel run by Chinese fugitive Guoi Wengui, who is linked to Bannon as a business partner, was hyping the damaged hard drives around the same time as the Dutch interview mentioned above. The channel claimed that Chinese politburo officials had sent the hard disks of evidence to the Justice Department and Nancy Pelosi -- they hyped it as "Bombshell...3 hard disk drives of videos and dossiers of Hunter Biden's connections to the	https://www.thedailybeast.com/chinese-billionaires-network-hyped-hunter-biden-dirt-weeks-before-rudy

	Source	Primary Sources	Intel	Relevant Links
			CCP have been sent to Nancy Pelosi and DOJ. Big money and sex scandal!"	
8	Fox News	Ratcliffe	"Let me be clear. The intelligence community doesn't believe that because there is no intelligence that supports that."	https://twitter.com/quintforgey/status/1318166732419235841?s=21
9	The Daily Beast	Congressional source, senior intelligence official	The bureau, according to the congressional source, is looking into the provenance of the material. And among the questions they're seeking to answer is whether the laptop dump is part of what the intelligence community's counterintelligence chief has already described as a Russian disinformation effort targeting the 2020 election. One senior intelligence official told The Daily Beast that the community is still working to determine if the Hunter Biden materials—which were leaked to the press by Trump's personal attorney Rudy Giuliani—stem from a specific Russian intelligence operation.	https://www.thedailybeast.com/fbi-examining-hunter-bidens-laptop-as-foreign-op-contradicting-john-ratcliffe-trumps-intel-czar
10	FITF	LE engagement	FITF does not know where the narrative is coming from that they're investigating this.	n/a
11	Politico	Letter from 50 former intel officials	More than 50 former senior intelligence officials have <u>signed on to a letter</u> outlining their belief that the recent disclosure of emails allegedly belonging to Joe Biden's son "has all the classic earmarks of a Russian information operation." "the IC leaders who have signed this letter worked for the past four presidents, including Trump," said Nick Shapiro, a former top aide under CIA director John Brennan	https://www.politico.com/news/2020/10/19/hunter-biden-story-russian-disinfo-430276

ON-PLATFORM/BEHAVIORAL FACTORS

3. Do we or our industry partners see on-platform evidence of deception by the assets engaged in sharing the leaked material?

[Insert Confidence]

	Source	Primary Sources	Intel	Relevant Links
1				
2				
3				
4				
5				

4. Are there links to or amplification by known foreign government espionage or IO threat actors?

Low Confidence

	Source	Primary Sources	Intel	Relevant Links
1	Graphika	Data from Graphika analysis on other networks	Researchers at Graphika, who have tracked the NAEBBC operation linked by law enforcement to IRA activity, have seen amplification of this story and content by Russian actors across platforms Parler and Gab	IRA-on-Biden-Facebook-1
2	Threat Intel Assessment	n/a	The NY Post story was the top story in the U.S. News section of the Russian state-funded outlet RT	
3	Threat Intel Assessment	internal data	Known RU actors were seen querying on platform for related topics such as Burisma	
4				

CONTENT FACTORS**5. Do we or other experts have clear evidence that the source documents are manipulated to facilitate the narrative of an influence operation?**

Medium Confidence

	Source	Primary Sources	Intel	Relevant Links
1	Thomas Rid	Metadata	PDF/image metadata is suspicious - seems to be recently created.	https://twitter.com/RidT/status/1316441781043712005
2	The Daily Beast	Metadata	metadata on the PDF files purporting to show Hunter Biden's emails published by the <i>NYP</i> suggest they were created on a Mac laptop on September 29 and October 10, 2019. However, Sen. Ron Johnson (R-WI) and his staff told other lawmakers on Wednesday that they had received materials related to the contents of the <i>Post</i> story on September 25, the day after the publishing of his team's Hunter Biden report...The timing of the creation of those PDF files—several months after Biden allegedly dropped off his laptop at the PC repair store in April 2019—raises questions about how and when Giuliani came into possession of the purported emails."	https://www.thedailybeast.com/trump-knew-for-weeks-that-rudy-giulianis-hit-on-hunter-biden-was-coming
3	Business Insider Investigations Team	Metadata	The metadata that Poulsen tweeted indicated that the PDF of the May 2014 email was created on October 10, 2019, and that the PDF of the April 2015 email was produced on September 28, 2019.	https://www.businessinsider.com/new-york-post-hunter-joe-biden-giuliani-red-flags-disinformation-2020-10
4	Business Insider Investigations Team	Repair shop owner	The owner of the repair shop said that he wasn't sure the laptop belonged to Hunter Biden but that the machine had a sticker from the Beau Biden Foundation	https://www.businessinsider.com/new-york-post-hunter-joe-biden-giuliani-red-flags-disinformation-2020-10
5	Business Insider Investigations Team	Leaked content vs. Biden schedule	In the alleged April 2015 email, Pozharskiy thanked Hunter Biden for inviting him to Washington, DC, to meet with Joe Biden. But there's no evidence Pozharskiy actually met the former vice president. The Biden campaign said in a statement that it "reviewed Joe Biden's official schedules from the time and no meeting, as alleged by the New York Post, ever took place."	https://www.businessinsider.com/new-york-post-hunter-joe-biden-giuliani-red-flags-disinformation-2020-10
6	NY Times, NY Post, other publications	Photos, quotes, interviews	Hunter Biden moved to Los Angeles in 2018.	https://www.nytimes.com/2020/02/28/arts/design/hunter-biden-art.html
7	The Washington Post	wide variety of sources, quotes, interviews	Numerous previously-debunked theories included in NY Post article	https://www.washingtonpost.com/politics/2019/09/23/fact-checking-trumps-latest-claims-biden-ukraine/
8	NY Mag Intelligencer	metadata	Hunter Biden's "emails" were created 3 months before Rudy Giuliani was supposedly told of their existence, raising questions of who exactly created these files in the first place.	https://twitter.com/ccallahan1988/status/1316618582269276160
9	n/a	metadata	Pozharskiy's name is spelled wrong consistently in the "email" and the Metadata . Vadym Pozharskiy vs. Vadim Pozharskiy = Ukrainian vs. Russian spelling	
10	SiriusXM	Giuliani	"was left by Hunter Biden, in an inebriated, heavily inebriated state with the merchant." in contrast to the story initially told by the repair shop owner	https://twitter.com/IsaacDovere/status/1316787994414796800?s=20
11	The Daily Beast	Repair shop owner	Shop owner alleges the FBI called him for tech support and for advice on which cord to use with the laptop	https://www.thedailybeast.com/man-who-reportedly-gave-hunters-laptop-to-rudy-speaks-out-in-bizarre-interview
12	n/a	email content analysis	In the "emails," the upper right hand corner has a "VP". That would indicate the person signed in to Gmail is VP (Vadym). When you receive an email from Gmail, this does not show up. So this is the SENT version of the email. This is NOT the received version. If you	https://twitter.com/BigotedVsBigots/status/1316427768519892992?s=20

Source	Primary Sources	Intel	Relevant Links	
		print a received version of an email from Gmail on a PC, you don't even get the initials. If this was copied off of Hunters computer and he is using a company email address then Google wouldn't be the provider, but that really looks like a Google icon.		
13	n/a	email content analysis	Also, all of this is based upon someone taking a hard drive out of a computer and putting it into another computer. This would mean they were able to get a PST or OST file, meaning it would not be gmail, which is cloud-based. As we are seeing Gmail, this has to be fake.	https://twitter.com/amadeov/status/1316449438416744450?s=20
14	n/a	email content analysis	some content analysis indicates that the gmail icon is a different resolution than the rest of the text -- analysis shows how these emails would look normally	https://eddiekrassenstein.medium.com/alleged-hunter-biden-email-from-giuliani-appears-forged-2d55b08140cc
15	The Washington Post	email content analysis	An Eastern European expert in digital forensics who has examined some of the Ukrainian documents leaked to the New York Post told me he found anomalies — such as American-style capitalization of the names of ministries — that suggest fakery.	https://www.washingtonpost.com/opinions/the-truth-behind-the-hunter-biden-non-scandal/2020/10/16/798210bc-0fd1-11eb-8074-0e943a91bf08_story.html
16	TechCrunch	Analysis	The serial number of the laptop suggests it was a 2017 MacBook Pro, probably running Mojave. Every Mac running Lion or later has easily enabled built-in encryption. It would be unusual for anyone to provide a laptop for repair that had no password or protection whatsoever on its files.	https://techcrunch.com/2020/10/14/suspect-provenance-of-hunter-biden-data-cache-prompts-skepticism-and-social-media-bans/
17	Dustin Miller, data engineer	alleged repair shop documents	Does show the laptop was dropped on Apr 12, 2019. They also show an external drive and its serial number. Western Digital's web site says that drive's **3-year** warranty expires Apr 18, 2022...meaning it was manufactured Apr *18*, 2019.	https://twitter.com/spdustin/status/1316621229751762945?s=21
18	Mediaite	two sources familiar with the matter	Fox News passed on this story over credibility concerns. according to two sources familiar with the matter, the lack of authentication of Hunter Biden's alleged laptop, combined with established concerns about Giuliani as a reliable source and his desire for unvetted publication, led the network's news division to pass.	https://www.mediaite.com/tv/exclusive-fox-news-passed-on-hunter-biden-laptop-story-over-credibility-concerns/
19	The Daily Beast	Giuliani	Trump personal attorney Rudy Giuliani argued on Tuesday that the American public deserved to see reports based off material from <u>Hunter Biden's laptop</u> "even if it isn't accurate."	https://www.thedailybeast.com/giuliani-says-even-if-hunter-laptop-story-isnt-accurate-americans-are-entitled-to-know-it

[Contact Support](#)

Conversation History

██████████ opened your conversation with ██████████

██████████ Aug 30 at 8:03 pm

██████████ added ██████████ to the thread Aug 30 at 6:52 pm

██████████ added you to a document Aug 30 at 6:46 pm

[REDACTED] added [REDACTED] to the thread *Aug 30 at 6:42 pm*

[REDACTED] added you to a document *Aug 30 at 6:37 pm*

[REDACTED] opened your conversation with [REDACTED]

Aug 30 at 5:27 pm

[REDACTED] edited *Oct 20, 2020 at 9:35 pm*

Current Assessment (10/19/2020) (10/20/2020):

- 10/19/2020 - Low to medium confidence

[REDACTED] opened your conversation with [REDACTED]

Oct 19, 2020 at 9:21 pm

[REDACTED] added [REDACTED] to the thread *Oct 19, 2020 at 9:21 pm*

[REDACTED] added you to a document *Oct 19, 2020 at 9:16 pm*

[REDACTED] edited *Oct 19, 2020 at 9:19 pm*

(A/C PRIV) Five Factors — Hack/Leak Policy Assessment - Laptop 1

Low to Medium Confidence
Low Medium Confidence

[REDACTED] edited *Oct 19, 2020 at 5:23 pm*

Current Assessment (morning 10/16/2020) (10/19/2020):

We currently have ____ low to medium confidence that these documents and story are part of a foreign government influence operation.

Previous Assessments:

- 10/16/2020 — Low confidence

[REDACTED] edited *Oct 19, 2020 at 6:36 am*

[REDACTED] edited *Oct 19, 2020 at 4:15 am*

[REDACTED] edited *Oct 18, 2020 at 7:03 pm*

[REDACTED] opened your conversation with [REDACTED]
[REDACTED] Oct 18, 2020 at 7:02 pm

[REDACTED] edited Oct 17, 2020 at 4:41 pm

[REDACTED] opened your conversation with [REDACTED]
[REDACTED] on a phone Oct 16, 2020 at 10:52 pm

[REDACTED] edited Oct 16, 2020 at 9:27 pm

[REDACTED] opened your conversation with [REDACTED]
[REDACTED] Oct 16, 2020 at 4:49 pm

[REDACTED] opened your conversation with [REDACTED]
[REDACTED] Oct 16, 2020 at 4:48 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:44 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:43 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:43 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:43 pm

[REDACTED] opened your conversation with [REDACTED]
[REDACTED] Oct 16, 2020 at 4:43 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:42 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:42 pm

[REDACTED] added [REDACTED]
[REDACTED] to the thread Oct 16, 2020 at 4:47 pm

[REDACTED] added you to a document Oct 16, 2020 at 4:42 pm

[REDACTED] edited Oct 16, 2020 at 5:22 pm

Current Assessment (10/15/2020) (morning 10/16/2020):

[Redacted] Oct 16, 2020 at 4:31 am

that's in the next section

[Redacted] Oct 16, 2020 at 4:30 am

Parler and Gab => IRA linked assets amplifying this content (not really an industry partner, though)

[Redacted] edited Oct 16, 2020 at 4:29 am

(A/C PRIV) Five Factors — Hack/Leak Policy Assessment

[Redacted] renamed Five Factors — Hack/Leak Policy Assessment to (A/C PRIV) Five Factors — Hack/Leak Policy Assessment Oct 16, 2020 at 4:34 am

[Redacted] opened your conversation with [Redacted]
[Redacted] Oct 16, 2020 at 4:26 am

[Redacted] added you to a document Oct 16, 2020 at 4:11 am

[Redacted] added [Redacted] and [Redacted] to the thread Oct 16, 2020 at 4:16 am

[Redacted] added you to a document Oct 16, 2020 at 4:11 am

[Redacted] Oct 16, 2020 at 4:11 am

I believe the answer is currently no? [Redacted]

[Redacted] edited Oct 16, 2020 at 5:40 am

Current Assessment (10/15/2020):

We currently have _____ confidence that these documents and story are part of a foreign government influence operation.

Policy Language: PRIVACY VIOLATIONS & IMAGE PRIVACY - On Escalation Only Policy:

OFF PLATFORM FACTORS

Low to Medium Confidence?

Source	B	Primary Sources
--------	---	-----------------

Medium Confidence?

Source		
B		
Primary Sources		
Source	B	Primary Sources

[Insert Confidence] Low Confidence

Source	B	Primary Sources
Source	B	Primary Sources

opened your conversation with [REDACTED]
 [REDACTED] Oct 15, 2020 at 11:03 pm

[REDACTED] edited Oct 15, 2020 at 11:06 pm
 Policy: **PRIVACY VIOLATIONS & IMAGE PRIVACY - On Escalation Only Policy:**

- a. Remove
 - i. source material that purports to reveal nonpublic information about the US/2020 election shared as part of a foreign government influence operation (*determined by Cyber XFN*)
 - ii. reporting on such a leak by state-controlled media entities from the country behind the leak (*determined by Cyber XFN*)

opened your conversation with [REDACTED]
 [REDACTED] Oct 15, 2020 at 9:57 pm

[REDACTED] edited Oct 15, 2020 at 10:06 pm
 [Insert Confidence] Low Confidence

[REDACTED] enabled link sharing · View/Edit Oct 15, 2020 at 8:45 pm

[REDACTED] edited Oct 15, 2020 at 9:20 pm

Five Factors — Hack/Leak Policy Assessment

1. Do we believe that the actor responsible for the leak is directed by a foreign gov't? (we will presume that a US government actor does *not* meet this factor)

OFF PLATFORM

Medium Confidence?

A	Source
B	Intel
C	Relevant Links

2. Do we believe that the leak is part of a foreign influence operation to manipulate the election? (with sufficiently strong consensus, this factor could necessitate action on a release from a US government actor)

Medium Confidence?

A	Source
---	--------

	Source
B	
	Intel
C	
	Relevant Links

ON-PLATFORM/BEHAVIORAL FACTORS

3. Do we or our industry partners see on-platform evidence of deception by the assets engaged in sharing the leaked material?

[Insert Confidence]

A	
	Source
B	
	Intel
C	
	Relevant Links

4. Are there links to or amplification by known foreign government espionage or IO threat actors?

[Insert Confidence]

A	
	Source
B	
	Intel
C	
	Relevant Links

CONTENT FACTORS

5. Do we or other experts have clear evidence that the source documents are manipulated to facilitate the narrative of an influence operation?

[Insert Confidence]

A	
	Source
B	
	Intel
C	
	Relevant Links

██████████ created the document Oct 15, 2020 at 8:40 pm

Exhibit 103

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]AB9>
To: [REDACTED]; [REDACTED]; [REDACTED]
Sent: 10/14/2020 9:36:03 AM
Subject: Message summary [{"otherUserFbld":null,"threadFbld":3504708586263336}]

[REDACTED] (10/14/2020 09:16:22 PDT):

> [REDACTED] -- I am sure you're tracking the NY Post story. While there are other ongoing fact checking escalations and other things going on to verify it, wondering if there's anything we can do on our end to see if it's being amplified or originating in some way from foreign actors, etc? I know it's probably doubtful that we'll have any evidence there, but figured I'd check in anyways

[REDACTED] (10/14/2020 09:29:44 PDT):

> [REDACTED] is starting to look at first posters. I would wait for their analysis before activating our hack/leak playbook.

[REDACTED] (10/14/2020 09:30:07 PDT):

>Got it! thanks 😊

[REDACTED] (10/14/2020 09:32:42 PDT):

>We also have a call with LE today and will try to get a sense from them

[REDACTED] (10/14/2020 09:34:40 PDT):

>do you think we'll get much from fbi?

[REDACTED] (10/14/2020 09:35:02 PDT):

>I think we should be on the record asking the question

[REDACTED] (10/14/2020 09:35:37 PDT):

>agree

[REDACTED] (10/14/2020 09:35:50 PDT):

>Doubt we will get much, but helpful if they say they don't have any information to support foreign direction

[REDACTED] (10/14/2020 09:36:03 PDT):

>Then we can at least use that as a data point

Exhibit 104

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=36DD561D704D4D8FBA964A7B8425D21C>
To: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Sent: 10/14/2020 8:02:54 AM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]

[REDACTED] (10/14/2020 06:06:09 PDT):
> [REDACTED] Can we check with FBI Delaware if they have anything in this:
<https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 06:06:40 PDT):
>Article claims that FBI has had the HDD since December.

[REDACTED] (10/14/2020 06:07:03 PDT):
>This has been escalated in the various election channels

[REDACTED] (10/14/2020 06:07:46 PDT):
>Cyber law ([REDACTED]) might also know about this and be in contact with FBI on it.

[REDACTED] (10/14/2020 06:07:53 PDT):
>I'll call them this morning. Is the questions just about any relation to FB or IG in terms of any stolen content?

[REDACTED] (10/14/2020 06:08:19 PDT):
>Yep, I think they is the proper scope.

[REDACTED] (10/14/2020 06:08:25 PDT):
>*that

[REDACTED] (10/14/2020 06:08:32 PDT):
>OK

[REDACTED] (10/14/2020 06:09:45 PDT):
> [REDACTED] says he asked [REDACTED] to ping FITF about this as well.

[REDACTED] (10/14/2020 06:14:26 PDT):
> [REDACTED] is not in touch with the FBI on this. I'll connect with Maryland and [REDACTED] will raise at the FITF meeting today.

[REDACTED] (10/14/2020 08:02:54 PDT):
>Thanks all for your work today in the meeting, amazing job. We've got so much going on and we truly packed ten pounds of shit into a 5 pound bag in that meeting. Thanks again so much for your prep and delivery.

Exhibit 105

Message

From: [REDACTED]@fb.com]
 Sent: 10/14/2020 9:36:53 PM
 To: [REDACTED]@fb.com]; [REDACTED]@fb.com]
 Subject: Message summary [{"otherUserFbId": [REDACTED], "threadFbId": null}]

[REDACTED] (10/14/2020 17:53:38 PDT):
 ><https://www.platformer.news/p/the-platforms-spy-a-hack-and-leak>

[REDACTED] (10/14/2020 17:53:43 PDT):
 >Quite a piece from Casey Newton.

[REDACTED] (10/14/2020 17:54:26 PDT):
 >We should workshop what I'm going to say tomorrow about our actions here. [REDACTED] and I are on with CBS at 8 am pst, exactly when you all will be meeting to assess next steps.

[REDACTED] (10/14/2020 19:53:51 PDT):
 >Also, Ben Smith wants to write for Monday if we can give him something

[REDACTED] (10/14/2020 19:53:57 PDT):
 >Let's talk early?

[REDACTED] (10/14/2020 19:55:14 PDT):
 >Do you think we can hold the line on the demotions and start applying them consistently?

[REDACTED] (10/14/2020 19:58:13 PDT):
 >God I hope so

[REDACTED] (10/14/2020 19:59:11 PDT):
 >how can I help?

[REDACTED] (10/14/2020 19:59:18 PDT):
 >this is so important.

[REDACTED] (10/14/2020 20:08:57 PDT):
 >Just speak up is all. Back channel where possible!

[REDACTED] (10/14/2020 20:09:16 PDT):
 >If I can help, get me into the meetings and I will :)

[REDACTED] (10/14/2020 20:09:54 PDT):
 >I promise I will!

[REDACTED] (10/14/2020 20:09:57 PDT):
 >In case it's helpful, here's my pitch:

[REDACTED] (10/14/2020 20:09:58 PDT):
 >Fwiw, demotion is an appropriate and effective mitigation for what we're almost certainly observing here. We're slowing it down so that the researchers can take time to validate and peel through the layers around the release.

>You sent

>53 minutes ago

>And something that was striking today (which will almost certainly get lost until the history of this gets written) is that the media largely followed our lead.

>You sent

>53 minutes ago

>NyT, WAPO, WSJ, all the major outlets.

>You sent

>52 minutes ago

>They heard all the warnings that have been coming out from us and gov't and others for the past several weeks. This didn't get blindly amplified by them in the way we've seen in the past.

>You sent

>51 minutes ago

>We're starting to see coverage now that is digging into what's true and what isn't, the suspicious elements of the release, etc.

>You sent

>50 minutes ago

>As stop-start as it's felt, it's the best response I've seen to an effort like this. And that includes the long list of historical examples that back up these campaigns.

>You sent

>49 minutes ago

>If we can be consistent and maintain / apply demotions to the violating content tomorrow, and watch how the coverage develops, we can actually walk the line between enabling the actual discussion and giving a bit of space for the investigators to work.

>You sent

>47 minutes ago

>And interestingly, the I think the demotions are landing better for us than Twitter -- I'm seeing criticism of Twitter for inconsistent application of their labels. I'm sure we'd do the same thing if we were labelling. But the fact that we're demoting hasn't given the media the opportunity to attack us like that.

[REDACTED] (10/14/2020 20:10:58 PDT):

>Totally agree with this and was same sentiment of reporters I've spoken with

[REDACTED] (10/14/2020 20:11:23 PDT):

>Seriously. We did something amazing today. And there are a bunch of reporters pinging me who want to tell the story.

[REDACTED] (10/14/2020 20:11:54 PDT):

>If we can hold the line, we can make this a big deal.

[REDACTED] (10/14/2020 20:22:53 PDT):

>Let me know if there's anyone in particular I should work on.

[REDACTED] (10/14/2020 20:52:02 PDT):

>Nick is a key stakeholder of course. Unsure where he'll land tomorrow - but we'll see

[REDACTED] (10/14/2020 20:52:56 PDT):

>Think I should drop my narrative above to him?

[REDACTED] (10/14/2020 20:53:01 PDT):

>Or will that be too on the nose for him?

[REDACTED] (10/14/2020 21:36:12 PDT):

>Prob too on the nose

[REDACTED] (10/14/2020 21:36:28 PDT):

>fair enough. I will be patient then :).

[REDACTED] (10/14/2020 21:36:53 PDT):

>I'll just get the IB reporting leadership email sent instead. You should see it in your inbox shortly.

Produced to HJC

Exhibit 106

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=07C2A306A49548F09A173D2C18EE4171>
To: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
Sent: 10/14/2020 11:21:24 AM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]

[REDACTED] (10/14/2020 10:33:29 PDT):

>Starting a small side-thread about reshare friction preparedness. Specifically if we get signal from the FBI about the Post article being part of a foreign influence op-- and leadership approves putting reshare friction in place per the agreed upon playbook-- how quickly can we execute on that?

[REDACTED] (10/14/2020 10:33:41 PDT):

>I think [REDACTED] was chasing that down

[REDACTED] (10/14/2020 10:33:48 PDT):

>But starting this thread to make sure we're all on the same page

[REDACTED] (10/14/2020 10:34:53 PDT):

>To my knowledge, reshare friction is not part of the agreed upon playbook for hack/leak
>
>Leadership decided not to prioritize it

[REDACTED] (10/14/2020 10:35:49 PDT):

>(But certainly would be great to be prepared if minds change!)

[REDACTED] (10/14/2020 10:38:41 PDT):

>(I'm basing my knowledge on the email thread "[Feedback requested] - Hack/Leak inform product options" that ended with [REDACTED]'s message of Sept. 30.)

[REDACTED] (10/14/2020 10:41:04 PDT):

>From [REDACTED] on separate thread: "Update from the FBI FITF call: The FBI has no information indicating foreign sponsorship, direction, or coordination of the hunter laptop issue."

[REDACTED] (10/14/2020 10:49:42 PDT):

>yes don't think we need to do anything here right now

[REDACTED] (10/14/2020 11:21:01 PDT):

>Okay great, thanks for closing the loop on this one. Just wanted to make sure we weren't dropping any balls on the product side!

[REDACTED] (10/14/2020 11:21:24 PDT):

>P.S. It is times like this I wish the counterspeech work was further along-- would be a really great lever in this situation.

Exhibit 107

Message

From: [REDACTED] [/O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]@fb.com] [REDACTED]@fb.com]
Sent: 10/14/2020 11:31:07 AM
To: [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbld":null,"threadFbld":3367245176667888}]
Attachments: 121491829_371166310698351_3629829665426730756_n.png; 56745567_540643336468266_8473293021226467328_n.gif

[REDACTED] (10/14/2020 07:35:46 PDT):
 >Hey, [REDACTED], another nudge on [REDACTED] Sonderby

[REDACTED] (10/14/2020 07:42:38 PDT):
 >Hey! I havent responded yet [REDACTED]

[REDACTED] (10/14/2020 07:42:39 PDT):
 > [REDACTED]

[REDACTED] (10/14/2020 07:43:43 PDT):
 > [REDACTED]

[REDACTED] (10/14/2020 07:43:57 PDT):
 > [REDACTED]

[REDACTED] (10/14/2020 07:44:31 PDT):
 >yep!

[REDACTED] (10/14/2020 07:47:00 PDT):
 >♥

[REDACTED] (10/14/2020 07:47:02 PDT):
 >You're the best, ty

[REDACTED] (10/14/2020 07:47:20 PDT):
 >not really, I have been delayed

[REDACTED] (10/14/2020 07:47:40 PDT):
 >And I am sooo, soo sorry, I was pulled into two election related things

[REDACTED] (10/14/2020 07:47:45 PDT):
 >I said best, not remarkable 😊

[REDACTED] (10/14/2020 07:48:00 PDT):
 >re helping check for admins of candidate grps havent been compromised, bc umm we havent done that of course

[REDACTED] (10/14/2020 07:48:18 PDT):
 >I was reading the NY Post story this morning

[REDACTED] (10/14/2020 07:48:24 PDT):
 >We basically have a version of the Ads Inc fact pattern

[REDACTED] (10/14/2020 07:48:36 PDT):
 >what NY post story?!

[REDACTED] (10/14/2020 07:48:46 PDT):
 >You honestly dont want to read it

[REDACTED] (10/14/2020 07:48:58 PDT):
 ><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 07:49:08 PDT):
 > [REDACTED]

shared: 121491829_371166310698351_3629829665426730756_n.png

[REDACTED] (10/14/2020 07:50:44 PDT):
 >You should have heard my conversation with FBI about the story this morning. :(

[REDACTED] (10/14/2020 07:51:01 PDT):
>Do they think there's something there?

[REDACTED] (10/14/2020 07:51:22 PDT):
>The story is rather...porous

[REDACTED] [REDACTED] (10/14/2020 07:51:52 PDT):
>by candidate grps/pgs, I dont mean the official ones, I mean the 1000s that have the word biden/trump in their title whose admins could be compromised and waiting to be operationalized

[REDACTED] (10/14/2020 07:51:54 PDT):
>Uh, well, the person I spoke with (at about 8 am) who should have been all over this pulled the story up as we spoke. I was his tip.

[REDACTED] [REDACTED] (10/14/2020 07:52:10 PDT):
>we started analysis on spanish speaking grps and grps/pg targeting battleground states

[REDACTED] (10/14/2020 07:52:21 PDT):
>Even my and Edward's groups?

[REDACTED] (10/14/2020 07:52:40 PDT):
>wait, there are battleground states?

[REDACTED] (10/14/2020 07:52:48 PDT):
>Who is battling there?

[REDACTED] (10/14/2020 07:52:51 PDT):
>Is DC one of them?

[REDACTED] (10/14/2020 07:52:53 PDT):
>And what weapons are they using?

[REDACTED] (10/14/2020 07:53:00 PDT):
>According to the Trump Campaign

[REDACTED] (10/14/2020 07:53:05 PDT):
>they spent \$1.6m in ads!

[REDACTED] (10/14/2020 07:53:41 PDT):

shared: 56745567_540643336468266_8473293021226467328_n.gif

[REDACTED] (10/14/2020 07:53:55 PDT):
>Interesting given the story claims the FBI executed a search warrant last December

[REDACTED] (10/14/2020 07:54:02 PDT):
>This was such a great toy

[REDACTED] (10/14/2020 07:54:15 PDT):
>Right, tracking that down, too.

[REDACTED] [REDACTED] (10/14/2020 07:54:32 PDT):
>Hey! Yep, on Sept 24th [REDACTED] held the Acct Sec XFN mtg, where [REDACTED] -- MediaOps (APAC -- Singapore) presented on protections for CVAs and 2FA being main mitigating factor. I asked if CVAs had also been reviewed for cookie compromise and the answer was no (she paused so i dont think she even understood what I was asking so I rephrased my ques). Then the next day AI reviewed tier 1 and tier 2 CVAs for cookie compromise. And I met with i3 Espionage to help them query for cookie compromise and compromise at large. I ran last week one of the HnH tracks on the admins of pgs/grps as described above

[REDACTED] (10/14/2020 07:54:33 PDT):
>I was on a call yesterday with MSFT

[REDACTED] (10/14/2020 07:54:53 PDT):
>And got rather disheartening news if I read in-between the lines

[REDACTED] [REDACTED] (10/14/2020 07:55:33 PDT):
>is this the Oct surprise everyone was waiting for?

[REDACTED] (10/14/2020 07:55:42 PDT):
>If the person wasn't just offering my conjecture, and I'm appropriately reading what they were really saying, they expect Trickbot to launch on Election Day/Night and screw up the tallies (but not change vote totals) to throw/delay the election announcement

[REDACTED] (10/14/2020 07:56:04 PDT):
>offering conjecture*

[REDACTED] (10/14/2020 07:56:07 PDT):

>No, this is fairly taim

[REDACTED] (10/14/2020 07:56:09 PDT):
>tame

[REDACTED] (10/14/2020 07:56:28 PDT):
>About what and who did you meet with?

[REDACTED] (10/14/2020 07:56:54 PDT):
>MSFT's Cyber & Democracy atty

[REDACTED] (10/14/2020 07:56:59 PDT):
>I led Trickbot work for years at the FBI, including right before 2018 election

[REDACTED] (10/14/2020 07:57:04 PDT):
>Person I've been negotiating the ISA with

[REDACTED] (10/14/2020 07:57:17 PDT):
>if you want an unclassified downlow of the threat, happy to key you in

[REDACTED] (10/14/2020 07:57:24 PDT):
>Do you feel like 1/ they understand cookie compromise now and 2/ we are in a good place vis-a-vis the election?

[REDACTED] (10/14/2020 07:57:41 PDT):
>This convo is AC priv, right?

[REDACTED] (10/14/2020 07:57:44 PDT):
>Yes, please.

[REDACTED] (10/14/2020 07:57:45 PDT):
>yes

[REDACTED] (10/14/2020 07:57:51 PDT):
>+2

[REDACTED] (10/14/2020 07:57:55 PDT):
>I went over this with [REDACTED] yesterday

[REDACTED] (10/14/2020 07:57:57 PDT):
>See the title

[REDACTED] (10/14/2020 07:58:19 PDT):
>I think it'll be way quicker over a call

[REDACTED] (10/14/2020 07:58:35 PDT):
>I technically have a 4 hr small HNH in 30 min but can do later today or tomorrow morning

[REDACTED] (10/14/2020 07:58:36 PDT):
>Oh, wait, [REDACTED], is that meeting still happening today and did I get [REDACTED]'s blessing?

[REDACTED] (10/14/2020 07:58:49 PDT):
>I'll find us 3 time

[REDACTED] (10/14/2020 07:58:59 PDT):
>Yes and no.

[REDACTED] (10/14/2020 07:59:02 PDT):
>:(

[REDACTED] (10/14/2020 07:59:20 PDT):
>That's ok

[REDACTED] (10/14/2020 07:59:24 PDT):
>He'll one day want something from me

[REDACTED] (10/14/2020 07:59:41 PDT):
>We have "too large a footprint"

[REDACTED] (10/14/2020 07:59:49 PDT):
>So, in my honest opinion, esp after the various mtgs with sister teams, I do not think we have done basic due diligence to account for other vectors that could be operationalized, esp for the non CVAS

[REDACTED] (10/14/2020 07:59:53 PDT):
>Isn't it just you from our team on that call?

[REDACTED] (10/14/2020 07:59:58 PDT):
>And doesnt he have like this entire team on it?

[REDACTED] (10/14/2020 08:00:24 PDT):
>Who do you include in the non-CVAs?

[REDACTED] (10/14/2020 08:00:31 PDT):
>for example, admins of all the pgs and grps that CVAs admin have not been reviewed for compromise. okay, a cva may be difficult. but you can have the same effect by popping one of the other admins on the pgs/grps they admin

[REDACTED] (10/14/2020 08:00:32 PDT):
>And why are they risky?

[REDACTED] (10/14/2020 08:00:49 PDT):
>there are over 100k trump pgs and grps that target the spanish population

[REDACTED] (10/14/2020 08:00:50 PDT):
>Uh, yeah.

[REDACTED] (10/14/2020 08:01:02 PDT):
>Ay caramba!

[REDACTED] (10/14/2020 08:01:20 PDT):
>whent he spanish vote matters, we need to also look at high volume grps/pgs that nation state actors could still use to seed misinfo

[REDACTED] (10/14/2020 08:01:39 PDT):
>i think espionage is doing this now

[REDACTED] (10/14/2020 08:01:58 PDT):
>and to be honest, my jaw almost dropped during the acct sec mtg when no CVAs had been yet reviewed for cookie ocpromise

[REDACTED] (10/14/2020 08:02:14 PDT):
>like hello - there two main vectors for compromise and cookie evades 2FA

[REDACTED] (10/14/2020 08:02:32 PDT):
>[REDACTED], was your mtg with [REDACTED] at MSFT?

[REDACTED] (10/14/2020 08:02:41 PDT):
>No

[REDACTED] (10/14/2020 08:02:43 PDT):
>

[REDACTED] (10/14/2020 08:03:38 PDT):
>I like [REDACTED]

[REDACTED] (10/14/2020 08:03:39 PDT):
>Or [REDACTED], rather

[REDACTED] (10/14/2020 08:03:46 PDT):
>Yeah, she's fantastic

[REDACTED] (10/14/2020 08:04:38 PDT):
>interesting...i havent worked with her

[REDACTED] (10/14/2020 08:06:48 PDT):
>I was thinking of calling [REDACTED], who is the GM of MSFTs Digital Crimes Unit.

[REDACTED] (10/14/2020 08:06:58 PDT):
>for thoughts on Trickbot

[REDACTED] (10/14/2020 08:07:10 PDT):
>Let me get our ISA executed

[REDACTED] (10/14/2020 08:07:13 PDT):
>today

[REDACTED] (10/14/2020 08:07:17 PDT):
>i would love to jump on that

[REDACTED] (10/14/2020 08:07:22 PDT):
>Bc she just sent it back over

[REDACTED] (10/14/2020 08:07:37 PDT):
>Unless you want to have the convo outside it

[REDACTED] (10/14/2020 08:08:05 PDT):

████ worked for me at FBI and I helped her get the job at MSFT, so maybe we could get some good (better) info from her

████ (10/14/2020 08:09:05 PDT):

>Yeah, was thinking of getting a download from her. But I can see if she is willing to put together something more formal.

████ (10/14/2020 08:09:14 PDT):

-- what would we want to hear from them?

████ (10/14/2020 08:09:33 PDT):

>OK, good, because who knows how long it'll take █████ to sign

████ (10/14/2020 08:09:43 PDT):

>Sometimes she signs in 5 minutes. Sometimes it's 5 years

████ (10/14/2020 08:11:02 PDT):

>Also, FWIW, █████ will be the signatory

████ (10/14/2020 08:11:12 PDT):

>For MSFT

████ (10/14/2020 08:28:17 PDT):

>did they see any evidence in monitoring of trickbot infra of using any of the fb accts they likely would have access to due to it evolving to also being a browser stealer

████ (10/14/2020 08:28:40 PDT):

>if they gained access to any of the C2s, they would know about the above ^^

████ (10/14/2020 11:30:36 PDT):

>hey!!

████ (10/14/2020 11:31:07 PDT):

>just realized you cant see the hnh block. i'm still in our mini hnh, i just rescheduled for 4pm

Produced to HJC

Exhibit 108

██████████@s.whatsapp.net/██████████@s.whatsapp.net/System

Message chatroom: chat transcript

Chat description: none provided

Chat type WhatsApp
 Private chat no
 Transcript timezone (UTC-08:00) Pacific Time (US & Canada)
 Transcript start 2020-10-14 06:20:56
 Transcript end 2020-10-14 11:31:52
 Transcript participants 3
 Initial participants ██████████@s.whatsapp.net); ██████████@s.whatsapp.net); System Message

Timestamp	Sender	Recipients	Message text
2020-10-14 06:20:56	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	hey there
2020-10-14 06:38:22	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	Hi
2020-10-14 06:38:28	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	Just saw your note
2020-10-14 06:39:14	██████████@s.whatsapp.net)	██████████@s.whatsapp.net); System Message; ██████████@s.whatsapp.net)	Re hunter emails

Timestamp	Sender	Recipients	Message text
2020-10-14 06:44:23	[REDACTED] (s.whatsapp.net)	@s.whats [REDACTED] [REDACTED] @s.whatsa pp.net); System Message; [REDACTED] [REDACTED] @s.whatsa pp.net)	Are you on the FITF call this afternoon?
2020-10-14 06:44:59	[REDACTED] (s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); System Message; [REDACTED] [REDACTED] @s.whatsa pp.net)	i added my preference but hadn't received an invite?
2020-10-14 06:46:32	[REDACTED] (s.whatsapp.net)	@s.whats [REDACTED] [REDACTED] @s.whatsa pp.net); System Message; [REDACTED] [REDACTED] @s.whatsa pp.net)	[REDACTED] is forwarding it
2020-10-14 06:47:00	[REDACTED] (s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); System Message; [REDACTED] [REDACTED] @s.whatsa pp.net)	thank you!
2020-10-14 10:26:05	[REDACTED] (s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); System Message; [REDACTED] [REDACTED] @s.whatsa pp.net)	Weird criminal had the laptop since dec 2019 w explosive Biden related material from a repairman in DE who can't identify the person who dropped off the laptop and never told FITF or anyone on natl security side
2020-10-14 10:27:29	[REDACTED] (s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); System Message; [REDACTED] [REDACTED] @s.whatsa pp.net)	And weird it's dropped off for a cost of \$85 and no one comes to pick it up and then repairman thinks of making a copy and sending to Giuliani's attorney before he turns it over to the Bu

Timestamp	Sender	Recipients	Message text
2020-10-14 10:32:43	[REDACTED] (app.net)	@s.whats [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Oh yeah def weird
2020-10-14 10:33:10	[REDACTED] (app.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	I wonder if it's criminal because it's some GOP discrediting op
2020-10-14 10:33:30	[REDACTED] (s.whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Or a ransom type thing?
2020-10-14 10:33:37	[REDACTED] (app.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Maybe
2020-10-14 10:34:48	[REDACTED] (s.whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	But either way hard to imagine all of the impeachment stuff going on in dec that this didn't make it's way to fit or at least national security side
2020-10-14 10:37:32	[REDACTED] (s.whatsapp.net)	@s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	The repairman got into the hard drive and reviewed it (and then made a copy) so he knew it had compromising info ... so the Bu couldn't say it sat for a year as they weren't aware of what was in it

Timestamp	Sender	Recipients	Message text
2020-10-14 10:38:22	[REDACTED] s.whatsapp.net)	@ [REDACTED] [REDACTED] @s.whatsa pp.net); Sy stem Mess age: [REDACTED] [REDACTED] @s.whatsa pp.net)	Could be but still would think national security side of the house would know
2020-10-14 10:40:22	[REDACTED] s.whatsapp.net)	@ [REDACTED] [REDACTED] @s.whatsa pp.net); Sy stem Mess age: [REDACTED] [REDACTED] @s.whatsa pp.net)	If Biden made the billions he reportedly made from Ukraine you'd think he could afford hiring a "cleared" IT guy for sensitive stuff ... particularly knowing his dad had been running for president since summer 2019
2020-10-14 10:47:24	[REDACTED] @s.whats app.net)	[REDACTED] [REDACTED] @s.whatsa pp.net); Sy stem Mess age: [REDACTED] [REDACTED] @s.whatsa pp.net)	It's all very fishy
2020-10-14 10:47:57	[REDACTED] s.whatsapp.net)	@ [REDACTED] [REDACTED] @s.whatsa pp.net); Sy stem Mess age: [REDACTED] [REDACTED] @s.whatsa pp.net)	But concerning the Bu criminal seemingly knowledgeable of it
2020-10-14 10:48:24	[REDACTED] @s.whats s.whatsapp.net)	[REDACTED] [REDACTED] @s.whatsa pp.net); Sy stem Mess age: [REDACTED] [REDACTED] @s.whatsa pp.net)	Unless of course it was a ICE or DHS subpoena in actuality?
2020-10-14 10:48:42	[REDACTED] @s.whats app.net)	[REDACTED] [REDACTED] @s.whatsa pp.net); Sy stem Mess age: [REDACTED] [REDACTED] @s.whatsa pp.net)	They did say Bu crim

Timestamp	Sender	Recipients	Message text
2020-10-14 10:48:50	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	I guess it'll play out
2020-10-14 10:49:26	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Bu crim guy said he could confirm such a laptop existed is what he said?
2020-10-14 10:49:48	[REDACTED] app.net)	@s.whats pp.net)	I thought he said it was a criminal matter on the Bu crim side
2020-10-14 10:49:56	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Hmm
2020-10-14 10:50:06	[REDACTED] app.net)	@s.whats pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	That's not what you heard?
2020-10-14 10:50:09	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	I noted he said he was from crim

Timestamp	Sender	Recipients	Message text
2020-10-14 10:50:22	[REDACTED] (s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	And I thought he said he could confirm it existed
2020-10-14 10:50:40	[REDACTED] (s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	I distinctly remember he said it was a crim matter
2020-10-14 10:51:11	[REDACTED] (s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	I do distinctly remember he said he was from crim but not that it was an fbi crim matter
2020-10-14 10:51:28	[REDACTED] (s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	Likely neither here nor there as it will play out in some way soon
2020-10-14 10:51:39	[REDACTED] (s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	So I prob assumed he meant on the Bu side vs ICE
2020-10-14 10:52:36	[REDACTED] (s.whatsapp.net)	[REDACTED] (@s.whatsapp.net); System Message; [REDACTED] (@s.whatsapp.net)	You may be right as to what he said ... I can't confirm I heard the part that the laptop was part of a Bu crim matter ... but he may hv well said it ... I'd

Timestamp	Sender	Recipients	Message text
2020-10-14 10:53:49	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	If it's Russians now they hv fbi implicated so Wray likely will need to say som ething
2020-10-14 10:54:50	[REDACTED] app.net)	@s.whats pp.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Feels so ham handed
2020-10-14 10:55:07	[REDACTED] app.net)	@s.whats pp.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	That I'd bet it's some GOP operative like Jacob Wohl
2020-10-14 10:55:55	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Could very well be
2020-10-14 10:57:13	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Which is why it might've started criminal ... but supposedly the repairman sp oke to the senate committee for homeland security on 05 oct 2020 ...
2020-10-14 10:57:48	[REDACTED] app.net)	@s.whats pp.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Yeah...

Timestamp	Sender	Recipients	Message text
2020-10-14 10:57:50	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Somehow the laptop should hv surfaced to the national security folks at bure au before today
2020-10-14 10:57:59	[REDACTED] app.net)	@s.whats pp.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	They seemed clueless
2020-10-14 10:58:14	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Really seemed genuine about that
2020-10-14 11:05:46	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	From [REDACTED]; You can read Joshua Wilson very clearly on here, which go es back (though it is a very common name obviously, so possibly multiple [REDACTED] [REDACTED] in the FBI) to an east coast FBI agent who exclusively works chil d exploitation cases, as of a couple years ago. Seems really QAnon-y.
2020-10-14 11:06:18	[REDACTED] app.net)	@s.whats pp.net) @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Yes I saw [REDACTED] flagged it too
2020-10-14 11:06:22	[REDACTED] s.whatsapp.net)	@ [REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	[REDACTED] name can be seen (maybe purposefully) in the photo in the ar ticle

Timestamp	Sender	Recipients	Message text
2020-10-14 11:06:38	[REDACTED] s.whatsapp.net)	[REDACTED] @s.whatsa pp.net); Sy stem Mess age; Susan Mitchell ([REDACTED]) @s.whatsa pp.net)	So it was an fbi warrant
2020-10-14 11:06:53	[REDACTED] app.net)	[REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Right
2020-10-14 11:07:06	[REDACTED] s.whatsapp.net)	[REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	The story does claim that 12min video exists
2020-10-14 11:31:40	[REDACTED] s.whatsapp.net)	[REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Maybe ham handed but now makes everyone look partisan
2020-10-14 11:31:52	[REDACTED] s.whatsapp.net)	[REDACTED] @s.whatsa pp.net); Sy stem Mess age; [REDACTED] @s.whatsa pp.net)	Fbi, Facebook

Nickname	Name	Surname	E-mail	Source PID	Type
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	User
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	User
System Message	System Message			[REDACTED]	User

Exhibit 109

Message

From: [REDACTED]@fb.com]
Sent: 10/14/2020 10:41:27 AM
To: [REDACTED]@fb.com]; [REDACTED]@fb.com]
Subject: Message summary [{"otherUserFbld": [REDACTED], "threadFbld": null}]

[REDACTED] (10/14/2020 10:11:59 PDT):
>What time is your FBI FITF meeting? And do you think they'd be able/willing to give us a signal on potential foreign origin of the NY Post article?

[REDACTED] (10/14/2020 10:14:55 PDT):
>its now.

[REDACTED] (10/14/2020 10:15:31 PDT):
>I'm skeptical that they'd tell us but we are going to ask

[REDACTED] (10/14/2020 10:19:43 PDT):
>please do -- would have huge implications on our next steps (e.g., whether to implement reshare friction)

[REDACTED] (10/14/2020 10:41:27 PDT):
>Just shared in the US2020 group but the Bureau has no information indicating foreign sponsorship, direction, or coordination of the hunter laptop issue.

Produced to HJC

Exhibit 110

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=09460C2DD67F442FB8CAA630918519A9>
 To: [REDACTED]
 Sent: 10/18/2020 11:50:55 AM
 Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]
 Attachments: 21730664_1385146588259970_2054126430672912384_n.gif; sticker.png

[REDACTED] (10/18/2020 09:32:39 PDT):

>Derkach is claiming there is a second laptop (on FB) <https://www.thedailybeast.com/rudys-russian-agent-pal-teases-second-laptop-with-hunter-biden-kompromat>

[REDACTED] (10/18/2020 09:32:56 PDT):

> [REDACTED] greenlit the escalation. I'm going to send this morning.

[REDACTED] (10/18/2020 09:58:12 PDT):

>Given that we've been warned about Derkach by LE, plus this statement by him, I would recommend upgrading our confidence assessment about foreign involvement. It's not clear which parts might be seeded/promoted by RU vs aligned amplification, but I think we're on solid ground saying at least some of the narrative is likely attributable to foreign gov

[REDACTED] (10/18/2020 10:11:11 PDT):

>do we think we are close to making the case for foreign gov links to warrant the new hack/leak policy kicking in?

[REDACTED] (10/18/2020 10:13:22 PDT):

>Depends on what confidence level leadership is comfortable with. We don't have independent confirmation yet, everything is circumstantial and based on LE and media reporting. I'd defer to the policy folks on the level needed.

[REDACTED] (10/18/2020 10:15:29 PDT):

>Agree. We don't want to be too far out ahead on this without leadership approval

[REDACTED] (10/18/2020 10:20:07 PDT):

>Hi, was trying to sneak in my sons hockey game a 5-1 win might I proudly say.

[REDACTED] (10/18/2020 10:20:32 PDT):

>Did he let the one goal in?

[REDACTED] (10/18/2020 10:20:50 PDT):

>Who has the pen on alerting leadership on this. I'm IMOC so happy to push it.

[REDACTED] (10/18/2020 10:21:47 PDT):

>Hah! Yes just one today. He was not completely going to break the other team's spirit 😊

[REDACTED] (10/18/2020 10:23:26 PDT):

> [REDACTED] I can update the sitrep/SEV. My sense is we should flip our assessment for "Foreign direction/sponsorship of the leak" from "NO" to "YES" with low confidence.

[REDACTED] (10/18/2020 10:26:43 PDT):

>Will do.

[REDACTED] (10/18/2020 10:29:20 PDT):

>I'm thinking we should probably also flag in the right small leadership chat as well but lmk if other think similarly

[REDACTED] (10/18/2020 10:30:20 PDT):

>ERE mid day ipoc update call

[REDACTED] (10/18/2020 10:43:14 PDT):

>Hey all

[REDACTED] (10/18/2020 10:43:24 PDT):

>Let's bump this to the WA thread with [REDACTED]

[REDACTED] (10/18/2020 11:04:27 PDT):

>JFYI: hearing that a source told one of our reporter friends that OAN was courting the derkach family pre pandemic. they offered his daughter a job. Now Chanel at OAN is supposedly pushing claims about porn stuff on 4chan (she then claims on twitter that it wasnt her). the journalists are speculating that this porn conspiracy may be coming from derkach's 2nd laptop

[REDACTED] (10/18/2020 11:04:44 PDT):

><https://mobile.twitter.com/chanelrion/status/1317128040577683463>

[REDACTED] (10/18/2020 11:05:49 PDT):

>I just connected with [REDACTED] at FITF. They're assessment is consistent - they're still not aware of any evidence linking the first laptop (Delaware IT shop) to gov interference. At this point this assessment has not changed, they have nothing to point to re foreign gov connection. Re the allegation of the existence of the second laptop by Derkach, [REDACTED] recommended treating that separately (basically two aligned narratives), and agrees Derkach's statement should be looked at with suspicious of foreign gov involvement, given Derkach's history and the fact he is sanctioned by Treasury. I'll update the SitRep with this info now.

[REDACTED] (10/18/2020 11:09:48 PDT):

[REDACTED] (10/18/2020 11:09:06 PDT):

>interesting story from june on this OAN angle

[REDACTED] (10/18/2020 11:24:47 PDT):

>Hey all - can we use the WA thread we set up for this?

[REDACTED] (10/18/2020 11:25:04 PDT):

>Trying to keep us in one place with our other colleagues as well to minimize telephone risks..

[REDACTED] (10/18/2020 11:25:24 PDT):

shared: sticker.png

[REDACTED] (10/18/2020 11:46:47 PDT):

> [REDACTED] and [REDACTED] can one of you add me to the 12 / 3 pm meeting?

[REDACTED] (10/18/2020 11:49:43 PDT):

>Oh. You should already be on it

[REDACTED] (10/18/2020 11:50:17 PDT):

>You must have added [REDACTED]

[REDACTED] (10/18/2020 11:50:33 PDT):

>Ah fixed

[REDACTED] (10/18/2020 11:50:41 PDT):

>I get you two confused all the time

[REDACTED] (10/18/2020 11:50:55 PDT):

shared: 21730664_1385146588259970_2054126430672912384_n.gif

Exhibit 111

From: [REDACTED] h </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]A86>
To: [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]; [REDACTED]
CC: [REDACTED]
Sent: 10/14/2020 11:28:46 AM
Subject: Current fact pattern re: alleged Hunter Biden laptop

Hi folks - @ [REDACTED] pulled together the below fact pattern based on open sources and our conversations with the FBI today. We'll keep updating this in the Quip here: <https://fb.quip.com/oslqApMaCO1M>. The **bolded** portion below (8-10) are the most compelling argument that the communications were obtained without consent.

1. FBI confirmed that they have one or more laptops in their custody
2. It was allegedly dropped off at a repair shop in Delaware
3. No evidence that this is Hunter Biden's laptop save some stickers
4. Shop owner allegedly did not know who dropped it off, but then produced a receipt for Hunter Biden
5. The shop owner allegedly alerted the FBI to the existence of the laptop
6. The shop owner allegedly made copied of the contents of the computer for Rudy Giuliani's lawyer (this likely violates the shop owner's responsibility to safeguard this private data)
7. The grand jury subpoena for the laptop does not connect the laptop to Hunter Biden
8. **These are private communications that - if authentic - belong to the person who owns the laptop**
9. **The repair guy disclosed those communications to third parties without approval of the story (his own claims)**
10. **Those communications were further disseminated by individuals also without approval of the owner (their own claims)**
11. The disinfo research community is broadly concerned that this pattern of dissemination (seed compromising and possibly forged material with an ideologically aligned cutout, then get that information published in a less-than-reputable press outlet)
12. The content from the laptop itself is unverified and exists in image form. Some analysts have alleged there may be evidence of photoshop or manipulation, including image file metadata showing it was processed in photoshop before being turned into an image file.

Exhibit 112

Message

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov]
Sent: 1/3/2020 11:45:29 PM
To: [REDACTED]@google.com); [REDACTED]@google.com]
CC: [REDACTED]@google.com); [REDACTED]@google.com]
Subject: Next FITF Meeting

Hi [REDACTED],

Happy New Year! I know you and [REDACTED] may have some conflicts, but we wanted to gauge your team's availability to meet with FITF next month. Here are the open dates/times:

February 10, 1 PM, 3 PM
February 14, 10 AM, 1 PM

The tentative agenda will include discussion of election related crimes with DOD and an IRA update. Hope all is well.

Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security Cyber
FBI San Francisco
Work: [REDACTED]
Cell: [REDACTED]
Email: [REDACTED]

This communication contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents or attachments are not to be distributed outside your agency.

Exhibit 113

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=4F4BF629C57347A8B6DA9B5CC8B347AB>
To: [REDACTED]
Sent: 10/14/2020 7:10:45 PM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]
Attachments: 121574359_403213744400511_7118563285716987168_n.jpg; sticker.png

[REDACTED] (10/14/2020 16:18:03 PDT):

>Sounds like pictures allegedly from the laptop are starting to surface. We may have more to do tonight.

[REDACTED] (10/14/2020 16:19:26 PDT):

>The bathtub photos or different ones?

[REDACTED] (10/14/2020 16:24:35 PDT):

>A bathtub one and one with a crack pipe allegedly.

[REDACTED] (10/14/2020 16:24:49 PDT):

><https://www.dailymail.co.uk/news/article-8841255/Man-Hunter-Bidens-emails-Trump-voter-say-told-FBI-came-him.html>

[REDACTED] (10/14/2020 16:25:03 PDT):

>yeah i've seen both of those

[REDACTED] (10/14/2020 16:25:26 PDT):

>right now are we only considering "source material" for the purposes of rejecting ads to be the images of the two emails?

[REDACTED] (10/14/2020 16:25:39 PDT):

>Q: Have we had our AI red team check to see whether these videos look manipulated?

[REDACTED] (10/14/2020 16:25:49 PDT):

>Would be useful to get a signal on that if we haven't.

[REDACTED] (10/14/2020 16:26:17 PDT):

>They are actually in the NY Post story

[REDACTED] (10/14/2020 16:26:22 PDT):

><https://nypost.com/2020/10/14/email-reveals-how-hunter-biden-introduced-ukrainian-biz-man-to-dad/>

[REDACTED] (10/14/2020 16:27:34 PDT):

>I did not know that.

[REDACTED] (10/14/2020 16:27:46 PDT):

>towards the bottom there's a series of four images

[REDACTED] (10/14/2020 16:28:02 PDT):

>the bathtub one, the crackpipe one, one of hunter smoking a cigarette in bed, and one of him taking a selfie in front of a mirror

[REDACTED] (10/14/2020 16:28:06 PDT):

>they've been in the story since this morning

[REDACTED] (10/14/2020 16:28:32 PDT):

>Right, but I'm not sure whether we've actually assessed to see if we see signs of manipulation.

[REDACTED] (10/14/2020 16:28:48 PDT):

>Either way it would give us valuable context for what to expect next

[REDACTED] (10/14/2020 16:28:52 PDT):

>And photos, fwiw

[REDACTED] (10/14/2020 16:29:06 PDT):

>right -- I meant photos.

[REDACTED] (10/14/2020 16:29:36 PDT):

>i havent seen any video yet (although i've seen allegations that there is video on the hard drive of hunter smoking crack while engaging in a sex act)

[REDACTED] (10/14/2020 16:29:54 PDT):

>nod -- it's photos at this point.

[REDACTED] (10/14/2020 16:30:15 PDT):

>I can ask [REDACTED] to route this, but [REDACTED] are you guys in a place to kick this off?

[REDACTED] (10/14/2020 16:30:32 PDT):

>I don't believe anyone in the misinfo world has looked into this.

[REDACTED] (10/14/2020 16:31:06 PDT):

>I am not personally (bedtime madness) But [REDACTED] and [REDACTED] are here for [REDACTED]

[REDACTED] (10/14/2020 16:31:09 PDT):

>hey guys, i have to run and grab my kids before they sell them to the highest bidder. Back in about an hour!

[REDACTED] (10/14/2020 16:31:29 PDT):

>[REDACTED] is on call for us and can assist as needed

[REDACTED] (10/14/2020 16:31:40 PDT):

>[REDACTED] would you guys want to take this? Feels like we should be using all tools to try to get a sense of how legit / illegit this is. Will help inform leadership's decisions tomorrow and how we handle going forward.

[REDACTED] (10/14/2020 16:31:58 PDT):

>But [REDACTED] would be super helpful for [REDACTED] to kick off the right process as we don't know who to send these to for technical evaluation of manipulation

[REDACTED] (10/14/2020 16:32:33 PDT):

>We can start outreach or glad for [REDACTED] to. Our contact will be on Misinfo Product side. Not sure if there are others in [REDACTED] that [REDACTED] would loop in?

[REDACTED] (10/14/2020 16:32:40 PDT):

>Isn't MMV video?

[REDACTED] (10/14/2020 16:33:07 PDT):

>Yes that policy applies to video only. But we can ask Misinfo Product team if they have classifiers that could try to detect photo manipulation.

[REDACTED] (10/14/2020 16:33:07 PDT):

>I don't know if the AI red team can analyze photos in any structured way, but we've asked them to look before, so I think it's doable in a one-off context.

[REDACTED] (10/14/2020 16:33:11 PDT):

>I don't know if they do.

[REDACTED] (10/14/2020 16:33:33 PDT):

>ok. I'll kick a thread off to ask. This could also get tasked up in the am tomorrow.

[REDACTED] (10/14/2020 16:33:38 PDT):

>Ok. So I'd say [REDACTED] isn't the right team on this then

[REDACTED] (10/14/2020 16:33:49 PDT):

>I'll include you @ [REDACTED].

[REDACTED] (10/14/2020 16:33:52 PDT):

>Anyone else want to be on?

Final Report 1509

[REDACTED] (10/14/2020 16:34:31 PDT):
>me (he says reluctantly) :)

[REDACTED] (10/14/2020 16:34:53 PDT):
>"want"

[REDACTED] (10/14/2020 16:34:54 PDT):
>Happy to join the chat

[REDACTED] (10/14/2020 16:35:09 PDT):
>if we find a manipulated image, what policy would apply?

[REDACTED] (10/14/2020 16:35:12 PDT):
>i do not think misinfo product has classifiers to detect manipulated photos, but it's worth asking. they detect false photos based on comparison to known manipulated photos, not based on signs of manipulation in the abstract

[REDACTED] (10/14/2020 16:35:51 PDT):
>if we find a manipulated image, we would enqueue with demotion as we have already, but i'd think we could also tell 3PFCs we found evidence of that and see if they can validate it. we've never done that...but i don't see why not

[REDACTED] (10/14/2020 16:37:20 PDT):
>yeah - pictures were also in the dailymail articles this morning

[REDACTED] (10/14/2020 16:39:18 PDT):
>On this... I added to [REDACTED] SOT doc: Do not enqueue or demote any further content making claims related to this story. If we become aware of new signals of falsity, please escalate to Content Policy leadership.

[REDACTED] (10/14/2020 16:39:32 PDT):
>Given sensitivity, I'd suggest we clear with this group before demoting any content based on manipulation signals.

[REDACTED] (10/14/2020 16:39:57 PDT):
>Even though it's our policy to demote if we see evidence of manipulation, just seems we should play it safe since leadership said don't demote any more of this.

[REDACTED] (10/14/2020 16:45:54 PDT):
> [REDACTED] one question from [REDACTED] I wanted to make sure you're aligned on...They are asking whether we should enforce at the ad level or the component level? If we enforce at the component level, other ads/advertisers that use the exact tagged/rejected component will also get their ads taken down (so closer to proactive detection and automated action for new ads).

>
>However, ad level enforcement seems much more aligned with the decision above as it's on an ad by ad basis and much more reactive.

[REDACTED] (10/14/2020 16:46:53 PDT):
> [REDACTED] myself think we should go with ad level as to avoid enforcement that goes out and automatically finds other ads.

[REDACTED] (10/14/2020 16:54:02 PDT):
>considering the guidance not to do any proactive sweeps above

[REDACTED] (10/14/2020 16:54:26 PDT):
>Twitter's policy explanation for their enforcement: <https://twitter.com/TwitterSafety/status/1316525303930458115?s=20>

[REDACTED] (10/14/2020 16:57:43 PDT):
>Ad level for now.

[REDACTED] (10/14/2020 17:05:16 PDT):
>Not assuming any policy applies at this point -- mainly just trying to inform leadership's analysis of how sketchy this is and how future analysis is likely to break.

[REDACTED] (10/14/2020 17:06:32 PDT):

>Manipulated image would be for fact checkers to rate as altered (depending on the manipulation). I don't think a manipulated media violates anything on its face.

[REDACTED] (10/14/2020 17:08:06 PDT):

>Agree. Evidence that the images were manipulated could inform our assessment of how the public will react and whether we'll see additional debunking stories.

[REDACTED] (10/14/2020 17:15:38 PDT):

>Okay - leadership wants to stay the course overnight.

[REDACTED] (10/14/2020 17:16:25 PDT):

>Right -- analyzing the photos is just to see if we can get more signal for leadership for their discussion in the am.

[REDACTED] (10/14/2020 17:16:31 PDT):

>no suggestion we should take action ahead of that.

[REDACTED] (10/14/2020 17:18:30 PDT):

>But can I ask APAC and then EMEA to work with Ops to see what's out there in terms of these images and whether they're being posted by publications in the NPI and/or by other users? If we are able to identify the scale of posts containing these images, that would be really helpful.

[REDACTED] (10/14/2020 17:19:37 PDT):

>the thought here is that they are hacked and not newsworthy as they are private images of the adult child of a candidate so we would remove under our hack policy, but it would be helpful to know the scope and if we can informally gauge whether news entities think the images are newsworthy.

[REDACTED] (10/14/2020 17:28:17 PDT):

>Flagging for awareness

[REDACTED] (10/14/2020 17:28:21 PDT):

><https://www.washingtonpost.com/politics/2020/10/14/hunter-bidens-alleged-laptop-an-explainer/>

[REDACTED] (10/14/2020 17:29:59 PDT):

>Basically says none of the NY post story has been verified and that VP Biden and Hunter both deny

[REDACTED] (10/14/2020 17:32:36 PDT):

>What specifically are they denying?

[REDACTED] (10/14/2020 17:33:03 PDT):

>That laptop was Hunter Biden's? That the emails are from him? Or the underlying allegations?

[REDACTED] (10/14/2020 17:33:26 PDT):

>Andrew Bates, a Biden campaign spokesman, said a review of Biden's schedules from 2015 finds no record of any such meeting. Officials who worked for Biden at the time told The Fact Checker that no such meeting took place.>"I was with the vice president in all of his meetings on Ukraine," said Michael Carpenter, Biden's foreign policy advisor in 2015. "He never met with this guy. In fact I had never heard of this guy until the New York Post story broke."

[REDACTED] (10/14/2020 17:33:37 PDT):

>More detail in the article

[REDACTED] (10/14/2020 17:34:03 PDT):

>Asked to verify whether the email is genuine, Hunter Biden's attorney George Mesires told The Fact Checker: "We have no idea where this came from, and certainly cannot credit anything that Rudy Giuliani provided to the NY Post, but what I do know for certain is that this purported meeting never happened."

[REDACTED] (10/14/2020 17:34:23 PDT):

>Interesting,

[REDACTED] (10/14/2020 17:37:13 PDT):

>Also from the article

Final Report 1511

[REDACTED] (10/14/2020 17:37:16 PDT):

>The New York Post article also cites an email from Pozharskyi to Hunter Biden saying he was "going to share this information with the US embassy here in Kyiv, as well as the office of Mr Amos Hochstein in the States.">"I know for a fact he never contacted me or my office," said Hochstein, who at the time worked closely with Biden as Special Envoy and Coordinator for International Energy Affairs. "I provided every record to the Senate investigation and no mention of this guy was ever made, no emails, no correspondence. I know almost every player in the energy sector in Ukraine. I never met this guy.">Carpenter said that the vice president wouldn't have had a meeting with a company executive. "He was the vice president of the United States," he said. "He met with prime ministers."

[REDACTED] (10/14/2020 17:50:04 PDT):

> [REDACTED] you're asking for the prevalence of the four images of hunter right?

[REDACTED] (10/14/2020 17:50:21 PDT):

>Yep.

[REDACTED] (10/14/2020 17:53:52 PDT):

>Ops is asking the proactive pod how to determine prevalence on those images - do we have any on plat content with the images yet that we are aware of?

[REDACTED] (10/14/2020 17:54:44 PDT):

>i'm only aware of the URLs with the images embedded

[REDACTED] (10/14/2020 17:57:12 PDT):

>That's really good news actually.

[REDACTED] (10/14/2020 18:00:59 PDT):

>+ @ [REDACTED] next OCP on call

[REDACTED] (10/14/2020 18:01:40 PDT):

> [REDACTED] what about NPI publishers that post articles that contain links back to the NY Post story with the images?

[REDACTED] (10/14/2020 18:04:04 PDT):

><https://www.facebook.com/Breitbart/posts/10166338582620354>

[REDACTED] (10/14/2020 18:18:39 PDT):

>It's like some sort of MC Escher disinformation hellscape.

[REDACTED] (10/14/2020 18:19:52 PDT):

>Honestly - whatever is easy for people to categorize. I'm not trying to create huge amounts of work - just trying to get a sense of what we're seeing. If it's something we can easily detect, then by all means. But if it requires jumping through kooky hoops, not worth it.

[REDACTED] (10/14/2020 18:20:53 PDT):

> [REDACTED] due to the fact that these ads would be removed as Privacy violations under IS, these would be removed from the Ad Library altogether instead of receiving the normal overlay for less egregious violations. This proposal was approved in March under Option 1 here [REDACTED]

>

>Before we proceed, I wanted to make sure we're ok to apply this protocol and remove these ads from the Library?

[REDACTED] (10/14/2020 18:21:02 PDT):

shared: sticker.png

[REDACTED] (10/14/2020 18:21:32 PDT):

>Interesting.

[REDACTED] (10/14/2020 18:21:43 PDT):

>Sorry, the thumb got away from me.

[REDACTED] (10/14/2020 18:21:56 PDT):

>Did we ever end up with a "trace" for this situation?

[REDACTED] (10/14/2020 18:22:22 PDT):

>We were going to try to leave a record of the ad while still removing the content, but I can't remember if it happened.

[REDACTED] (10/14/2020 18:23:16 PDT):

>I believe trace work was de-pried due to COVID, but good callout. Lemme check status.

[REDACTED] (10/14/2020 18:24:59 PDT):

>If we don't have the trace, I think that, if it's possible, we should probably just do the overlay. They're as core political ads as you can get and the content isn't overtly harmful so it feels weird to remove all signs of the ad.

[REDACTED] (10/14/2020 18:25:12 PDT):

>Especially since we aren't removing in organic.

[REDACTED] (10/14/2020 18:25:56 PDT):

>that makes sense to me, and the overlay is the default for when these are disapproved, so this will happen. I'll chase the trace!

[REDACTED] (10/14/2020 18:29:50 PDT):

>Terrific, thanks. Very good call out.

[REDACTED] (10/14/2020 18:33:56 PDT):

>Well. I've found at least one copy. From my own newsfeed. With [REDACTED] tagged in it 😬

[REDACTED] (10/14/2020 18:34:05 PDT):

shared: 121574359_403213744400511_7118563285716987168_n.jpg

[REDACTED] (10/14/2020 18:34:35 PDT):

>Everyone needs to be very nice to [REDACTED]

[REDACTED] (10/14/2020 18:34:46 PDT):

>Agreed.

[REDACTED] (10/14/2020 18:34:55 PDT):

>Yeah, this is exactly what we need to know if it's floating around.

[REDACTED] (10/14/2020 18:35:18 PDT):

>Maybe they can just track where [REDACTED] is being tagged.

[REDACTED] (10/14/2020 18:35:51 PDT):

>Yeah. POOL

[REDACTED] (10/14/2020 19:10:26 PDT):

[REDACTED] - where Ops is collecting info on posts of the personal hunter Biden photos, including VPVs and who posted

[REDACTED] (10/14/2020 19:10:45 PDT):

>Working doc here: [REDACTED]

Exhibit 114

From: [REDACTED] </O=THEFACEBOOK/OU=EXTERNAL (FYDIBOHF25SPDLT)/CN=RECIPIENTS/CN=8E98834A8DAB4AA28B1A5C9B98E6C555>
To: [REDACTED]; [REDACTED]
Sent: 10/14/2020 8:22:08 AM
Subject: Message summary [{"otherUserFbld":100045157310260,"threadFbld":null}]

[REDACTED] (10/14/2020 08:16:30 PDT):
>Hi! FYSA - the Actor Level Enforcement topic ([REDACTED]'s issue that [REDACTED] emailed us about Mon night) is going through IDM tomorrow.

[REDACTED] (10/14/2020 08:17:41 PDT):
>On this h/l issue, is there anything I could have done to help you since it started early am? I did call [REDACTED] and asked him about the FIFT/FBI outreach, and weighing in. But, please flag if there's something I could have done to help while you were still sleeping! :-)

[REDACTED] (10/14/2020 08:18:36 PDT):
>i don't think so - i think it's more of a misinfo policy issue vs a hack and leak scenario because the content isn't on the platform and it's just news reporting, so interesting to see that play out. [REDACTED] has been pretty all over it so think we're good but thank you!

[REDACTED] (10/14/2020 08:18:55 PDT):
>ha - I was just correcting and saying no h/l issue! NY Post!

[REDACTED] (10/14/2020 08:22:08 PDT):
>Totally with you - very interesting to see how this plays out here

Produced to HJC

Exhibit 115

Message

From: ██████████@fb.com]
Sent: 10/14/2020 9:35:06 PM
To: ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]; ██████████@fb.com]
Subject: Message summary [{"otherUserFbId":null,"threadFbId":3170631142987191}]
Attachments: 121161847_1316086545401657_7329363007398542195_n.png;
 44921221_2042068942551652_3469405441325268992_n.gif

██████████ (10/14/2020 10:15:00 PDT):
 >Does anyone understand what happened here? why did ██████████ tweet that we were reducing?

██████████ (10/14/2020 10:15:42 PDT):
 >I presume just people moving too fast

██████████ (10/14/2020 10:39:35 PDT):
 >I think everyone was trigger happy about this type of content being leaked, and made decisions that they should not have made individually and without consultation

██████████ (10/14/2020 10:39:57 PDT):
 >This was the content that people were most primed by LE, etc. to expect in a hack/leak

██████████ (10/14/2020 10:42:35 PDT):
 >Everything ██████████ tweeted is true and consistent with how we've responded to other types of content. He moved too quickly.

██████████ (10/14/2020 15:06:00 PDT):
 >ok what's the latest?

██████████ (10/14/2020 15:06:04 PDT):
 >I was offline

██████████ (10/14/2020 15:06:16 PDT):
 >maybe just give me a traffic light - red? :)

██████████ (10/14/2020 15:11:21 PDT):
 ><https://twitter.com/realDonaldTrump/status/1316501350658707456>

██████████ (10/14/2020 15:11:42 PDT):
 >I see this as a feature not a bug.

██████████ (10/14/2020 15:16:48 PDT):
 >I'm having real second thoughts about the wisdom of a label

██████████ (10/14/2020 15:17:59 PDT):
 >TBH: I think we are in a good place now if we did nothing further. Don't remove anything and don't add anything

██████████ (10/14/2020 15:18:42 PDT):
 >You mean don't remove demotion for the couple of original posts, don't enqueue anything else, don't demote anything else

██████████ (10/14/2020 15:18:44 PDT):
 >Meaning: not to remove demotion, keep demotion while fact checkers work to fact check

██████████ (10/14/2020 15:18:55 PDT):
 >Keep demotion for those couple of posts only

██████████ (10/14/2020 15:19:40 PDT):
 >Think that's right

██████████ (10/14/2020 15:20:09 PDT):
 >What do we say to questions about why we aren't demoting more?

██████████ (10/14/2020 15:20:27 PDT):
 >Demoting other instances?

██████████ (10/14/2020 15:21:36 PDT):
 >I know if we're OK I don't see what we get from a label. Are we being criticized / pushed really hard? It looks like we kind of got benefit of doubt b/c we moved fast on demotion, who'd believe.

[REDACTED] (10/14/2020 15:21:53 PDT):

>Yeah

[REDACTED] (10/14/2020 15:22:26 PDT):

>I think that the issue is that some of us (especially Joel) feel that demotion isn't really defensible and we need to pull it

[REDACTED] (10/14/2020 15:22:42 PDT):

>And then Nick feels that we can't leave zero enforcement

[REDACTED] (10/14/2020 15:23:16 PDT):

>I think the label is dumb

[REDACTED] (10/14/2020 15:23:40 PDT):

>I think the precedent of label is REALLY problematic.

[REDACTED] (10/14/2020 15:23:44 PDT):

>Yeah

[REDACTED] (10/14/2020 15:23:53 PDT):

>I also just don't think that it helps anything

[REDACTED] (10/14/2020 15:24:07 PDT):

>is it a label for hacked content?

[REDACTED] (10/14/2020 15:24:10 PDT):

>[REDACTED], what happens if we lift demotion based on feedback from factcheckers

[REDACTED] (10/14/2020 15:24:12 PDT):

>Yes

[REDACTED] (10/14/2020 15:24:25 PDT):

shared: 121161847_1316086545401657_7329363007398542195_n.png

[REDACTED] (10/14/2020 15:24:30 PDT):

>It's this

[REDACTED] (10/14/2020 15:24:35 PDT):

>Stilly

[REDACTED] (10/14/2020 15:24:56 PDT):

>yeah - as soon as i saw the actual label mock, i had the exact same reaction

[REDACTED] (10/14/2020 15:25:24 PDT):

>team did a good job, but just doesn't cut the mustard compared to what twitter is doing, we will look very weak.

[REDACTED] (10/14/2020 15:25:56 PDT):

>What specifically do you find stronger about Twitter's?

[REDACTED] (10/14/2020 15:26:03 PDT):

>whereas right now in the press/left, we are in a good place. the concern about how do we answer questions from the right about these things still is probelmatic.

[REDACTED] (10/14/2020 15:26:09 PDT):

>its an interstitial

[REDACTED] (10/14/2020 15:26:23 PDT):

>introduces friction, and prevents you from posting

[REDACTED] (10/14/2020 15:26:56 PDT):

>Got it. That's several hours away - tonight maybe; was not planned as an arbitrary label. - and I think equally a problematic precedent so I would not advise.

[REDACTED] (10/14/2020 15:49:20 PDT):

>? how did that happen? thats what [REDACTED] and i wanted... how did we end up there?

[REDACTED] (10/14/2020 15:49:32 PDT):

>Where?

[REDACTED] (10/14/2020 15:49:32 PDT):

>Mark and sheryl

[REDACTED] (10/14/2020 15:49:50 PDT):

>not making any changes today.

[REDACTED] (10/14/2020 15:50:08 PDT):

>Mind meld. ...whoever made this happen, thank you

[REDACTED] (10/14/2020 16:19:25 PDT):

>Can it please stop

[REDACTED] (10/14/2020 16:21:56 PDT):

>I feel I am like 5 layers deep in escalations and can't even remember which other thing someone is pinging me about

[REDACTED] (10/14/2020 16:22:08 PDT):

>Break glass seems so old!

[REDACTED] (10/14/2020 16:22:11 PDT):

>Same

[REDACTED] (10/14/2020 16:22:24 PDT):

>I have no memory of what occurred today

[REDACTED] (10/14/2020 16:24:29 PDT):

>This whole thing feels like I'm the guy from the movie Memento

[REDACTED] (10/14/2020 16:24:35 PDT):

>Can't remember where the f- I am

[REDACTED] (10/14/2020 16:24:43 PDT):

shared: 44921221_2042068942551652_3469405441325268992_n.gif

[REDACTED] (10/14/2020 16:26:29 PDT):

>What are your thoughts on the non-newsworthy stuff?

[REDACTED] (10/14/2020 16:26:37 PDT):

>Which we can chase all over the platform?

[REDACTED] (10/14/2020 16:29:56 PDT):

>I'm unsure we should chase. Aren't these so wide spread that it's totally moot?

[REDACTED] (10/14/2020 17:02:29 PDT):

>just once - i don't really understand "hack and leak" as well but honestly this feels like a weak "hack"

[REDACTED] (10/14/2020 17:03:04 PDT):

>hunter gave it to a computer guy to get fixed, and something something something, fbi got it too

[REDACTED] (10/14/2020 17:04:20 PDT):

>Well, it's not coming from FBI

[REDACTED] (10/14/2020 17:04:36 PDT):

>Computer guy gave one copy to FBI and one to Rudy Guiliani

[REDACTED] (10/14/2020 17:04:50 PDT):

>Who is now sharing it with press

[REDACTED] (10/14/2020 17:05:21 PDT):

>It is a weird hack

[REDACTED] (10/14/2020 17:17:35 PDT):

>I totally missed this in all the action, did you see Twitter also updated policies to remove Holocaust Denial?

>

>Nice to be first a bit...

[REDACTED] (10/14/2020 19:00:36 PDT):

>yeah - i noted to [REDACTED] maybe its time for an enterprising reporter to write a counternarrative story about how twitter of late has been following our lead - trump post, NYPost, holocaust, election rules, etc.

[REDACTED] (10/14/2020 19:50:24 PDT):

>I like it. Also, this thread is helpful

[REDACTED] (10/14/2020 19:50:29 PDT):

><https://twitter.com/kantrowitz/status/1316569785824612353?s=21>

[REDACTED] (10/14/2020 19:51:06 PDT):

>(Golden Rule: The Press is only as good to you as you are bad to Trump)

[REDACTED] (10/14/2020 20:15:26 PDT):

>I miss nuance

[REDACTED] (10/14/2020 20:15:59 PDT):
>Though this is accurate

[REDACTED] (10/14/2020 21:34:24 PDT):
>Is anyone aware if Mark is going to post something about preparations or break glass levers? (as a follow on to his SG post about why policies are changing etc)

[REDACTED] (10/14/2020 21:35:06 PDT):
>Believe he is mentioning in Q&A tomorrow, not posting yet

Produced to HJC

Exhibit 116

From: [REDACTED] /O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED] CHA86>
To: [REDACTED]
Sent: 10/14/2020 9:33:47 PM
Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]
Attachments: sticker.png

[REDACTED] (10/14/2020 08:59:45 PDT):
>should we be considering pushing for reducing distribution or reshare friction for the nypost story until it is fact checked? just reading some ideas out there from [REDACTED] and others

[REDACTED] (10/14/2020 09:01:43 PDT):
>We have

[REDACTED] (10/14/2020 09:01:47 PDT):
>We reduced about an hour ago.

[REDACTED] (10/14/2020 09:01:53 PDT):
>We reduced distro

[REDACTED] (10/14/2020 09:02:04 PDT):
><https://twitter.com/shannonpareil/status/1316402316233252865?s=21>

[REDACTED] (10/14/2020 09:02:04 PDT):
>:-D

[REDACTED] (10/14/2020 09:02:05 PDT):
>At this point it's not fact checked so there isn't an interstitial for sharing tho, fwiw

[REDACTED] (10/14/2020 09:02:19 PDT):
>Right - we demoted pending 3PFC review.

[REDACTED] (10/14/2020 09:02:25 PDT):
>We can't go further unless/until they review

[REDACTED] (10/14/2020 09:02:33 PDT):
>We've also enqueued to fact checkers

[REDACTED] (10/14/2020 09:02:34 PDT):
>Also I'm so happy we did that news moment two weeks ago

[REDACTED] (10/14/2020 09:02:49 PDT):
>Yep.

[REDACTED] (10/14/2020 09:02:59 PDT):
>Worth noting that we were almost exactly right in our prediction.

[REDACTED] (10/14/2020 09:03:05 PDT):
>Day before a "debate"

[REDACTED] (10/14/2020 09:03:30 PDT):
>Yup

[REDACTED] (10/14/2020 09:13:16 PDT):
>Can you guys circle w/ [REDACTED] and ask the Q of whether we think there's enough here to claim this is a "leak as a part of a foreign influence operation" ?

[REDACTED] (10/14/2020 09:14:07 PDT):
>I doubt we see the evidence at this point, but would like to make sure we map to our factors and have an answer if leadership asks.

[REDACTED] (10/14/2020 09:14:27 PDT):
>yeah doubtful as well but I'll check in with him

[REDACTED] (10/14/2020 09:14:59 PDT):

Final Report 1522

shared: sticker.png

[REDACTED] (10/14/2020 09:15:07 PDT):

>Can you keep me on the thread w [REDACTED]?

[REDACTED] (10/14/2020 09:16:40 PDT):

>One question

[REDACTED] (10/14/2020 09:16:48 PDT):

>Where did we net out on off platform evidence?

[REDACTED] (10/14/2020 09:16:53 PDT):

>We have a meeting with FITF today

[REDACTED] (10/14/2020 09:29:19 PDT):

>This was the template [REDACTED] put together [REDACTED]

[REDACTED] (10/14/2020 09:38:25 PDT):

>No evidence at this point that I'm aware of. Will be interested to see what you hear from FITF.

[REDACTED] (10/14/2020 10:21:21 PDT):

>FYSA FITF confirmed that such a laptop does exist and is in the hands of the criminal division

[REDACTED] (10/14/2020 10:21:24 PDT):

>that's all they could say

[REDACTED] (10/14/2020 10:26:44 PDT):

>heh -- about as expected.

[REDACTED] (10/14/2020 11:31:08 PDT):

>can you guys add me to the facts doc?

[REDACTED] (10/14/2020 11:31:19 PDT):

>Just want to make sure I'm solid on them for the discussions I can anticipate internally...

[REDACTED] (10/14/2020 11:31:28 PDT):

>added

[REDACTED] (10/14/2020 11:31:39 PDT):

>NG - do you have the list of domains that Aoel is going to blacklist?

[REDACTED] (10/14/2020 11:31:41 PDT):

>*Yoel

[REDACTED] (10/14/2020 11:31:45 PDT):

>if not i can send to u

[REDACTED] (10/14/2020 11:31:46 PDT):

>link?

[REDACTED] (10/14/2020 11:31:48 PDT):

>I do

[REDACTED] (10/14/2020 11:31:58 PDT):

><https://fb.quip.com/oslqApMaCOIM>

[REDACTED] (10/14/2020 11:32:39 PDT):

>doc says they were disclosed "without approval of the story"

[REDACTED] (10/14/2020 11:32:46 PDT):

>that should be "without approval of the owner" right/

[REDACTED] (10/14/2020 11:32:47 PDT):
>?

[REDACTED] (10/14/2020 11:33:08 PDT):
>yeahhh probably

[REDACTED] (10/14/2020 11:33:15 PDT):
>move fast, break things

[REDACTED] (10/14/2020 11:33:34 PDT):
>yeah, w/o approval of the owner

[REDACTED] (10/14/2020 11:33:59 PDT):
>awesome!

[REDACTED] (10/14/2020 12:51:23 PDT):
>what are the key points to suggest that this info is inauthentic?

[REDACTED] (10/14/2020 12:51:58 PDT):
>I know the photoshop issue

[REDACTED] (10/14/2020 12:52:02 PDT):
>is there more?

[REDACTED] (10/14/2020 12:52:09 PDT):
>this is an asap thing if you know anything.

[REDACTED] (10/14/2020 12:52:12 PDT):
>1) No evidence the laptop was indeed Hunter Biden's

[REDACTED] (10/14/2020 12:53:43 PDT):
>from [REDACTED] after claiming the shop owner couldn't identify the customer, the piece includes a receipt that was issued to "Hunter Biden" and includes an email and phone # So why would the shop owner produce a receipt for Hunter Biden if he didn't know the ID of the customer?)

[REDACTED] (10/14/2020 12:54:08 PDT):
>2) the grand jury subpoena shown does not connect the laptop to Hunter Biden

[REDACTED] (10/14/2020 12:54:50 PDT):
>thats all i have off the top of my head

[REDACTED] (10/14/2020 12:55:33 PDT):
>got it -- thank you!

[REDACTED] (10/14/2020 12:55:45 PDT):
>Q: Do you guys think we should remove these stories?

[REDACTED] (10/14/2020 13:00:23 PDT):
>Yes. This is unverified and OCP

[REDACTED] (10/14/2020 13:00:33 PDT):
>OCP's case is relatively strong here

[REDACTED] (10/14/2020 13:39:44 PDT):
>Yeah

[REDACTED] (10/14/2020 13:39:56 PDT):
>We may need to lean harder into why publicly

[REDACTED] (10/14/2020 13:41:20 PDT):
>what's going on with the escalation/decision?

[REDACTED] (10/14/2020 13:50:29 PDT):
>Probably heading toward labelling the content, as opposed to removal.

[REDACTED] (10/14/2020 13:51:22 PDT):
>any friction?

[REDACTED] (10/14/2020 13:51:37 PDT):

>I don't think so - I'm not sure we have an option to do that.

[REDACTED] (10/14/2020 15:59:17 PDT):

[REDACTED] Just curious if you can share at some point how the decision came about and landed where it did. Just reading snippets in these chats and trying to understand

[REDACTED] (10/14/2020 21:23:02 PDT):

[REDACTED] I threw on a sync tomorrow for a few of us east coasters in the early am tomorrow.

[REDACTED] (10/14/2020 21:23:12 PDT):

[REDACTED] It's at 930 am est, so I spared you the invite.

[REDACTED] (10/14/2020 21:23:24 PDT):

>Thanks ;)

[REDACTED] (10/14/2020 21:23:51 PDT):

>But goal is to do an initial brainstorm on how to expose these guys, and then start a doc between a few of us to kick ideas around async throughout tomorrow.

[REDACTED] (10/14/2020 21:27:34 PDT):

>Fun! [☺] what can I do to prepare tonight? Already going down some rabbit holes

[REDACTED] (10/14/2020 21:29:13 PDT):

>Get some rest :-P

[REDACTED] (10/14/2020 21:29:40 PDT):

[REDACTED] approve my travel request to Moscow I have some leads to follow up on

[REDACTED] (10/14/2020 21:29:00 PDT):

>They don't have covid there should be safe I saw it in komsomolskaya pravda

[REDACTED] (10/14/2020 21:29:21 PDT):

>(Good luck y'all)

[REDACTED] (10/14/2020 21:29:29 PDT):

>The idea is to think about ways we could knock them off their game if they pop on our systems in some way

[REDACTED] (10/14/2020 21:31:06 PDT):

>so (a) where to look; (b) ways to trick them into exposing themselves [REDACTED] think of your demotion/amplification point); (c) how to find them if they do pop.

[REDACTED] (10/14/2020 21:32:03 PDT):

>Also, [REDACTED] can you update the XFN lines in the IB report so I can send?

[REDACTED] (10/14/2020 21:32:16 PDT):


>Ya doing now

[REDACTED] (10/14/2020 21:33:47 PDT):

>Done

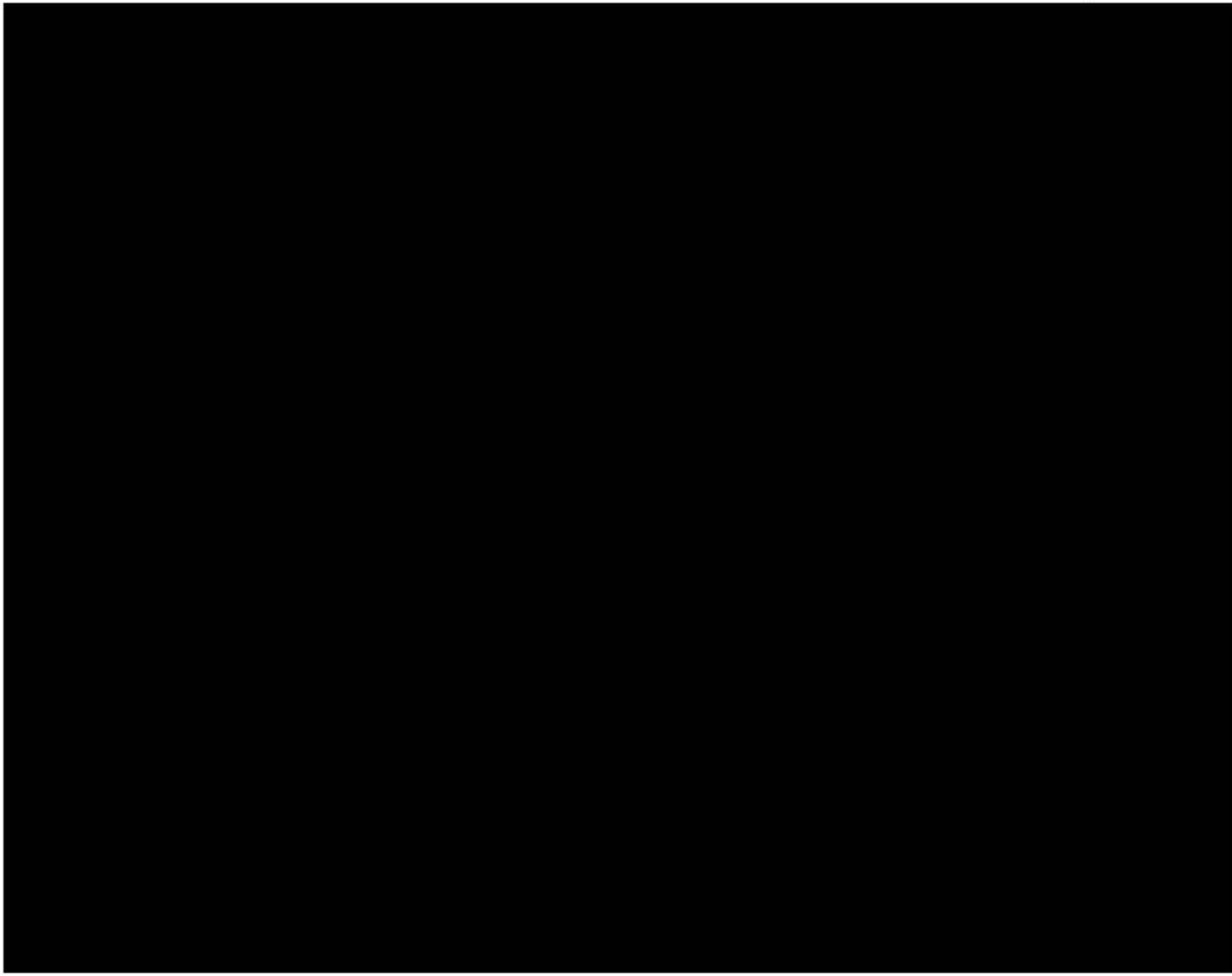
Exhibit 117

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]

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] subscribed [Redacted]

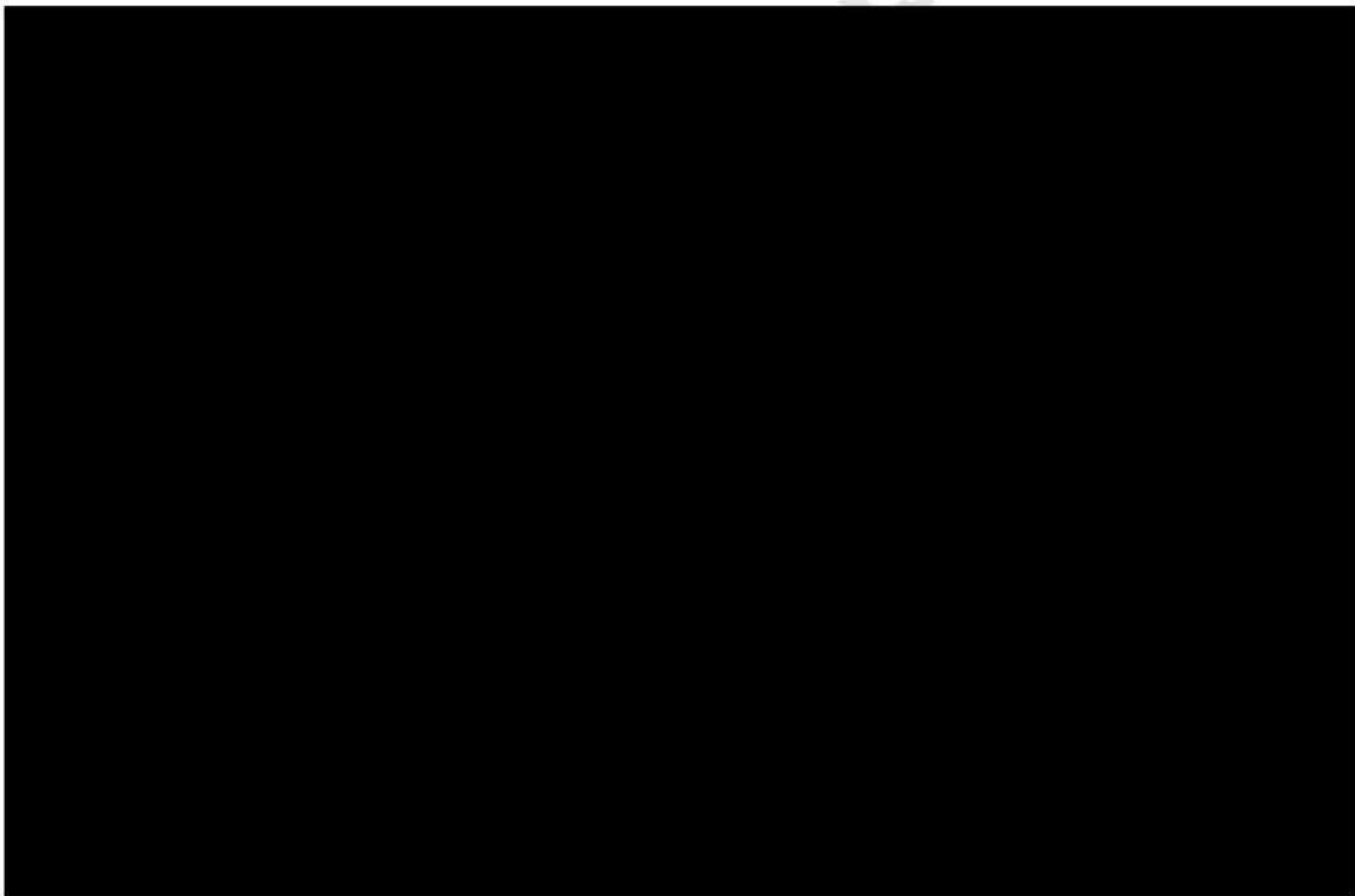
October 15, 2020 · Like

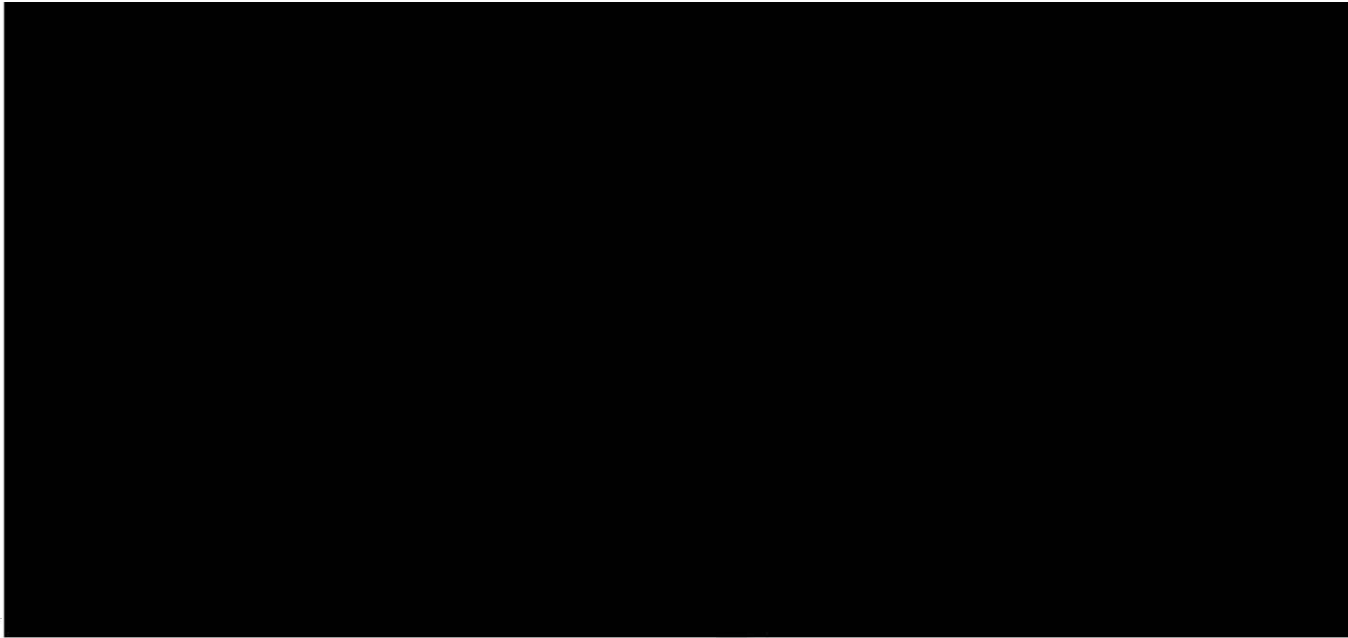


[Redacted]

Here is where I will be working through the various hack/leak policy factors: <https://fb.quip.com/elfiA8ZQDBzL>

October 15, 2020 · Like · Reply





Produced by

Exhibit 118

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]237>
To: Chan, Elvis M. (SF) (FBI); [REDACTED] (CD) (FBI)
CC: [REDACTED]; [REDACTED]; [REDACTED]
Sent: 10/15/2020 2:15:01 PM
Subject: Re: follow up

Thanks for the call Elvis, appreciate it.

From: "Chan, Elvis M. (SF) (FBI)" <[REDACTED]@fbi.gov>
Date: Thursday, October 15, 2020 at 5:13 PM
To: [REDACTED] <[REDACTED]@fb.com>, "[REDACTED] (CD) (FBI)" <[REDACTED]@fbi.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@fb.com>
Subject: Re: follow up

[REDACTED] - closed the loop with [REDACTED].

Regards,
 Elvis

Elvis M. Chan
 Supervisory Special Agent
 Squad CY-1
 San Francisco Division
 Federal Bureau of Investigation
 W: [REDACTED]
 C: [REDACTED]

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, October 15, 2020 10:03 AM
To: [REDACTED] (CD) (FBI) <[REDACTED]@fbi.gov>; Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: [EXTERNAL EMAIL] - follow up

Hey [REDACTED] and Elvis,

Wanted to touch base after the FITF call yesterday to follow up on one of the topics we raised. Would you have time for a quick phone call this week (today/tomorrow)?

[REDACTED]

Exhibit 119

From: [REDACTED] </O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[REDACTED]@9C>
 To: [REDACTED]
 Sent: 10/15/2020 8:26:18 PM
 Subject: Message summary [{"otherUserFbld":null,"threadFbld": [REDACTED]}]

[REDACTED] (10/15/2020 08:50:04 PDT):

>hey team, can we have a quick call on something i'm hearing from reporters? need 10 min max

[REDACTED] (10/15/2020 08:50:20 PDT):

>might be nothing, but wanted to flag

[REDACTED] (10/15/2020 08:51:05 PDT):

>what's the topic ([REDACTED])?

[REDACTED] (10/15/2020 08:51:18 PDT):

>I have 9 mins.

[REDACTED] (10/15/2020 08:51:26 PDT):

>cant type

[REDACTED] (10/15/2020 08:51:29 PDT):

>I'm avail now as well

[REDACTED] (10/15/2020 08:51:53 PDT):

[REDACTED] (10/15/2020 08:54:05 PDT):

>@ [REDACTED] -- try to rejoin!

[REDACTED] (10/15/2020 08:54:56 PDT):

>Says I can't rejoin bc [REDACTED] removed me.

[REDACTED] (10/15/2020 08:55:44 PDT):

[REDACTED] (10/15/2020 08:56:00 PDT):

>try now?

[REDACTED] (10/15/2020 08:56:04 PDT):

>someone giv readout im getting serious fomo

[REDACTED] (10/15/2020 08:56:10 PDT):

>{ i cant join, am on external call}

[REDACTED] (10/15/2020 08:56:14 PDT):

>good lucky to you all

[REDACTED] (10/15/2020 09:29:50 PDT):

>jfyi, nothing to do here, but got this from buzzfeed in ukraine:

>
 >Regarding Facebook's decision today to reduce the distribution of a New York Post story about the Biden family, I wanted to ask... were all accounts sharing the story impacted? I ask because I followed several Ukrainian accounts, including those of several high-profile individuals who have worked with Rudy Giuliani to help Donald Trump's campaign. One of the individuals, Andriy Derkach, was sanctioned by the US and labeled an "active Russian agent." The others are Andriy Telichenko and Andriy Onyshchenko, both of whom have been involved in spreading Russian disinformation about Joe Biden.

[REDACTED] (10/15/2020 10:09:27 PDT):

><https://www.the-sun.com/news/1629764/joe-biden-hunter-emails-ukraine-smoking-gun-video/>

[REDACTED] (10/15/2020 10:10:29 PDT):

>thats somethin

Final Report 1533

[REDACTED] (10/15/2020 10:10:52 PDT):
>sounds it is being pitched as a file from the laptop

[REDACTED] (10/15/2020 10:11:25 PDT):
>yeah there were allegedly some photos on teh laptop. they look very fishiy

[REDACTED] (10/15/2020 10:20:53 PDT):
>a story's coming out shortly on Guo media amplifying this stuff

[REDACTED] (10/15/2020 10:21:03 PDT):
>Guo?

[REDACTED] (10/15/2020 10:21:04 PDT):
><https://twitter.com/billowypie/status/1315496175794697956>

[REDACTED] (10/15/2020 10:21:16 PDT):
>https://en.wikipedia.org/wiki/Guo_Wengui

[REDACTED] (10/15/2020 10:21:54 PDT):
>exiled chinese dude who's facing an indictment in china

[REDACTED] (10/15/2020 10:22:02 PDT):
>ah that guo

[REDACTED] (10/15/2020 10:22:30 PDT):
>this was a few days ago

[REDACTED] (10/15/2020 10:29:51 PDT):
>will we be announcing the new IRA linked behavior [REDACTED] just shared to Twitter? Or is that just CE?

[REDACTED] (10/15/2020 10:31:46 PDT):
>we can make a case to announce even if it's CE if we need to

[REDACTED] (10/15/2020 10:32:00 PDT):
>but i dont know much about the case

[REDACTED] (10/15/2020 10:34:24 PDT):
>@ [REDACTED] -- are you joining our meeting (with legal folks)? or are you on the [REDACTED] call?

[REDACTED] (10/15/2020 10:35:38 PDT):
>coming.

[REDACTED] (10/15/2020 10:42:11 PDT):
><https://twitter.com/AlKapDC/status/1316755251647610881>

[REDACTED] (10/15/2020 10:44:36 PDT):
>interesting.

[REDACTED] (10/15/2020 12:38:51 PDT):
>Here we go <https://twitter.com/ChanelRion/status/1316737397943395329?s=20>

[REDACTED] (10/15/2020 12:46:14 PDT):
>oh god its chanel

[REDACTED] (10/15/2020 12:47:17 PDT):
>it's gonna break at some point and people will start sharing links to these tapes/images. we sorta need a plan:)

[REDACTED] (10/15/2020 12:49:29 PDT):
>I think the legal consensus is to NOT take the tapes/images. Whatever benefit we may gain would be outweighed by the backlash from us getting the images and videos

[REDACTED] (10/15/2020 12:49:41 PDT):
>@ [REDACTED] -- I think that's what Joel said, too.

[REDACTED] (10/15/2020 12:48:43 PDT):

>copy

[REDACTED] (10/15/2020 12:49:44 PDT):

>Right?

[REDACTED] (10/15/2020 12:49:00 PDT):

>Can we get a vendor to get them?

[REDACTED] (10/15/2020 12:49:21 PDT):

>lets take offline if at all

[REDACTED] (10/15/2020 14:04:58 PDT):

>Can anyone point me to the hack & leak policy?

[REDACTED] (10/15/2020 14:13:15 PDT):

>@ [REDACTED] -- people are telling me that you should have this. Don't ghost me!

[REDACTED] (10/15/2020 14:13:50 PDT):

>it's in the community standards

[REDACTED] (10/15/2020 14:14:07 PDT):

>Oh, sneaky

[REDACTED] (10/15/2020 14:14:09 PDT):

> [REDACTED] - it's in hte CS Privacy section

[REDACTED] (10/15/2020 14:14:32 PDT):

>FYI - just connected with FBI (Elvis) to follow up on the question re foreignness. Elvis reiterated that he is now up to speed on the criminal matter and can confirm that at this point they don't see any foreign connections. @ [REDACTED] - would you like me to document this anywhere?

[REDACTED] (10/15/2020 14:16:37 PDT):

>Can you put it here? <https://www.internalfb.com/cases/215252>

[REDACTED] (10/15/2020 14:17:07 PDT):

>@ [REDACTED] are the factors you mentioned discussed anywhere?

[REDACTED] (10/15/2020 14:17:59 PDT):

>Not in the CS

[REDACTED] (10/15/2020 14:18:04 PDT):

>Those are captured in the IS

[REDACTED] (10/15/2020 14:21:58 PDT):

>https://www.internalfb.com/intern/wiki/Content_Policy/CO_Resources/Implementation_Standards/#11-privacy-violations-an

[REDACTED] (10/15/2020 14:22:00 PDT):

>scroll down to the last portion

[REDACTED] (10/15/2020 15:58:40 PDT):

>Hi all - before I share this with the broader Hack/Leak chat thread, here is a draft of the current sitrep for I3 investigation to date. Per Hack/Leak playbook, i'll plan to share this in the broader A/C priv Hack/Leak coordination thread for awareness, unless there are any objections from this group: [REDACTED]

[REDACTED] (10/15/2020 16:05:00 PDT):

>@ [REDACTED] -- should the doc be marked "confidential" or something like that? Not sure if this is DSS3 level information.

[REDACTED] (10/15/2020 16:07:15 PDT):

>DSS3?

[REDACTED] (10/15/2020 16:07:47 PDT):

>I can mark it A/C Priv or confidential or both?

Final Report 1535

[REDACTED] (10/15/2020 16:09:50 PDT):

[REDACTED] (10/15/2020 16:09:55 PDT):

>DSS3=Don't Send [REDACTED] 3nything

[REDACTED] (10/15/2020 16:09:14 PDT):

>Not sure if it rises to the level of DSS 3, but for consideration due to the potential impact

[REDACTED] (10/15/2020 16:09:26 PDT):

>I can also link it in the SEV, and share the SEV S#. The SEV is private, so we can control access that way

[REDACTED] (10/15/2020 16:10:01 PDT):

>My other question is whether this is something that has to go to the H/L chat thread.

[REDACTED] (10/15/2020 16:10:25 PDT):

>I like that idea. I think we should try to keep a close hold on this info

[REDACTED] (10/15/2020 16:11:09 PDT):

>tbh i'm a little surprised that thread hasn't been activated yet - it's explicitly listed as a coordination mechanism by Strategic Response in the Hack/Leak playbook

[REDACTED] (10/15/2020 16:11:55 PDT):

>Here is the SR H/L Playbook: [REDACTED]

[REDACTED] (10/15/2020 16:11:55 PDT):

>[REDACTED] -- can you point me to the H/L playbook? Unless that is Don't Send [REDACTED] 3nything restricted.

[REDACTED] (10/15/2020 16:12:06 PDT):

[REDACTED] - for "is there evidence of a hack" - you're really answering if there is evidence of a hack *on FB*

[REDACTED] (10/15/2020 16:12:22 PDT):

>whereas the broader KIQ is "was the information on teh laptop from hacked sources"

[REDACTED] (10/15/2020 16:12:41 PDT):

>Correct, I can clarify

[REDACTED] (10/15/2020 16:13:20 PDT):

>although we do incorporate LE/vendor/industry assessment, so it's broader than just on platform.

[REDACTED] (10/15/2020 16:14:39 PDT):

>[REDACTED] - can I mark it A/C PRIV - CONFIDENTIAL? Is that a thing?

[REDACTED] (10/15/2020 16:16:17 PDT):

>Yes. They are two separate markings. If this is going to the entire h/l can, should not be a/c priv, though. That is too large a group and works not be for legal advice at that point

[REDACTED] (10/15/2020 16:17:19 PDT):

>gotcha, i'll change to confidential only then

[REDACTED] (10/15/2020 16:24:18 PDT):

>https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43159900-0ef5-11eb-b1e9-16b59b92b36d_story.html

[REDACTED] (10/15/2020 16:26:35 PDT):

>Good context

[REDACTED] (10/15/2020 16:36:51 PDT):

>Any comments/edits before I share the sitrep with the H/L thread? I'll share the SEV only

[REDACTED] (10/15/2020 16:37:57 PDT):

> [REDACTED] - not worried about this getting spread to widely w the chat thread?

[REDACTED] (10/15/2020 16:38:23 PDT):

>My inclination is to keep this fairly tight.

[REDACTED] (10/15/2020 16:38:38 PDT):

>Do we feel like it needs to go to the full thread?

[REDACTED] (10/15/2020 16:40:02 PDT):

>If we want to keep it tight I can put this in the SEV and not chime in on the thread yet, but I assume at some point folks will be reaching out for updates. Do we want to have a sanitized version of this that is more broadly shareable?

[REDACTED] (10/15/2020 17:19:27 PDT):

>No. I don't think the entire xfn is or should be involved in this incident. The people who should be involved will get access.

[REDACTED] (10/15/2020 17:21:48 PDT):

>Ok, so not sharing it in the H/L thread then. The sitrep is linked in the SEV [REDACTED]. Both the sitrep doc and the SEV are access restricted. If you would like to have anyone added to the SEV, let [REDACTED] or I know and we'll add folks.

[REDACTED] (10/15/2020 17:58:00 PDT):

[REDACTED] (10/15/2020 18:12:11 PDT):

>I agree...just declined a handful of randoms from some of the tasks. The litmus test is if I don't know you or can't explain why you're critical...no access. I think we do need to be really careful for sake of leaks on this stuff.

[REDACTED] (10/15/2020 18:13:15 PDT):

>Had to do the same on the SEV as well.

[REDACTED] (10/15/2020 19:39:42 PDT):

><https://twitter.com/vijaya/status/1316923549236551690?s=20>

>

>

>1. We will no longer remove hacked content unless it is directly shared by hackers or those acting in concert with them

>

>2. We will label Tweets to provide context instead of blocking links from being shared on Twitter

[REDACTED] (10/15/2020 20:03:26 PDT):

><https://www.rawstory.com/2020/10/revealed-feds-investigating-whether-questionable-hunter-biden-story-was-planted-by-foreign-intelligence/>

[REDACTED] (10/15/2020 20:25:36 PDT):

>Separately, [REDACTED] just let me know that she was tipped by a friend that Google will be putting out a blog tomorrow similar to their previous one on attempted Chinese and Iranian election interference.

[REDACTED] (10/15/2020 20:26:18 PDT):

>also on CH and IR targeting or something else?

Exhibit 120

Exhibit 121

From: [REDACTED] (CD) (FBI) <[REDACTED]@fbi.gov>
To: **Meta Employee 3**
Sent: 10/18/2020 10:52:51 AM
Subject: [EXTERNAL EMAIL] - Article

Sure, give me a call when you are free.

-
On Oct 18, 2020 1:36 PM, **Meta Employee 3** wrote:

Are you tracking this? <https://www.thedailybeast.com/rudys-russian-agent-pal-teases-second-laptop-with-hunter-biden-kompromat?ref=home>

Does that change anything in your posture? Let me know if you're avail to catch up on the phone.

Meta Employee 3

Produced to HJC

Exhibit 122

[Redacted]

From: [Redacted]@fbi.gov>
Sent: Wednesday, April 24, 2024 10:26 AM
To: [Redacted]
Cc: Elvis Chan; [Redacted]; [Redacted]
Subject: FBI San Francisco Weekly Cyber Newsletter

This Message Is From an External Sender

Good morning Private Sector Partners –

Please see the below information provided by ASAC Chan for this week’s cyber briefing. He welcomes any feedback on the newsletter!

FBI SAN FRANCISCO CYBER THREAT BRIEFING 05-24-2024

The FBI does not request or expect your company to take any particular action regarding this information other than holding it in confidence due to its sensitive nature.

The FBI does not conduct its investigative activities or base attribution solely on activities protected by the First Amendment. Your company has no obligation to respond or provide information back to FBI in response to this engagement. If, after reviewing the information, your company decides to provide referral information to the FBI, it must do so consistent with federal law.

Current Events

Russia: [Redacted]

Morocco: [Redacted]

India: [Redacted]

[Redacted]

Netherlands: [Redacted]

United States:

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Recommendations

- Determine if your organization is impacted by the [REDACTED] vulnerability and follow the prescribed remediation process [REDACTED]

FBI Posture

- On 04/18/2024, Section 702 of the Foreign Intelligence Surveillance Act was reauthorized. As a reminder, this legislative tool allows the FBI to conduct electronic surveillance of Non-U.S. Persons who are residing overseas and using American internet service providers.

Thank you,

[REDACTED]

Intelligence Analyst
FBI San Francisco Private Sector Engagement Squad

Exhibit 123

Message

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=AD3998532E0E4B3D9BCDD5D44146E8D1-[REDACTED]]

Sent: 7/31/2020 4:57:51 PM

To: Graham Brookie [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ff607d9285134727b689a7dee86cffaf-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b1de80fc07404b22940cc28960422d10-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=167b19d1a7c44fc6830292788830d858-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=288ea1809383491ba909fc1a5bb1330d-[REDACTED]]

CC: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ab2f69c32a94430caac7988ba7180918-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4d1b4c008a0446b69c4afb07b645ebc0-[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e73979d414b94481a4a2590754791734-[REDACTED]]

Subject: Re: Quick question -- Park Advisors

10-4, when they first approached us we did refer them to the DFRLab. They then circled back about a month later and indicated the GeoTech Commission and some other activities with the GeoTech Center were of interest, so we looped in [REDACTED] on a draft potential collaboration we sorted out what this would could be - recognizing it was draft and might not pan out.

Probably the best POC to help coordinate would be [REDACTED] and then we all assemble to share the different efforts occurring?

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]@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

From: [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>
Date: Monday, July 20, 2020 at 7:50 PM
To: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>, [REDACTED]
 <[REDACTED]@ATLANTICCOUNCIL.ORG>, [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>, [REDACTED]
 <[REDACTED]@ATLANTICCOUNCIL.org>
Cc: [REDACTED] <[REDACTED]@atlanticcouncil.org>, [REDACTED] <[REDACTED]@atlanticcouncil.org>
Subject: Re: Quick question -- Park Advisors

Hi Graham,

Yes, we've been working with [REDACTED] on this agreement - GEC/Park Advisors haven't finalized the agreement yet however in the most recent drafts [REDACTED] is looking to put aside a modest amount of funds (\$25k) for engagement of the broader Atlantic Council's international community on the issues. You're right, [REDACTED] with Park Advisors (and thus the GEC) is former U.S. Army Intelligence Officer in the and someone I knew from my days with the People-Centered Internet and work with U.S. SOCOM.

The GEC/Park Advisors reached out in part because of the GeoTech Commission and a desire to involve [REDACTED] and some of the other Commissioners. In addition, the GEC and Park Advisors will also have a separate funding stream for just GeoTech looking for three events (two mid-sized, one large) on the geopolitics + technology solutions to counter election interference and other GEC-related topics.

For the \$25k, I think they're looking for us, as in the Atlantic Council as a whole to weigh-in on a planned DHS app that plans to teach the public about fake news and how election interference might occur.

Hope this helps,

[REDACTED]

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Monday, July 20, 2020 14:25
To: [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.ORG>
Cc: [REDACTED] <[REDACTED]@atlanticcouncil.org>; [REDACTED] <[REDACTED]@atlanticcouncil.org>
Subject: Quick question -- Park Advisors

[REDACTED], [REDACTED] -

Hope the start of the week is going well.

We just had a call with our partners at GEC and their new "Technology and Engagement Team," which has a number of people we've worked with before and seems to be mostly a number of former IC and contractors. One in particular - [REDACTED] of Park Advisors - said that Park Advisors is working on a partnership with Geotech Center to leverage international partnerships with Park Advisors (and thus with GEC).

First, that sounds great! Second, I wanted to reach out and get any additional context on that effort given the amount of work DFRLab are currently doing with GEC.

Thanks,
 Graham

Exhibit 124

From: [REDACTED] <[REDACTED]@google.com>
To: [REDACTED]
CC: [REDACTED]; [REDACTED]; [REDACTED] (CELA); [REDACTED]; [REDACTED]; [REDACTED]
Sent: 9/15/2020 5:34:33 PM
Subject: Re: Industry statement on election USG meeting TOMORROW

Thanks [REDACTED] -- best of luck to you! [REDACTED] -- I added you to the cal invite for the call tomorrow.

On Tue, Sep 15, 2020 at 5:07 PM [REDACTED] <[REDACTED]@reddit.com> wrote:
Hi [REDACTED] - Thanks for this. Adding in my colleague, [REDACTED], who will take this on as I am heading out on parental leave very soon.

Best,
[REDACTED]

On Tue, Sep 15, 2020 at 4:59 PM [REDACTED] <[REDACTED]@fb.com> wrote:

Thank you for sharing, [REDACTED]! The plan makes sense to us, happy to help with the image card if needed.

Looking forward to chatting tomorrow!

[REDACTED]

From: [REDACTED] <[REDACTED]@google.com>
Date: Tuesday, September 15, 2020 at 3:33 PM
To: "[REDACTED] (CELA)" <[REDACTED]@microsoft.com>, [REDACTED] <[REDACTED]@wikimedia.org>, [REDACTED] <[REDACTED]@linkedin.com>, [REDACTED] <[REDACTED]@google.com>, [REDACTED] <[REDACTED]@reddit.com>, [REDACTED] <[REDACTED]@twitter.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@verizonmedia.com>, [REDACTED] <[REDACTED]@verizonmedia.com>, [REDACTED] <[REDACTED]@pinterest.com>, [REDACTED] <[REDACTED]@twitter.com>, [REDACTED] <[REDACTED]@fb.com>, [REDACTED] <[REDACTED]@google.com>
Subject: Industry statement on election USG meeting TOMORROW

Hi all -- our colleagues on the security and policy side are planning to do another industry/USG meeting tomorrow. Thought this would be a good time to do another joint statement to remind reporters that this work is ongoing. Apologies for the rush job on this, but thinking we'd want to get this statement out right after the meeting tomorrow (3:30PM ET/12:30PM PT) so we'll need to gather signatures quickly.

Statement is pasted below -- added a bit more detail this time so that it could stand on its own. Please take a look and let this group know if your company is OK signing on. Realizing this is moving quickly, I'm also going to send

a calendar invite to everyone on this email for a quick call at 8 AM PT tomorrow. If you have questions/concerns, please feel free to join the call or have someone from your team join. Final Report 1550

For press strategy, think we can do something simple again like posting an image card with the statement on Twitter (and/or your newsroom) at 3:30PM ET/12:30PM PT. For Google, our plan would be to post from our policy handle and potentially have a few execs retweet.

We did run into an issue last time where some stories tried to position this as a *new* coalition, so we're being very clear in the statement that this work has been happening for several years and there is no new coalition/group forming -- just an update on ongoing work. It would be great if we could all help reinforce that message with reporters if we get calls/follow ups on this tomorrow.

Thanks all -- look forward to chatting tomorrow.

STATEMENT:

"For several years, tech companies have worked together, and with U.S. government agencies tasked with protecting the integrity of elections, to counter election threats across our respective platforms. As we approach the November election, we continue to prepare, meet regularly, and share updates on the threats we see. At today's meeting, we specifically discussed:

- 1. Ways to help provide real-time, clear information about the voting process and election results given expected logistical disruptions posed by COVID-19.*
- 2. Ways to counter targeted attempts to undermine the election conversation before, during, and after the election. This includes preparing for possible so-called "hack and leak" operations attempting to use platforms and traditional media to amplify unauthorized information drops.*
- 3. Detection efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.*

As the global pandemic poses unprecedented challenges for the 2020 U.S. election, we will continue this ongoing communication and close work between industry and U.S. institutions tasked with election security to share key findings and operational insights in the weeks to come."

Can confirm:

Among participants in today's industry-government meeting were: Google, Microsoft, Facebook, Twitter, Reddit, Verizon Media, Pinterest, LinkedIn, Wikimedia Foundation, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI's Foreign Influence Task Force, DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI).

--

[REDACTED]

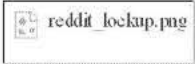
Google Communications & Public Affairs

[REDACTED]

--

[REDACTED]

Communications



--

[REDACTED]

Google Communications & Public Affairs

[REDACTED]

Produced to HJC

Exhibit 125



Federal Bureau of Investigation Counterintelligence Division

Providing Foreign Malign Influence Threat Information to Social Media Platforms

(U) Purpose:

(U) To provide FBI personnel a standard operating procedure (“SOP”) by which the Federal Bureau of Investigation (“FBI”) transmits Foreign Malign Influence (“FMI”) threat information (“tearlines”) to companies hosting social media (“Social Media Platforms”).¹

(U) Background and Authorities:

(U) In executing its primary mission to keep the American people safe, the Department of Justice has prioritized countering foreign malign influence operations, including online operations. One of the ways the FBI supports this mission is by providing FMI threat information to Social Media Platforms so that they may, in their discretion, take steps to mitigate such threats.² It is also Department “policy to alert the victims and unwitting targets of foreign influence activities, when appropriate and consistent with the Department’s policies and practices, and with our national security interests.”³ One of the appropriate reasons for disclosing FMI threat information is, as outlined in the Justice Manual, “to alert technology companies or other private sector entities to foreign influence operations when their services

¹ (U) While courts evaluating our interactions with social media companies have not explicitly defined “Social Media Platforms,” FBI personnel should apply this guidance to the transmission of FMI to Social Media Platforms as that phrase is commonly understood, and questions about whether a particular company should be viewed as a Social Media Platform should be directed to OGC. In general, Social Media Platforms include:

a website or internet medium that—(A) permits a person to become a registered user, establish an account, or create a profile for the purpose of allowing users to create, share, and view user-generated content through such an account or profile; (B) enables 1 or more users to generate content that can be viewed by other users of the medium; and (C) primarily serves as a medium for users to interact with content generated by other users of the medium.

See 42 U.S.C. § 1862w(a)(2).

² (U) See U.S. Department of Justice, Report of the Attorney General’s Cyber Digital Task Force (2018), located at justice.gov/archives/ag/page/file/1076696/download, at 12 (“[T]he FBI and IC partners may be able to identify and track foreign agents as they establish their infrastructure and mature their online presence, in which case authorities can work with social media companies to illuminate and ultimately disrupt those agents’ activities through voluntary removal of accounts that violate a company’s terms of service.”).

³ (U) Justice Manual 9-90.730 – Disclosure of Foreign Influence Operations.



are used to disseminate covert foreign government propaganda or disinformation, or to provide other covert support to political organizations or groups.”⁴ Any actions the companies may take in response to receiving information from FBI in this context are strictly voluntary.

(U) In 2019, bipartisan majorities of Congress recognized the threat to national security posed by FMI in Title 50, section 3369 of the United States Code titled, “Cooperative Actions to Detect and Counter Foreign Influence Operations,” which includes the finding that foreign actors have used the platforms provided by technology companies to engage in activities that threaten the United States, and will likely continue to do so. Specifically, Congress found that:

“(1) [a hostile power deployed] information warfare against the United States, its allies and partners, with the goal of advancing the strategic interests of the [hostile power]... (2) One line of effort deployed as part of these information warfare operations is the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion. (3) These information warfare operations are a threat to the national security of the United States and that of the allies and partners of the United States. As former Director of National Intelligence Dan Coats stated, “These actions are persistent, they are pervasive and they are meant to undermine America’s democracy . . . (7) Because these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms.”

(U) Congress stated in the same section that “it is the sense of Congress that information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations.”

(U//FOUO) In the fall of 2017, Director Wray established the FBI’s Foreign Influence Task Force (“FITF”) as a multi-division section comprised of operational and analytical personnel from the Counterintelligence Division, Cyber Division, and Criminal Investigative Division with the authority and mandate to combat FMI operations targeting U.S. democratic institutions.

(U//FOUO) One of FITF’s key lines of effort has been to “[l]ead the engagement with social media and Internet technology providers to enable an effective dialogue focused on 1) understanding and leveraging the visibility and capabilities of these providers, and 2) providing actionable direction to enable self-monitoring and mitigation efforts of those organizations’

⁴ Id.

platforms.”⁵(U) In 2022, the attorneys general of Missouri and Louisiana, who were eventually joined by a number of private plaintiffs, filed a lawsuit in the U.S. District Court for the Western District of Louisiana alleging that U.S. Government officials violated the First Amendment by “coercing” or “significantly encouraging” technology companies to remove, demote, or label certain content on their private-sector platforms. In July 2023, a federal district court issued a preliminary injunction that was later modified by the U.S. Court of Appeals for the Fifth Circuit. The injunction imposed certain restrictions on several departments and agencies, including the FBI, as well as certain officials in their official capacities. In October 2023, the U.S. Supreme Court agreed to hear the case and also stayed the injunction, eliminating the restrictions imposed by the injunction while the case is pending before the Court.

NSC REQUESTED REDACTION
[Redacted text block]

(U) The FBI Office of the General Counsel (“OGC”) has already provided guidance on engagement with social media platforms during the pendency of the litigation described above. See Attachment 2. This SOP supplements that guidance and provides procedures to be followed, in coordination with FITF, when an FBI employee seeks to share information regarding specific FMI activities or accounts, such as particular posts or uploads of videos, with Social Media Platforms. This SOP does not apply to general threat awareness briefings, or to

[Redacted text block]

communications regarding service of legal process, threats to life, or any other non-FMI activity, as otherwise covered in the November 4 guidance.

(U) Core Definitions and Principles:

(U//FOUO) **Foreign Malign Influence (FMI)** is **subversive, covert (or undeclared), coercive, or criminal** activities by foreign governments, nonstate actors, or their proxies designed to sow division, undermine democratic processes and institutions, or steer policy and regulatory decisions in favor of the foreign actors' strategic objectives and to the detriment of their adversaries.⁶

(U//FOUO) **Subversive Influence** means FMI activity aimed at undermining or overthrowing elements of, or the entirety of, a government or political system.

(U//FOUO) **Covert (or Undeclared) Influence** means foreign influence efforts whose nexus to a foreign government, foreign political party, and/or foreign entity is deliberately obscured, hidden, or misrepresented.

(U//FOUO) **Coercive Influence** activities can include foreign actors' threats or use of violence or litigation, or economic coercion, such as denying access to strategically important resources.

(U//FOUO) **Criminal Influence** activities involve violations of U.S. Federal criminal laws during foreign influence operations/campaigns.⁷

(U) Standard Operating Procedures:

(U//FOUO) FBI employees may provide information regarding FMI activities to Social Media Platforms where the following conditions are satisfied:

1. (U//FOUO) The employee determines whether the activities are being conducted covertly by, on behalf of, or pursuant to instruction from a foreign government and/or actor and in support of an FMI operation.

⁶ (U) See 50 USC Section 3059(f)(2) ("The term 'foreign malign influence' means any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means – (A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States.")

⁷ (U//FOUO) **Foreign influence** can be malign, as described above, but can also be conducted through overt or diplomatic channels which do not typically hide the association with a foreign government. Examples include language and cultural exchanges, official government statements, delegation visits and diplomatic engagements, and trade and commerce. This is not the type of activity the FBI is charged with investigating and will not form the basis for providing any type of warning to a technology company.

2. (U//FOUO) The employee identifies specific, credible, and articulable facts that provide high confidence⁸ for assessing that the activity is attributed to a foreign government, foreign nonstate actor or their proxy engaged in FMI.
3. (U//FOUO) The employee records all of the above information in an appropriate system of records that can be referenced in the details section of a dissemination EC. Serialize all approved ECs to a case number as detailed below.
4. (U//FOUO) FITF, in coordination and deconfliction with relevant partners, drafts a version of the information ("tearline"), sanitized in order to protect sources and methods, for dissemination to relevant recipients. The tear line must contain the following caveat:

Please note that no adverse action will be taken by the FBI based on your company's decision about whether or how to respond to this information. Indeed, the FBI does not request or expect your company to take any particular action regarding this information other than holding it in confidence due to its sensitive nature. The FBI is providing the below information about accounts or identifiers believed with high confidence to be using your platform to engage in foreign malign influence activity based on data we have obtained about the likely underlying user of the account(s), and not based on any statements, posts or comments made by the account(s). The FBI does not conduct its investigative activities or base attribution solely on activities protected by the First Amendment. Your company has no obligation to respond or provide information back to FBI in response to this engagement, but it is free to do so if it chooses. If, after reviewing the information, your company decides to provide referral information to the FBI, it must do so consistent with federal law.

5. (U//FOUO) The employee routes the dissemination through a designated attorney(s) in the National Security & Cyber Law Branch ("NSCLB") for prior review, obtains approval from the FITF Section Chief ("SC"), and then assigns a lead to the appropriate field office ("FO") National Security or Cyber ASAC to provide the tearline to individual Social Media Platforms.

6. (U//FOUO) Once approved by NSCLB and FITF SC, the FO uploads the tearline to Teleporter, an FBI-controlled data-sharing repository, ensuring that the capability to view whether the file was accessed is disabled. The FBI shall not attempt to discern whether a company viewed a particular hyperlink without NSCLB approval (for example, in the event that there was a system malfunction). The FO will then share the unique hyperlink to the tearline via an email to the relevant Social Media Platform(s). The email communication with the hyperlink shall say:

The FBI is making information available to your company. That information is available [here]. The FBI will not know whether your company accesses this link, but we may contact you to ensure that the system is functional. The information will be available for [x] days. If your company no longer wishes to receive this information, please reply to this email and we will remove you from this repository.

Please note that no adverse action will be taken by the FBI based on your company's decision about whether or how to respond. Indeed, the FBI does not request or expect your company to take any particular action regarding this information other than holding it in confidence due to its sensitive nature. The FBI is providing the below information about accounts or identifiers believed with high confidence to be using your platform to engage in foreign malign influence activity based on data we have obtained about the likely underlying user of the account(s), and not based on any statements, posts or comments made by the account(s). The FBI does not conduct its investigative activities or base attribution solely on activities protected by the First Amendment. Your company has no obligation to respond or provide information back to FBI in response to this information but it is free to do so if it chooses. If, after reviewing the information, your company decides to provide referral information to the FBI, it must do so consistent with federal law.

If you have any questions, please reach out to [insert contact name, phone number, and appropriate FBI email address].

- a. (U//FOUO) The communication with the social media provider and the dissemination of the hyperlink must be serialized to one of the following appropriate case files:

████████████████████████████████████████████████████████████████████████████████

████████████████████████████████████████████████████████████████████████████████

████████████████████████████████████████████████████████████████████████████████

- b. (U//FOUO) The FBI may not affirmatively follow-up with the Social Media Platform to relay the information in the tearline in any other manner without NSCLB approval or to inquire what, if any, action the social media company has taken. Proposed responses to questions or requests for additional information from the Social Media Platform following their review of the tearline must be approved by OGC.
- c. (U//FOUO) Meetings with Social Media Platforms that will result in FBI sharing information about specific content or accounts on a company's social media platform or that relate in any way to content moderation must be preapproved by NSCLB, and must be conducted in accordance with OGC's November 4, 2023, guidance on engagement with social media platforms during the pendency of the litigation described above.
7. (U//FOUO) Should a Social Media platform proactively reach out to an FBI FO, agents may meet with the Social Media Platform employees solely to receive information, in accordance with OGC's November 4, 2023, guidance. Records of such engagements should be documented in the appropriate case file identified above.

Prepared by the Foreign Influence Task Force Section in consultation with the Office of the General Counsel



**THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION:
AN AGENCY'S OVERREACH TO HARASS ELON MUSK'S TWITTER**

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 7, 2023

EXECUTIVE SUMMARY

Freedom of speech is among the most important rights guaranteed to every American. Elon Musk’s acquisition of Twitter last year served to revitalize this fundamental freedom in the digital age. Now, in wake of this acquisition, the Federal Trade Commission (FTC) is orchestrating an aggressive campaign to harass Twitter and deluge it with demands about its personnel decisions in each of the company’s departments, every internal communication relating to Elon Musk, and even Twitter’s interactions with journalists. These demands have no basis in the FTC’s statutory mission and appear to be the result of partisan pressure to target Twitter and silence Musk.

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.”¹ As part of this responsibility, and consistent with the Committee’s oversight responsibilities of the FTC, the Committee has been conducting oversight of the unusual response by the FTC to Musk’s acquisition of Twitter last year.² While the Committee and its Select Subcommittee continue to investigate these issues, this interim staff report fulfills the Committee’s ongoing obligation to identify and report on the weaponization of the federal government.³

The Committee recently obtained new, nonpublic information that falls directly within the Committee’s mandate to investigate and report on instances of the federal government’s authority being weaponized against U.S. citizens. Consisting of over a dozen FTC letters to Twitter that—in the span of less than three months following Musk’s acquisition—make more than 350 specific demands, this information shows how the FTC has been attempting to harass Twitter and pry into the company’s decisions on matters outside of the FTC’s mandate.

The timing, scope, and frequency of the FTC’s demands to Twitter suggest a partisan motivation to its action. When Musk took action to reorient Twitter around free speech, the FTC regularly followed soon thereafter with a new demand letter. The ostensible legal basis for the demand letters—including monitoring Twitter’s privacy and information security program under a revised consent decree between the company and the FTC⁴—fails to provide adequate cover for the FTC’s action. A number of the FTC’s demands have little to no nexus to users’ privacy and information. For example, the FTC has demanded that Twitter provide, among other things:

- Information relating to journalists’ work protected by the First Amendment, including their work to expose abuses by Big Tech and the federal government;⁵

¹ H.R. Res. 12, § 1(b)(D) 118th Cong. (2023) (enacted) (attached hereto as App. 1).

² See Letter from Ranking Member Jim Jordan to FTC Chair Lina Khan (May 4, 2022) (attached hereto as App. 2); Letter from Congressman Scott Fitzgerald, Ranking Member Jim Jordan, and others to FTC Chair Lina Khan (May 24, 2022) (attached hereto as App. 3).

³ See H.R. Res. 12, *supra* n.1.

⁴ *Twitter, Inc.*, Decision and Order, C-4316, FTC (May 26, 2022) (attached hereto as App. 4) (hereinafter “FTC Order”); see also *United States v. Twitter, Inc.*, No. 3:22-cv-3070 (N.D. Cal. May 26, 2022), ECF No. 11 (Stipulated Order) (attached hereto as App. 5).

⁵ Request 1, Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Dec. 13, 2022).

- Every single internal communication “relating to Elon Musk,” by any Twitter personnel—including communications sent or received by Musk—not limited by subject matter, since the day Musk bought the company;⁶
- Information about whether Twitter is “selling its office equipment”;⁷
- All of the reasons why Twitter terminated former Twitter employee and FBI official Jim Baker;⁸
- When Twitter “first conceived of the concept for Twitter Blue,” Twitter’s new \$8/month verified account subscription;⁹ and
- Information disaggregated by “each department, division, and/or team,” regardless of whether the work done by these units had anything to do with privacy or information security.¹⁰

The Committee does not dispute that protecting user privacy and mitigating information security risks are important duties. Because of its consent decree with Twitter, the FTC has the authority to monitor how Twitter is protecting users’ private information, such as their phone numbers and email addresses.¹¹ But the FTC is currently imposing some demands on Twitter that have no rational basis in user privacy. There is no logical reason, for example, why the FTC needs to know the identities of journalists engaging with Twitter. There is no logical reason why the FTC, on the basis of user privacy, needs to analyze all of Twitter’s personnel decisions. And there is no logical reason why the FTC needs every single internal Twitter communication about Elon Musk.

* * *

The strong inference from these facts is that Twitter’s rediscovered focus on free speech is being met with politically motivated attempts to thwart Elon Musk’s goals. The FTC’s demands did not occur in a vacuum. They appear to be the result of loud voices on the left—including elected officials—urging the federal government to intervene in Musk’s acquisition and management of the company. The FTC’s harassment of Twitter is likely due to one fact: Musk’s self-described “absolutist” commitment to free expression in the digital town square.

⁶ Request 17, Letter FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 30, 2022); *see also* Request 1, Letter from FTC Staff Attorney, FTC Division of Enforcement to Twitter’s Head of Product, Legal, *Twitter, Inc.*, No. C-4316 (Feb. 1, 2023) (same).

⁷ Request 13, FTC Letter (Dec. 13, 2022), *supra* n.5.

⁸ Request 4, Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Dec. 9, 2022).

⁹ Request 8(d), Letter from FTC Staff Attorney, FTC Division of Enforcement Regarding Twitter Blue and Resignations to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 10, 2022); *see also* Request 3(d), Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 21, 2022) (request for when Twitter “first conceived of the concept for Blue Verified”).

¹⁰ Request 1, FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; Request 1, Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter Regarding Terminations, *Twitter, Inc.*, No. C-4316 (Nov. 10, 2022).

¹¹ *See* FTC Order, *supra* n.4.

TABLE OF CONTENTS

Executive Summary	1
Table of Contents	3
I. The FTC’s Harassment Campaign against Twitter.....	4
A. The FTC’s Demands about the Twitter Files and Journalist Interactions	5
B. The FTC’s Demands about Twitter Blue and the Company’s Revenue Streams	8
C. The FTC’s Demands for All Elon Musk-related Communications and Other Inappropriate Demands.....	10
D. The FTC’s Reliance on Its Existing Consent Decree Is a Pretext to Harass Twitter	11
II. The FTC’s Actions Appear to be the Result of Left-wing Pressure	14
III. Conclusion	18
Appendix.....	19

I. THE FTC'S HARASSMENT CAMPAIGN AGAINST TWITTER

On April 25, 2022, Elon Musk announced his intention to buy Twitter.¹² Previously describing himself as a free speech absolutist,¹³ Musk proclaimed at the time: “Free speech is the bedrock of a functioning democracy, and Twitter is the digital town square where matters vital to the future of humanity are debated.”¹⁴



Elon Musk completed his acquisition of Twitter on October 27, 2022.¹⁵ Just two weeks later, the FTC launched the first of over a dozen demand letters to the company.¹⁶ Between just November 10 and January 18, the FTC issued over 350 requests—an average of roughly 35 requests per week.¹⁷ The FTC’s demand letters often followed shortly after Musk took a step that was controversial to activists on the left.¹⁸ While aspects of the FTC’s demands of Twitter may have had some plausible relevance to Twitter’s compliance with the consent decree, several demands did not. In addition, the scope, timing, and volume of the requests, following substantial left-wing pressure to use the consent decree to go after Musk, strongly support an inference that the motivation of many of the demands is political.

¹² *Elon Musk to Acquire Twitter* (provided by Twitter, Inc.), PR NEWswire (Apr. 25, 2022), <https://www.prnewswire.com/news-releases/elon-musk-to-acquire-twitter-301532245.html>; see Elon Musk (@elonmusk), TWITTER (Apr. 25, 2022, 3:43 PM), <https://twitter.com/elonmusk/status/1518677066325053441?lang=en>.

¹³ See, e.g., Elon Musk (@elonmusk), TWITTER (Mar. 5, 2022, 12:15 AM), <https://twitter.com/elonmusk/status/1499976967105433600?lang=en>; see also Dan Milno, *How ‘free speech absolutist’ Elon Musk would transform Twitter*, THE GUARDIAN (Apr. 14, 2022).

¹⁴ Elon Musk (@elonmusk), TWITTER (Apr. 25, 2022), *supra* n.12; *Elon Musk to Acquire Twitter*, PR NEWswire, *supra* n.12.

¹⁵ Billy Perrigo, *Elon Musk Finalizes Deal to Buy Twitter*, TIME (Oct. 27, 2022).

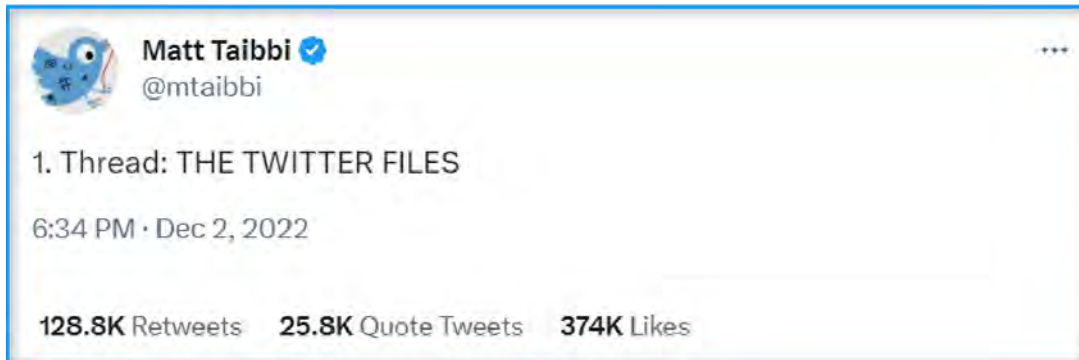
¹⁶ FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.

¹⁷ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10; Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 15, 2022); FTC Letter (Nov. 21, 2022), *supra* n.9; FTC Letter (Nov. 30, 2022), *supra* n.6; Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Dec. 6, 2022); FTC Letter (Dec. 9, 2022), *supra* n.8; FTC Letter (Dec. 13, 2022), *supra* n.5; Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Jan. 3, 2023); Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Jan. 18, 2023).

¹⁸ Cf. Elon Musk (@elonmusk), TWITTER (Nov. 19, 2022, 7:53 PM), <https://twitter.com/elonmusk/status/1594131768298315777> (“Trump will be reinstated.”); FTC Letter (Nov. 21, 2022), *supra* n.9.

A. The FTC’s Demands about the Twitter Files and Journalist Interactions

On December 2, 2022, journalist Matt Taibbi published the first edition of the Twitter Files, a series of reports documenting how Twitter was previously used by government actors to censor speech online.¹⁹ On December 10, Musk tweeted that “Twitter is both a social media company and a crime scene.”²⁰ Three days later, on 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.²¹



¹⁹ Matt Taibbi (@mtaibbi), TWITTER (Dec. 2, 2022, 6:34 PM), <https://twitter.com/mtaibbi/status/1598822959866683394?lang=en>.

²⁰ Elon Musk (@elonmusk), TWITTER (Dec. 10, 2022, 2:56 PM), <https://twitter.com/elonmusk/status/1601667312930590721?lang=en>.

²¹ Request 1, FTC Letter (Dec. 13, 2022), *supra* n.5.

The Twitter Files are a series of eighteen reports,²² and counting, that began soon after Elon Musk acquired Twitter. The most recent edition was published on March 2.²³ Twitter allowed the journalists, as part of their reporting on government censorship by proxy, to review internal communications and correspondence between Twitter employees and federal agencies, including the Federal Bureau of Investigation.²⁴ The journalists' reporting did *not* concern private user data or information that Twitter users wanted private. Quite the opposite, the reporting in the Twitter Files concerned content that users attempted to publicly share but that the government had pressured Twitter to restrict.²⁵



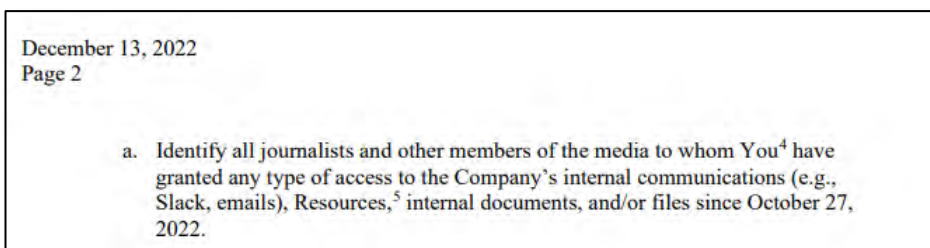
²² See Matt Taibbi (@mtaibbi), TWITTER (Dec. 2, 2022), *supra* n.19; Bari Weiss (@bariweiss) TWITTER (Dec. 8, 2022, 7:15 PM), https://twitter.com/bariweiss/status/1601007575633305600?s=20&t=ilqbULreQtFhJ_mVOCOoQ; Matt Taibbi (@mtaibbi), TWITTER (Dec. 9, 2022, 6:04 PM), <https://twitter.com/mtaibbi/status/1601352083617505281>; Michael Shellenberger (@ShellenbergerMD), TWITTER (Dec. 10, 2022, 6:28 PM), <https://twitter.com/ShellenbergerMD/status/1601720455005511680?s=20&t=jppprcOnLGDKC426tJ0uLA>; Bari Weiss (@bariweiss) TWITTER (Dec. 12, 2022, 1:06 PM), <https://twitter.com/bariweiss/status/1602364197194432515?s=20&t=6Ub9NU39Uhx1rOQdqf9f6g>; Matt Taibbi (@mtaibbi), TWITTER (Dec. 16, 2022, 4:00 PM), <https://twitter.com/mtaibbi/status/1603857534737072128?s=20&t=jOrUd1Ta8GPNhq1XVwZBLw>; Michael Shellenberger (@ShellenbergerMD), TWITTER (Dec. 19, 2022, 11:09 AM), <https://twitter.com/ShellenbergerMD/status/1604871630613753856?s=20&t=eCTz19ucVpfiKlo-pgwLQ>; Lee Fang (@lhfang), TWITTER (Dec. 20, 2022, 3:02 PM), <https://twitter.com/lhfang/status/1605292454261182464?s=20&t=SGeGDuZZN9eZ7cYVGnHOXQ>; Matt Taibbi (@mtaibbi), TWITTER (Dec. 24, 2022, 12:20 PM), https://twitter.com/mtaibbi/status/1606701397109796866?s=20&t=K5THm_CCLPrRig6XIFli7g; David Zweig (@davidzweig), TWITTER (Dec. 26, 2022, 9:10 AM), <https://twitter.com/davidzweig/status/1607378386338340867?s=20&t=NiuAY7UaXXiefwZN7e66LQ>; Matt Taibbi (@mtaibbi), TWITTER (Jan. 3, 2023, 3:27 PM), <https://twitter.com/mtaibbi/status/1610372352872783872?s=20&t=37uOcXgrG6IapxEIoRWvkQ>; Matt Taibbi (@mtaibbi), TWITTER (Jan. 3, 2023, 4:54 PM), <https://twitter.com/mtaibbi/status/1610394197730725889?s=20&t=j4oONRN5hwxTyNfGn1-s6A>; Alex Berenson (@AlexBerenson), TWITTER (Jan. 9, 2023, 2:08 PM), https://twitter.com/AlexBerenson/status/1612526697038897167?s=20&t=DhQ_5IksIhwChTWhfogB5Q; Matt Taibbi (@mtaibbi), TWITTER (Jan. 12, 2023, 12:29 PM), <https://twitter.com/mtaibbi/status/1613589031773769739?s=20&t=G4k4hjes88Bq235wSl3QIA>; Lee Fang (@lhfang), TWITTER (Jan. 16, 2023, 10:30 AM), <https://twitter.com/lhfang/status/1615008625575202818?s=20&t=c2a6Ez2nx5i-yrFEimrpQw>; Matt Taibbi (@mtaibbi), TWITTER (Jan. 27, 2023, 12:49 PM), <https://twitter.com/mtaibbi/status/1619029772977455105?s=20&t=YXrgzXGKpBZl0jBLxFOxSw>; Matt Taibbi (@mtaibbi), TWITTER (Feb. 18, 2023, 7:13 PM), <https://twitter.com/mtaibbi/status/1627098945359867904?lang=en>; Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), <https://twitter.com/mtaibbi/status/1631338650901389322>.

²³ Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023), *supra* n.22.

²⁴ *Matt Taibbi REVEALS Future Twitter Files Releases | Breaking Points*, YOUTUBE (Dec. 15, 2022), <https://www.youtube.com/watch?v=gExHIgWqDSo> (discussing access provided, how it has evolved, and noting that the journalists did not have “global access to every single document”).

²⁵ See, e.g., Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023), *supra* n.22 (describing how entities funded by the federal government requested Twitter to take down thousands of “inauthentic” accounts that belonged to real Americans).

Tellingly, the FTC’s first demand in its letter sent after the initial installment of the Twitter Files did not concern what private user information may have been at risk. Instead, the FTC demanded that Twitter “[i]dentify all journalists and other members of the media to whom” Twitter has granted access to since Musk bought the company.²⁶ The FTC even named some of the specific journalists—“Bari Weiss, Matt Taibbi, Michael Shellenberger, [and] Abigail Shrier”—with whom Twitter has engaged on the Twitter Files.²⁷ The FTC also demanded to know any “other members of the media to whom You have granted any type of access to the Company’s internal communications” for any reason whatsoever.²⁸



There is no reason the FTC needs to know every journalist with whom Twitter was engaging. Even more troubling than the burden on the company, the FTC’s demand represents a government inquiry into First Amendment-protected activity. It is an agency of the federal government demanding that a private company reveal the names of the journalists who are engaged in reporting about matters of public interest, including potential government misconduct. While the FTC’s inquiry would be inappropriate in any setting, it is especially inappropriate in the context of journalists disclosing how social media companies helped the government to censor online speech.

²⁶ Request 1, FTC Letter (Dec. 13, 2022), *supra* n.5.

²⁷ *Id.*

²⁸ *Id.*, Request 1(a) (footnote omitted).

B. The FTC’s Demands about Twitter Blue and the Company’s Revenue Streams

Many of the FTC’s demands relate to Twitter Blue, an \$8-per-month subscription service that provides Twitter a revenue stream separate from its advertising revenue.²⁹ After Musk announced his intention to buy Twitter in April 2022 and continuing after the acquisition was completed in October, activists on the left called for companies to stop advertising on Twitter.³⁰ Some speculated, if not cheered on, Twitter’s predicted financial demise.³¹



²⁹ See, e.g., FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter (Nov. 21, 2022), *supra* n.9; FTC Letter (Nov. 30, 2022), *supra* n.6; see also James Surowiecki, *Why Elon Musk Is Blowing Up Twitter’s Business*, THE ATLANTIC (Nov. 18, 2022).

³⁰ See, e.g., Glorinda Rodriguez, *Activists put pressure on advertisers to drop Twitter ads over Musk takeover, employee layoffs*, ABC NEWS (Nov. 4, 2022); Letter from Accountable Tech and others to Twitter’s Advertisers (May 3, 2022) (attached hereto as App. 6); *Calling on Advertisers to Pause Their Spend on Twitter*, STOP HATE FOR PROFIT (Nov. 4, 2022) (“[W]e are calling on advertisers to pause their spend globally until it becomes clear whether Twitter remains committed to being a safe place for advertisers as well as society overall.”).

³¹ See, e.g., Alex Kirshner, *The Advertising Industry Is Bringing Elon Musk to His Knees*, THE ATLANTIC (Nov. 8, 2022); Naomi Nix and Jeremy B. Merrill, *Advertisers are dropping Twitter. Musk can’t afford to lose any more.*, WASH. POST (Nov. 22, 2022); Halisia Hubbard, *Twitter has lost 50 of its top 100 advertisers since Elon Musk took over, report says*, NPR (Nov. 25, 2022); Suzanne Vranica, Patience Haggin, and Alexa Corse, *Elon Musk’s Campaign to Win Back Twitter Advertisers Isn’t Going Well*, WALL ST. J. (Dec. 22, 2022).

On October 27, Musk completed his purchase of Twitter and began to reshape Twitter's focus and its workforce.³² A few days later, Twitter announced the roll-out of its new subscription service, Twitter Blue.³³ On November 10, the FTC sent two demand letters asking for voluminous information about Twitter's personnel actions—terminations and resignations—and about the Twitter Blue service.³⁴ To date, the FTC has submitted nearly 60 requests related to Twitter Blue.³⁵ Some of the FTC's demands about Twitter Blue—such as when the service was “first conceived”—appear to serve little purpose other than to pile on to the already burdensome requests.³⁶ One such demand came just two days after Twitter reactivated President Trump's account.³⁷ In this letter, the FTC demanded nearly twenty additional categories of information about Twitter Blue.³⁸



³² Thomas Barrabi and Theo Wayt, *Elon Musk completes \$44B Twitter takeover, begins firing execs*, N.Y. POST (Oct. 27, 2022).

³³ Elon Musk (@elonmusk), TWITTER (Nov. 1, 2022, 1:36 PM), <https://twitter.com/elonmusk/status/1587498907336118274>.

³⁴ FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.

³⁵ FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter (Nov. 21, 2022), *supra* n.9; FTC Letter (Nov. 30, 2022), *supra* n.6; FTC Letter (Dec. 6, 2022), *supra* n.17; FTC Letter (Dec. 9, 2022), *supra* n.8; FTC Letter (Dec. 13, 2022), *supra* n.5.

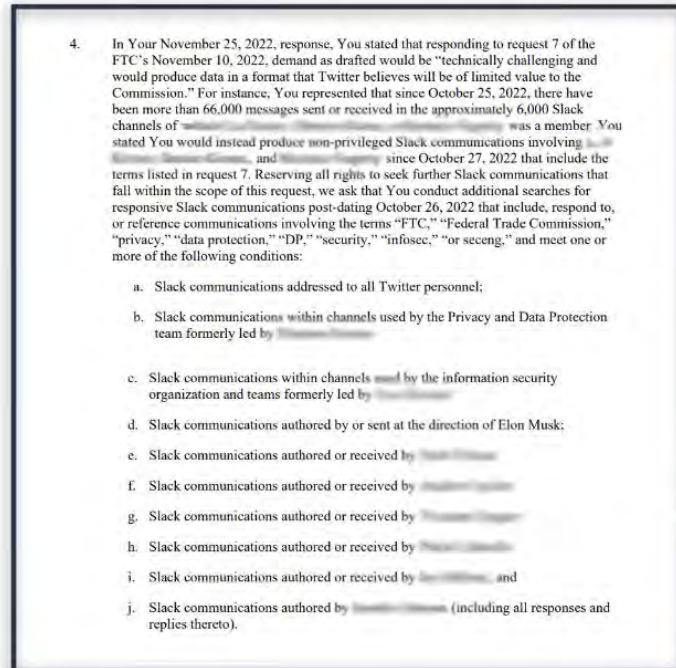
³⁶ See, e.g., Request 8(d), FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; see also Request 3, FTC Letter (Nov. 21, 2022) (request for when Twitter “first conceived of the concept for Blue Verified”), *supra* n.9.

³⁷ Cf. Elon Musk (@elonmusk), TWITTER (Nov. 19, 2022, 7:53 PM), <https://twitter.com/elonmusk/status/1594131768298315777> (“Trump will be reinstated.”); FTC Letter (Nov. 21, 2022), *supra* n.9.

³⁸ See FTC Letter (Nov. 21, 2022), *supra* n.9.

C. The FTC’s Demands for All Elon Musk-related Communications and Other Inappropriate Demands

In total, the FTC has now sent Twitter well over a dozen demand letters since Musk acquired the company.³⁹ These letters include demands for both written narratives and document productions.⁴⁰ In one 10-week stretch, the FTC averaged one new letter and 35 new requests per week.⁴¹ In addition to their frequency, the breadth of many of these demands make them particularly—perhaps intentionally—burdensome.



For example, on November 30, the FTC demanded that Twitter produce every internal Twitter communication—“including but not limited to emails, memos, and Slack communications”—“relating to Elon Musk,” including all communications sent or received by Musk himself.⁴² This demand came after the FTC had already asked for all communications for three employees in one request⁴³ and eight search terms in another request for just Slack communications.⁴⁴ Based on a subsequent FTC letter to Twitter, it appears that the company combined the requests (i.e., limiting its search by the three custodians *and* the eight search terms *and* only Slack communications), which still produced more than 66,000 hits across 6,000 Slack channels.⁴⁵ This one example illustrates that the FTC’s collective demands presented a substantial burden on the company’s operations.

³⁹ See, e.g., *supra* n.17; Letter from FTC Staff Attorney, FTC Division of Enforcement to Twitter’s Head of Product, Legal, *Twitter, Inc.*, No. C-4316 (Jan. 23, 2023); FTC Letter (Feb. 1, 2023), *supra* n.6.

⁴⁰ *Id.*

⁴¹ See *supra* n.17.

⁴² Request 17, FTC Letter (Nov. 30, 2022), *supra* n.6; Request 1, FTC Letter (Feb. 1, 2023), *supra* n.6.

⁴³ Request 6, FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9.

⁴⁴ *Id.*, Request 7.

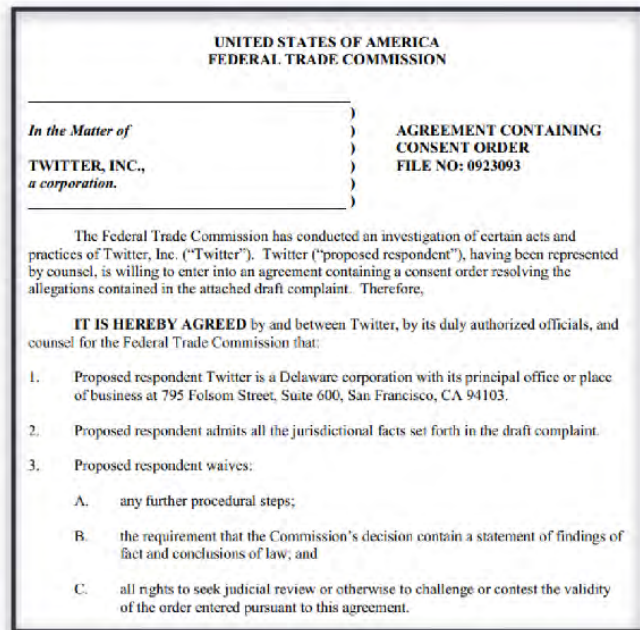
⁴⁵ See Request 4, FTC Letter (Dec. 6, 2022), *supra* n.17 (describing Twitter’s response dated November 25, 2022, and asking for additional communications from ten related sub-topics or custodians); see also *id.*, Request 3.

In other invasive demands, the FTC has demanded to know Twitter’s explanation for firing Jim Baker, a former FBI General Counsel who helped to censor the Hunter Biden laptop story on Twitter as a company executive in October 2020.⁴⁶ The FTC even demanded information about “whether, as part of its reduction in workforce or other cost-cutting measures, Twitter is also selling its office equipment.”⁴⁷



D. The FTC’s Reliance on Its Existing Consent Decree Is a Pretext to Harass Twitter

In 2022, FTC Chair Lina Khan claimed to the Committee the FTC “acts only in the public interest” and is “confined by [its] statutory authorities”⁴⁸ as the FTC considered whether to use its enforcement authority against Twitter in the wake of Musk’s potential acquisition of the company. The information obtained by the Committee makes clear that the FTC has inappropriately stretched its regulatory power to harass Twitter. The FTC is doing so consistent with the approach that partisan actors and interest groups have urged it to do: misusing a revised consent decree between the FTC and Twitter to justify its campaign of harassment.



⁴⁶ Request 4, FTC Letter (Dec. 9, 2022), *supra* n.8.

⁴⁷ Request 13, FTC Letter (Dec. 13, 2022), *supra* n.5.

⁴⁸ Response from FTC Chair Lina Khan to Ranking Member Jim Jordan (May 6, 2022) (attached hereto as App. 7).

In a 2011 consent agreement, Twitter settled claims that the company had improper safeguards against unauthorized access to users' personal information.⁴⁹ Twitter agreed to monitoring to ensure the platform maintained and protected user information in the future.⁵⁰ The limited nature of the settlement concerned "the security, privacy, and confidentiality of nonpublic consumer information."⁵¹ In a subsequent settlement in May 2022, Twitter paid a fine and agreed to implement a privacy and information security program by November 22, 2022, on account of violating the 2011 consent decree in this regard.⁵²

Twitter's May 2022 settlement concerned conduct that predated Musk's acquisition of Twitter and was limited in scope to the company's misuse of consumers' email addresses and phone numbers.⁵³ Like similar misconduct by Facebook, Twitter self-reported that it had collected consumers' telephone numbers and email addresses for security purposes, such as for account recovery or for two-factor authentication, but failed to disclose to users that it would also use that consumer information for targeted advertising.⁵⁴

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (e.g., two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

Although each of the counts against Twitter related only to this specific fact pattern,⁵⁵ the FTC's enforcement actions in wake of news of Musk's acquisition of Twitter have not been so limited. Just two weeks after Musk's acquisition, the FTC publicly announced that it was "tracking recent developments at Twitter with deep concern" and warned that the "revised

⁴⁹ Press Release, *FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information*, FTC (Mar. 11, 2011).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Press Release, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads*, FTC (May 25, 2022); see FTC Order, *supra* n.4; Stipulated Order, *supra* n.4.

⁵³ *Id.*

⁵⁴ *Concurring Statement of Commissioner Christine S. Wilson and Commissioner Noah Joshua Phillips*, Matter No. 2023062 (Twitter), FTC (May 25, 2022) ("Twitter allegedly collected telephone numbers and email addresses from consumers for security purposes, but then used that information for targeted advertisements") (attached hereto as App. 8); *but see Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter*, Matter No. 2023062 (Twitter), FTC (May 25, 2022) (attached hereto as App. 9).

⁵⁵ See *United States v. Twitter, Inc.*, No. 3:22-cv-3070 (N.D. Cal. May 26, 2022), ECF No. 1, at ¶¶ 60-75; see also *Concurring Statement of Commissioner Christine S. Wilson and Commissioner Noah Joshua Phillips*, *supra* n.54 ("This Twitter order includes a data use restriction tied to the core allegation of illegality in the complaint: the company may not use for advertising any phone numbers or email addresses that had been gathered for security purposes.").

consent order gives us new tools to ensure compliance, and we are prepared to use them.”⁵⁶ That same day, citing its consent decree with the company, the FTC began its barrage of demands of Twitter with two letters including over a dozen specific demands to the company.⁵⁷

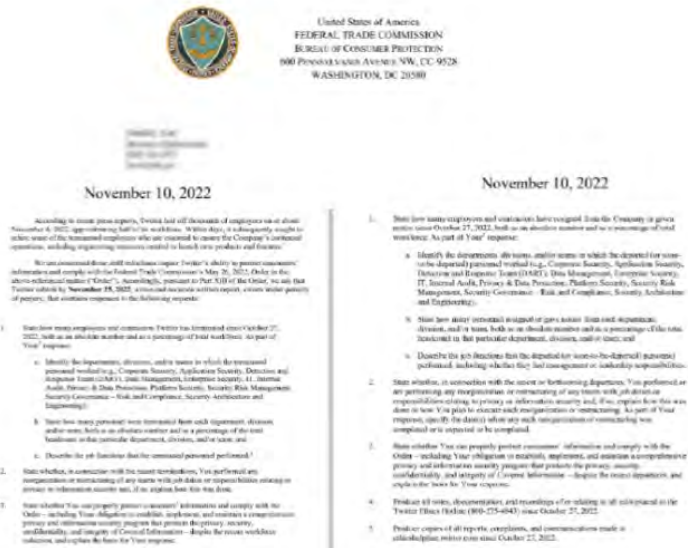
The timing of the FTC’s actions strongly suggests that its reliance on the consent decree is a pretext. Musk acquired Twitter on October 27, 2022.⁵⁸ Two weeks later, on November 10, the FTC sent two letters with over a dozen requests.⁵⁹ But Twitter’s new privacy and information security program—*i.e.*, the program ostensibly providing the main basis for the FTC’s demands—did not have to be established and implemented until November 22, per the terms of an FTC order from May 2022.⁶⁰



Federal Trade Commission
Public Comment

“We are tracking recent developments at Twitter with deep concern,” an FTC spokesperson said in a statement. “No CEO or company is above the law, and companies must follow our consent decrees. Our revised consent order gives us new tools to ensure compliance, and we are prepared to use them.”

November 10, 2022



United States of America
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION
100 PENNSYLVANIA AVENUE, N.W., CC-9528
WASHINGTON, DC 20580

November 10, 2022

November 10, 2022

In other words, the FTC started this heavy-handed compliance monitoring two weeks after Musk acquired Twitter, but two weeks before there was even a program in place to monitor. In fact, the FTC sent a total of four demand letters, which included over two dozen requests, before the deadline that the FTC imposed.⁶¹

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, **must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of such Covered Information.** To satisfy this requirement, Respondent must at a minimum:

⁵⁶ Brad Dress, *FTC says it’s ‘tracking the developments at Twitter with deep concern’*, THE HILL (Nov. 10, 2022).
⁵⁷ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.
⁵⁸ Thomas Barrabi and Theo Wray, *Elon Musk completes \$44B Twitter takeover, begins firing execs*, N.Y. POST (Oct. 27, 2022).
⁵⁹ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.
⁶⁰ See Sec. V, FTC Order, *supra* n.4.
⁶¹ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10; FTC Letter (Nov. 15, 2022), *supra* n.17; FTC Letter (Nov. 21, 2022), *supra* n.9.

II. THE FTC'S ACTIONS APPEAR TO BE THE RESULT OF LEFT-WING PRESSURE

Elon Musk's acquisition of Twitter, and his affirmation of online freedom of speech, generated an enormous amount of backlash among elected officials and activists on the left.⁶² In response to the acquisition, key voices on the left called for the federal government to intervene to "block" the purchase. Some groups, including the organization where FTC Chair Khan once worked, urged the FTC to use the existing consent decree with Twitter as a vehicle to attempt to thwart Musk's efforts to reorient the company. As this report shows, the FTC did just that.

The pressure campaign began almost immediately after Musk announced his interest in purchasing Twitter. Some in Congress criticized the planned acquisition and Musk's intention to allow more speech on the platform. In May 2022, then-Judiciary Committee Chairman Jerrold Nadler (D-NY) lamented Musk's proposed changes to content moderation, warning it would allow so-called "disinformation" to proliferate.⁶³ Congressman David Cicilline (D-RI), then-Chairman of the House Antitrust Subcommittee, criticized the acquisition, saying "there are a lot of reasons to be concerned."⁶⁴ Congresswoman Alexandria Ocasio-Cortez (D-NY) claimed without any evidence that Musk's takeover of Twitter would precipitate an "explosion of hate crimes."⁶⁵ Not to be outdone, Senator Elizabeth Warren (D-MA) decried the deal as "dangerous for our democracy."⁶⁶



⁶² See, e.g., Jordan Boyd, *The Left Is Freaking Out Over Elon Musk Because Twitter Rigs The Game For Democrats*, THE FEDERALIST (Apr. 14, 2022); Ben Weingarten, *Elon Musk's Battle For Twitter Is A Proxy War For Americans Against The Ruling Class*, THE FEDERALIST (Apr. 20, 2022); Brian Schwartz, *Biden officials worry Musk will allow Trump to return to Twitter*, CNBC (Apr. 25, 2022); Mike Lillis, *Democrats sound alarm about Musk bringing Trump back to Twitter*, THE HILL (May 13, 2022).

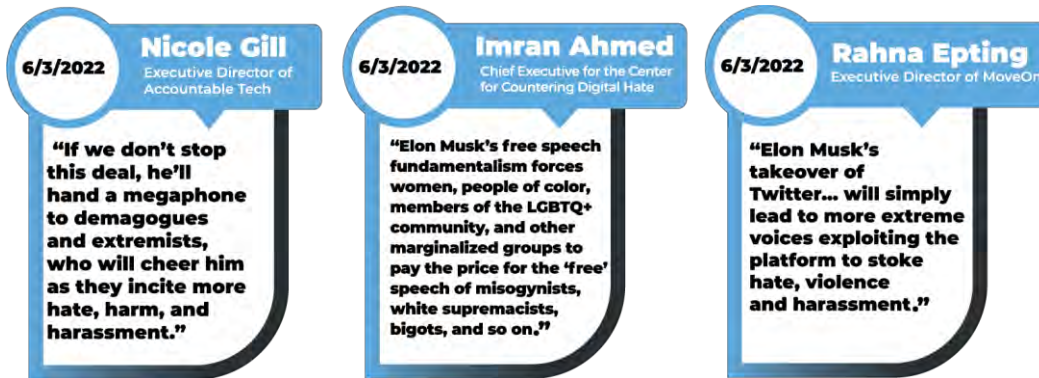
⁶³ Karl Herchenroeder, *Musk Twitter Deal Renews Partisan Debate Over Speech*, COMM'NS DAILY (May 2, 2022).

⁶⁴ *Antitrust Chair Cicilline on Big Tech Bill in Limbo*, BLOOMBERG (Aug. 22, 2022).

⁶⁵ Alexandria Ocasio-Cortez (@AOC), TWITTER (Apr. 29, 2022, 2:41 PM), <https://twitter.com/AOC/status/1520111152411389954>.

⁶⁶ Elizabeth Warren (@SenWarren), TWITTER (Apr. 25, 2022, 5:22 PM), <https://twitter.com/SenWarren/status/1518702084048179200>.

Organizations on the left immediately mobilized against Musk, creating a “Stop the Deal” website to serve as the hub for the “multi-pronged effort.”⁶⁷ This pro-censorship coalition mischaracterized Musk’s commitment to the First Amendment, warned of a parade of horrors, and initiated a litany of personal attacks, including:



These organizations demanded that the FTC and other federal agencies act quickly to prevent Musk’s acquisition of Twitter.⁶⁸

The Open Markets Institute (OMI), a left-wing political advocacy organization where current FTC Chair Lina Khan used to work,⁶⁹ urged regulators at the FTC to “block” the purchase.⁷⁰ At the time, Judiciary Committee Republicans investigated whether the FTC had inappropriate coordination with third parties about its response to Musk’s acquisition of Twitter, which the FTC denied.⁷¹ The FTC, however, refused to disclose its communications with the White House.⁷²

On October 27, 2022, Musk completed the purchase and officially became the CEO of Twitter.⁷³ Again, left-wing hysteria erupted immediately. OMI released a public statement claiming that Musk’s ownership of Twitter “poses a number of immediate and direct threats to American democracy, free speech, and national security.”⁷⁴ OMI asserted that “the deal violates existing law” and that the FTC and other regulators “have ample authority to block it.”⁷⁵ A few weeks later, OMI sent a letter to FTC Chair Khan, Jonathan Kanter, Assistant Attorney General

⁶⁷ *Stop The Deal: Nonprofit Coalition Launches Campaign Against Elon Musk’s Twitter Takeover*, ACCOUNTABLE TECH (June 3, 2022), <https://accountabletech.org/media/stop-the-deal-nonprofit-coalition-launches-campaign-against-elon-musks-twitter-takeover/>; see also Letter from Accountable Tech and others to Twitter’s Advertisers (May 3, 2022), *supra* n.30 (attached hereto as App. 6).

⁶⁸ *Id.*

⁶⁹ Nancy Scola, *How a liberal think tank is driving 2020 Dems to crack down on Big Tech*, POLITICO (June 14, 2019).

⁷⁰ See Barry Lynn, *OMI Statement on Elon Musk and Twitter*, OPEN MARKETS INSTITUTE (Apr. 26, 2022) (attached hereto as App. 10).

⁷¹ Response from FTC Chair Lina Khan to Ranking Member Jim Jordan (May 6, 2022) (attached hereto as App. 7).

⁷² Response from FTC Chair Lina Khan to Ranking Member Jim Jordan and others (June 24, 2022) (attached hereto as App. 11).

⁷³ Thomas Barrabi and Theo Wayt, *Elon Musk completes \$44B Twitter takeover, begins firing execs*, N.Y. POST (Oct. 27, 2022).

⁷⁴ Barry Lynn, *Open Markets Institute Statement in response to Elon Musk Buying Twitter*, OPEN MARKETS INSTITUTE (Oct. 27, 2022) (attached hereto as App. 12).

⁷⁵ *Id.*

of the Antitrust Division at the Department of Justice (DOJ), and Jessica Rosenworcel, Chair of the Federal Communications Commission (FCC), demanding that each of their offices “fully investigate Elon Musk’s takeover of the communications platform Twitter” because the U.S. government should be “using *every* existing authority” at its disposal.⁷⁶ OMI conceded that “FTC enforcement of its consent decree with Twitter on privacy” is “not sufficient,” and “that this deal does not fit easily into some of the categories your agencies have relied on in recent years to determine when and how to investigate takeovers or certain corporate actions”;⁷⁷ but OMI assured the FTC, DOJ, and the FCC that they have very “ample authority to fully review this takeover, and if necessary to unwind or restructure the deal and/or regulate the actions of the combined corporations.”⁷⁸

Another fourteen left-wing organizations—including the Center for American Progress, Common Cause, MoveOn, and Public Citizen—demanded that the FTC investigate whether Musk had already “violate[d] the company’s existing consent decree.”⁷⁹ Partisan activists agreed, publicly advocating that the consent decree provided sufficient legal grounds for the FTC to achieve the left’s political ends.⁸⁰



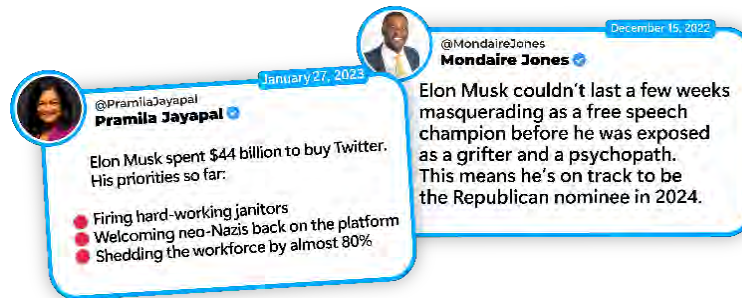
⁷⁶ Letter from OMI to FTC, DOJ, and FCC (Nov. 16, 2022) (emphasis in original) (attached hereto as App. 13).

⁷⁷ *Id.*

⁷⁸ *Id.* For good measure, OMI also noted that “[a]t least six other departments, agencies, and offices have a responsibility to work with [the FTC, DOJ, and the FCC] on a thorough investigation of Mr. Musk’s takeover and management of Twitter, and his management of Starlink: the Committee on Investment in the United States (CFIUS), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB), the Department of Defense, the Department of Treasury, and the Federal Reserve.”

⁷⁹ *The FTC, Congress, and Advertisers Must Hold Elon Musk and Twitter Accountable, Say Progressive Groups*, AMERICAN PROGRESS (Dec. 21, 2022) (attached hereto as App. 14).

⁸⁰ See, e.g., Brian Fung, *Musk’s Twitter may have already violated its latest FTC consent order, legal experts say*, CNN (Nov. 11, 2022).



Following the completed acquisition, Democrats in Washington renewed their pressure campaign.⁸¹ Seven Democrat senators issued a joint press release calling for the FTC to investigate Musk’s so-called “alarming steps” at Twitter.⁸² These senators demanded that the FTC “vigorously oversee its consent decree” with Twitter, and outlined the different purported grounds on which Elon Musk could have already violated the terms of the decree in his first few weeks of ownership.⁸³ Even President Biden signaled support for government intervention, saying that “there’s a lot of ways” the government could review the transaction.⁸⁴



While efforts to have other agencies “block” the deal failed,⁸⁵ the persistent, fever-pitched pressure campaign by left-wing activists and Democrats implored the FTC to use the user-privacy consent decree as a cudgel against Twitter. It appears that the FTC has done exactly that.

⁸¹ See, e.g., Pramila Jayapal (@PramilaJayapal), TWITTER (Jan. 27, 2023, 2:08 PM), <https://twitter.com/PramilaJayapal/status/1619049608960741381>; Mondaire Jones (@MondaireJones), TWITTER (Dec. 15, 2022, 10:13 PM), <https://twitter.com/MondaireJones/status/1603589202867884034>; *Klobuchar After Musk Takeover: Twitter Is 'Making Money Off Of This Violence'*, NBC News, YOUTUBE (Oct. 30, 2022)

<https://www.youtube.com/watch?v=UJRKDVyeHSU> (Senator Amy Klobuchar, Chair of the Senate Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights, stated after the acquisition that she did not trust Musk to run Twitter, and lamented that Musk was spreading “pro-Trump, [Make America Great Again]-crowd rhetoric).

⁸² Letter from Democratic Senators to FTC Chair Lina Khan (Nov. 17, 2022) (attached hereto as App. 15).

⁸³ *Id.*

⁸⁴ Rebecca Kern, *Musk's foreign investors in Twitter are 'worthy' of review, Biden says*, POLITICO (Nov. 9, 2022).

⁸⁵ In addition to the FTC, the FBI was also involved in reviewing the transfer of Twitter’s ownership, with officials looking “into the potential counterintelligence risks posed by the deal.” Faiz Siddiqui, Jeff Stein, and Joseph Menn, *U.S. exploring whether it has authority to review Musk’s Twitter deal*, WASH. POST (Nov. 2, 2022). And just days before the deal ultimately went through, there were reports that the Biden Administration would consider subjecting

III. CONCLUSION

Our democratic republic depends on American citizens having the right to express themselves freely in the town square, whether that forum is in person or in a digital space. As Justice Brandeis counseled almost a century ago, the best remedy for false speech is “more speech, not enforced silence.”⁸⁶ Elon Musk recognizes this truth and he has reshaped Twitter to revitalize freedom of speech online.

The FTC wields enormous authority to regulate large swaths of the modern American economy. The information presented in this interim staff report demonstrates the threat posed by wildly inappropriate use of this power. The FTC has no business demanding to know with which journalists a private company is communicating. The FTC has no need for all of Twitter’s communications related to its CEO. And yet, on the basis of an existing consent decree about user privacy, the FTC made these demands—and more—of Twitter. These demands should be exposed for what they are: pure and absolute attempts to harass, intimidate, and target an American business.

The Committee and the Select Subcommittee remain steadfast in our mission to investigate the weaponization of the federal government and to pursue legislative reforms to stop it.

the deal to review by the Committee on Foreign Investment in the United States (CFIUS), an interagency panel led by the Treasury Department, which involves DHS, the State Department, and the Defense Department, among others. Jennifer Jacobs and Saleha Mohsin, *Twitter Tumbles as US Weighs Security Reviews for Musk Deals*, BLOOMBERG (Oct. 20, 2022). This reporting was followed by Twitter’s stock plunging five percent and jeopardized the deal. *Id.* And even though, on November 15—weeks after the deal went through—Secretary of the Treasury Janet Yellen said “[w]e really have no basis – to the best of my knowledge – to examine [Musk’s] finances of his company” she had to walk back her statements, claiming on November 30 that “it would be appropriate for CFIUS to take a look” at the Twitter deal. Christopher Condon and Gregory Korte, *Janet Yellen changes course and says she ‘misspoke’ when she said there was ‘no basis’ for the government to review Elon Musk’s Twitter buy*, FORTUNE (Nov. 30, 2022).

⁸⁶ *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

APPENDIX

Appendix 1 – House Resolution 12, 118th Congress

Appendix 2 – May 4, 2022 Letter from Ranking Member Jim Jordan to FTC Chair Lina Khan

Appendix 3 – May 24, 2022 Letter from Congressman Scott Fitzgerald, Ranking Member Jim Jordan, et al. to FTC Chair Lina Khan

Appendix 4 – *In the Matter of Twitter, Inc.*, No. C-4316, FTC Decision and Order (May 2022)

Appendix 5 – *United States v. Twitter, Inc.*, No. 3:22-cv-3070 (N.D. Cal. May 26, 2022), ECF No. 11 (Stipulated Order)

Appendix 6 – May 3, 2022 Letter from Accountable Tech and others to Twitters’ Advertisers

Appendix 7 – May 6, 2022 Response from FTC Chair Lina Khan to Ranking Member Jim Jordan

Appendix 8 – FTC Matter No. 2023062 (Twitter), Concurring Statement of Commissioner Christine S. Wilson and Commissioner Noah J. Phillips

Appendix 9 – FTC Matter No. 2023062 (Twitter), Statement of Chair Lina M. Khan Joined by Commissioner Rebecca K. Slaughter

Appendix 10 – Statement from the Open Markets Institute (April 2022)

Appendix 11 – June 24, 2022 Response from FTC Chair Khan to Ranking Member Jim Jordan

Appendix 12 – Statement from the Open Markets Institute (Oct. 2022)

Appendix 13 – Nov. 16, 2022 Letter from the Open Markets Institute to FTC, DOJ, and FCC

Appendix 14 – Statement from Progressive Groups to the FTC, Congress, and Advertisers (Dec. 21, 2022)

Appendix 15 – Nov. 17, 2022 Letter from Democratic Senators to FTC Chair Khan

Appendix 1

.....
(Original Signature of Member)

118TH CONGRESS
1ST SESSION

H. RES.

Establishing a Select Subcommittee on the Weaponization of the Federal Government as a select investigative subcommittee of the Committee on the Judiciary.

IN THE HOUSE OF REPRESENTATIVES

Mr. JORDAN submitted the following resolution; which was referred to the Committee on _____

RESOLUTION

Establishing a Select Subcommittee on the Weaponization of the Federal Government as a select investigative subcommittee of the Committee on the Judiciary.

1 *Resolved,*

2 **SECTION 1. SELECT SUBCOMMITTEE ON THE**
3 **WEAPONIZATION OF THE FEDERAL GOVERN-**
4 **MENT.**

5 (a) ESTABLISHMENT; COMPOSITION.—

6 (1) ESTABLISHMENT.—There is hereby estab-
7 lished for the One Hundred Eighteenth Congress a
8 select investigative subcommittee of the Committee

1 on the Judiciary called the Select Subcommittee on
2 the Weaponization of the Federal Government (here-
3 inafter referred to as the “select subcommittee”).

4 (2) COMPOSITION.—

5 (A) The select subcommittee shall be com-
6 posed of the chair and ranking minority mem-
7 ber of the Committee on the Judiciary, together
8 with not more than 13 other Members, Dele-
9 gates, or the Resident Commissioner appointed
10 by the Speaker, of whom not more than 5 shall
11 be appointed in consultation with the Minority
12 Leader. The Speaker shall designate one mem-
13 ber of the select subcommittee as its chair. Any
14 vacancy in the select subcommittee shall be
15 filled in the same manner as the original ap-
16 pointment.

17 (B) Each member appointed to the select
18 subcommittee shall be treated as though a
19 member of the Committee on the Judiciary for
20 purposes of the select subcommittee.

21 (b) INVESTIGATIVE FUNCTIONS AND AUTHORITY.—

22 (1) INVESTIGATIVE FUNCTIONS.—The select
23 subcommittee is authorized and directed to conduct
24 a full and complete investigation and study and, not
25 later than January 2, 2025, issue a final report to

1 the House of its findings (and such interim reports
2 as it may deem necessary) regarding—

3 (A) the expansive role of Article II author-
4 ity vested in the Executive Branch to collect in-
5 formation on or otherwise investigate citizens of
6 the United States, including ongoing criminal
7 investigations;

8 (B) how executive branch agencies work
9 with, obtain information from, and provide in-
10 formation to the private sector, non-profit enti-
11 ties, or other government agencies to facilitate
12 action against American citizens, including the
13 extent, if any, to which illegal or improper, un-
14 constitutional, or unethical activities were en-
15 gaged in by the Executive Branch or private
16 sector against citizens of the United States;

17 (C) how executive branch agencies collect,
18 compile, analyze, use, or disseminate informa-
19 tion about citizens of the United States, includ-
20 ing any unconstitutional, illegal, or unethical
21 activities committed against citizens of the
22 United States;

23 (D) the laws, programs, and activities of
24 the Executive Branch as they relate to the col-
25 lection of information on citizens of the United

1 States and the sources and methods used for
2 the collection of information on citizens of the
3 United States;

4 (E) any other issues related to the viola-
5 tion of the civil liberties of citizens of the
6 United States; and

7 (F) any other matter relating to informa-
8 tion collected pursuant to the investigation con-
9 ducted under this paragraph at any time during
10 the One Hundred Eighteenth Congress.

11 (2) AUTHORITY.—

12 (A) The select subcommittee may report to
13 the House or any committee of the House from
14 time to time the results of its investigations and
15 studies, together with such detailed findings
16 and legislative recommendations as it may deem
17 advisable.

18 (B) Any markup of legislation shall be held
19 at the full Committee level consistent with
20 clause 1(l) of rule X of the Rules of the House
21 of Representatives.

22 (c) PROCEDURE.—

23 (1) Rule XI of the Rules of the House of Rep-
24 resentatives and the rules of the Committee on the
25 Judiciary shall apply to the select subcommittee in

1 the same manner as a subcommittee except as fol-
2 lows:

3 (A) The chair of the select subcommittee
4 may, after consultation with the ranking minor-
5 ity member, recognize—

6 (i) members of the select sub-
7 committee to question a witness for periods
8 longer than five minutes as though pursu-
9 ant to clause 2(j)(2)(B) of such rule XI;
10 and

11 (ii) staff of the select subcommittee to
12 question a witness as though pursuant to
13 clause 2(j)(2)(C) of such rule XI.

14 (B) The Committee on the Judiciary (or
15 the chair of the Committee on the Judiciary, if
16 acting in accordance with clause 2(m)(3)(A)(i)
17 of rule XI) may authorize and issue subpoenas
18 to be returned at the select subcommittee.

19 (C) With regard to the full scope of inves-
20 tigative authority under subsection (b)(1), the
21 select subcommittee shall be authorized to re-
22 ceive information available to the Permanent
23 Select Committee on Intelligence, consistent
24 with congressional reporting requirements for
25 intelligence and intelligence-related activities,

1 and any such information received shall be sub-
2 ject to the terms and conditions applicable
3 under clause 11 of rule X.

4 (2) The provisions of this resolution shall gov-
5 ern the proceedings of the select subcommittee in
6 the event of any conflict with the rules of the House
7 or of the Committee on the Judiciary.

8 (d) SERVICE.—Service on the select subcommittee
9 shall not count against the limitations in clause 5(b)(2)(A)
10 of rule X of the Rules of the House of Representatives.

11 (e) SUCCESSOR.—The Committee on the Judiciary is
12 the “successor in interest” to the select subcommittee for
13 purposes of clause 8(c) of rule II of the Rules of the House
14 of Representatives.

15 (f) SUNSET.—The select subcommittee shall cease to
16 exist 30 days after filing the final report required under
17 subsection (b).

Appendix 2

ONE HUNDRED SEVENTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6216
(202) 225-3951
judiciary.house.gov

May 4, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan:

The day after Twitter’s board of directors agreed to sell Twitter to Mr. Elon Musk, the Open Markets Institute (OMI), an extreme left-wing political advocacy organization,¹ called on Biden regulators at the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the Justice Department to “block” the purchase.² We are concerned that OMI—where you were previously employed as Legal Director³—may be trying to leverage its close relationship with you to take action to further limit free speech online. The author of OMI’s statement has called you a “dear friend,” a “close colleague,” and someone who “understands the nature of the crisis and how to use existing law and authority to master it.”⁴

¹ One commentator has noted that “OMI’s loudest voices are largely unencumbered by economic or legal education” Nancy Scola, *How a liberal think tank is driving 2020 Dems to crack down on Big Tech*, POLITICO (June 14, 2019), <https://www.politico.com/story/2019/06/14/open-market-institute-silicon-valley-monopolies-1507673>. And it has been reported that the author of OMI’s statement recently participated in the Antitrust Section Spring Meeting of the American Bar Association and “rattled off a list of social ills, including outsized influence of tech companies, environmental problems and wealth inequality.” Christine S. Wilson, *Marxism and Critical Legal Studies Walk into the FTC: Deconstructing the Worldview of the Neo-Brandeisians*, REMARKS FOR THE JOINT CONFERENCE ON PRECAUTIONARY ANTITRUST: THE RULE OF LAW AND INNOVATION UNDER ASSAULT 5 (Apr. 8, 2022) (citation omitted), https://www.ftc.gov/system/files/ftc_gov/pdf/Marxism%20and%20Critical%20Legal%20Studies%20Walk%20into%20the%20FTC%20Deconstructing%20the%20Worldview%20of%20the%20Neo-Brandeisians.pdf. He “told attendees that “[t]his all—to a great degree—[is] your doing. It is your doing because you conspired to use a false science, an idiot science, to blind the law to dangerous concentrations of power, to blind the citizenry to the fist of monopoly.” *Id.* (first alternation in original) (citation omitted).

² See generally Press Release, OMI Statement on Elon Musk and Twitter (Apr. 26, 2022), <https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/6268076a3b1aa57bfcdbd0487/1650984811013/OMI+Musk+and+Twitter.pdf>.

³ See Press Release, Lina Khan’s Confirmation as Commissioner on the Federal Trade Commission is Momentous (June 15, 2021), <https://www.openmarketsinstitute.org/publications/lina-khans-confirmation-as-commissioner-on-the-federal-trade-commission-is-momentous>.

⁴ *Id.*

The Honorable Lina Khan

May 4, 2022

Page 2

OMI claims without evidence that Mr. Musk’s purchase is a “threat to free communications and debate in the United States.”⁵ In reality, Mr. Musk has proposed “softening [Twitter’s] stance on content moderation,” which will increase speech, and he has said that “Twitter should be more cautious when deciding to take down tweets or permanently ban users’ accounts.”⁶ OMI’s desire to restrict and suppress free speech online helps explain why it supports a package of ill-advised Democrat-led antitrust bills that will lead to more censorship, and thus less speech, in the digital arena.⁷

OMI appears to believe that the FTC will be receptive to its cavalier effort to influence a federal agency that is run by its former employee. It is true that the Biden FTC is moving to promote progressive values that undermine capitalism and threaten innovation.⁸ And under your leadership, the Biden FTC has sought to “recast[] antitrust law into a tool to enable government to control capitalism,”⁹ which disrupts free markets and is inconsistent with fundamental American freedoms. Perhaps this is why OMI seems to think it may have a friendly ear in the FTC.

To assist the Committee in its oversight of the FTC, please provide a written response to the following questions:

1. Did you or anyone else at the FTC solicit or play any role in drafting OMI’s statement?
2. Has the FTC taken any actions in response to the statement released by OMI?

Please answer these questions as soon as possible but no later than 5:00 p.m. on May 18, 2022.

⁵ Press Release, *supra* note 2, at 2.

⁶ Cara Lombardo et al., *Twitter Accepts Elon Musk’s Offer to Buy Company in \$44 Billion Deal*, WALL ST. J. (Apr. 25, 2022).

⁷ See Press Release, Open Markets Applauds New Bipartisan Legislation to Rein in Big Tech as Important First Step (June 11, 2021), <https://www.openmarketsinstitute.org/publications/open-markets-applauds-new-bipartisan-legislation-to-rein-in-big-tech-as-important-first-step>; Rep. Jim Jordan & Mark Meadows, Opinion, *Rep. Jim Jordan & Mark Meadows: Big Tech merged with Big Government – radical Dems’ bills would transform US*, FOX NEWS (June 22, 2021) (“Make no mistake, Big Tech is out to get conservatives and must be reined in. But these bills do nothing to fight Big Tech’s anti-conservative bias and censorship. These Democrat bills will only make things worse. If you think Big Tech is bad now, just wait until Apple, Amazon, Facebook and Google are working in collusion with Big Government.”).

⁸ See, e.g., Draft FTC Strategic Plan for FY 2022-2026, FTC, at 21 (Oct. 2021) (listing the objective to “[a]dvance racial equity, and all forms of equity, and support underserved and marginalized communities through the FTC’s competition mission”); Bryan Koenig, *Nontraditional Questions’ Appearing In FTC Merger Probes*, LAW 360 (Sept. 24, 2021) (“[W]hen quizzed about the need for the less traditional input, ‘staff have been unable to articulate how these issues relate to the agency’s mission to promote competition, leaving the outside world guessing as to the role they play in agency decision making’” (citation omitted)), <https://www.law360.com/articles/1425218>.

⁹ Robert Bork Jr., *Why Free Thinkers Need to Block Lina Khan’s FTC Nomination*, REAL CLEAR MARKETS (June 15, 2021), https://www.realclearmarkets.com/articles/2021/06/15/why_free_thinkers_need_to_block_lina_khans_ftc_nomination_781419.html.

The Honorable Lina Khan

May 4, 2022

Page 3

Furthermore, this letter serves as a formal request to preserve all records and materials relating to Mr. Musk's pending acquisition of Twitter. 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 is or may be potentially 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.

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 style with a large, stylized "J" and "D".

Jim Jordan
Ranking Member

cc: The Honorable Jerrold L. Nadler, Chairman
The Honorable Noah J. Phillips, Commissioner, Federal Trade Commission
The Honorable Rebecca K. Slaughter, Commissioner, Federal Trade Commission
The Honorable Christine S. Wilson, Commissioner, Federal Trade Commission

Appendix 3

Congress of the United States
Washington, DC 20510

The Honorable Lina Khan
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

May 24, 2022

Dear Chair Khan:

We write to express concerns about the Federal Trade Commission's (FTC) approach to reviewing Elon Musk's \$44 billion purchase of Twitter given the recent politicization at the FTC.

Big Tech has been relentlessly attacking free speech over the past several years, and Twitter specifically has gained a reputation for heavy-handed censorship of conservative views that are not popular in Silicon Valley. These censorship activities undermine our country's First Amendment principles and poison public discourse. Mr. Musk has proposed reversing Twitter's harsh and one-sided content moderation policies and replacing them with a more measured approach that only removes clearly unlawful tweets and user accounts.¹

We are concerned that the politicization seen at the FTC during the Biden Administration will slow or even halt Twitter's moves toward more free speech under the leadership of Elon Musk. Since the start of the Administration, the Biden FTC has taken radical measures that abandon traditional procedures and norms of civility and bipartisanship, while pushing the limit of the statutory bounds Congress placed on it. Measures such as suspending early termination of merger review transactions with no competitive concerns for well over a year,² using a zombie vote to adopt prior approval for merging parties and divestiture buyers on future transactions for 10 years,³ and frequent use of pre-consummation warning letters have damaged the FTC's reputation as an unbiased enforcement agency.⁴

¹ Elon Musk, Twitter post, April 26, 2022, 3:33 p.m.,

<https://twitter.com/elonmusk/status/1519036983137509376?s=20&t=PB7uC6fFnUJHXjd5ZCtFA>.

² Press Release, Fed. Trade Comm'n, FTC, DOJ Temporarily Suspend Discretionary Practice of Early Termination (Feb. 4, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/02/ftc-doj-temporarily-suspend-discretionary-practice-early-termination>.

³ Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Statement of the Commission on Use of Prior Approval Provisions in Merger Orders (Oct. 29, 2021), https://www.ftc.gov/system/files/documents/public_statements/1598095/wilson_phillips_prior_approval_dissenting_statement_102921.pdf.

⁴ Holly Vedova, Dir., Bureau of Competition, Adjusting merger review to deal with the surge in merger filings, FED. TRADE COMM'N COMPETITION MATTERS BLOG (Aug. 3, 2021), <https://www.ftc.gov/enforcement/competition-matters/2021/08/adjusting-merger-review-deal-surge-merger-filings>.

Even worse, the lack of transparency surrounding withdrawn enforcement guidance without replacing it with new rules of the road and moving away from the traditional “consumer welfare standard⁵” have led to fears of politicization of the FTC. These fears are validated when the FTC appears to take direction from the White House and partisan third-party organizations. Just a few months ago, the FTC heeded the White House’s call to investigate oil and gas companies for price gouging to distract from the Administration’s own policies that clamp down on domestic production.⁶ Even more recently, the Open Markets Institute’s call to block Mr. Musk’s purchase of Twitter coincided with your own investigation of the deal.⁷

Decisions related to Twitter’s governance will shape digital free speech in the years to come. In light of our concerns regarding the FTC’s politicization, and the risk that partisan pressures will encourage the FTC to continue exceeding its statutory authorities, we ask that you provide us with the following information:

1. All documents and communication between or among the Federal Trade Commission and any third-party organizations referring or relating to Mr. Musk’s purchase of Twitter;
2. All documents and communication between or among the Federal Trade Commission and members and staff of the White House Competition Council referring or relating to Mr. Musk’s purchase of Twitter;
3. All documents and communications, including all plans, proposals, or other communications, referring or relating to the FTC’s purpose in making inquiries related to Mr. Musk’s purchase of Twitter that deviate from typical reviews;

We ask that you respond to this inquiry no later than May 31st, 2022.

⁵ [The New Progressives Fight Against Consumer Welfare - WSJ](#)

⁶Letter to President Biden Calling Out Administration for Distracting from Disastrous Energy Policies, November 29, 2021, <https://fitzgerald.house.gov/media/press-releases/fitzgerald-armstrong-lead-house-colleagues-calling-out-biden-administrations>.

⁷ <https://republicans-judiciary.house.gov/wp-content/uploads/2022/05/2022-05-04-JDJ-to-FTC-Musk-purchase.pdf>.

Sincerely,



Scott Fitzgerald
Member of Congress



Jim Jordan
Ranking Member



Louie Gohmert
Member of Congress



Andy Biggs
Member of Congress



Dan Bishop
Member of Congress

Appendix 4

202-3062

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair**
 Noah Joshua Phillips
 Rebecca Kelly Slaughter
 Christine S. Wilson

In the Matter of

TWITTER, INC., a corporation.

DECISION AND ORDER

Docket No. C-4316

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed presenting the draft Complaint to the Commission. If issued, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1) and (l), 53(b), and 56(a)(1).

Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe Respondent has violated the Decision and Order the Commission previously issued in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent Twitter, Inc. (“Twitter”) is a Delaware corporation with its principal office or place of business at 1355 Market Street, Suite 900, San Francisco, CA 94103.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.
3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Provision I of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).

4. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.
5. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

DEFINITIONS

For the purpose of this Order, the following definitions apply:

- A. **“Covered Incident”** means any instance affecting 250 or more Users in which: (1) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) individually identifiable Covered Information collected or received, directly or indirectly, by Respondent, was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. “Covered Incident” does not include instances where the only unauthorized access, acquisition, or exposure was due to a User communicating through Respondent’s services (e.g., public tweets, protected tweets, retweets, or direct messages) information that was obtained from sources other than Respondent.
- B. **“Covered Information”** means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (4) a mobile or other telephone number; (5) photos and videos; (6) Internet Protocol (“IP”) address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; (7) a Social Security number; (8) a driver’s license or other government issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; or (13) any information combined with any of (1) through (12) above. “Covered Information” does not include information that a User intends to make public using Respondent’s services.
- C. **“Representatives”** means Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.
- D. **“Resources”** means networks, systems, and software.
- E. **“Respondent”** means Twitter, Inc. (“Twitter”), and its successors and assigns. For purposes of Parts V and VI, Respondent means Twitter, Inc., its successors and assigns, and any business that Respondent controls directly or indirectly, except for any business that: (1) does not provide services that are offered to U.S. residents; or (2) does not collect, maintain, use, disclose,

access, or provide access to the Covered Information of U.S. residents to enable Respondent’s microblogging, social networking, or communications services.

F. “**Timeline Notice**” means a message Respondent places in a User’s Twitter timeline (*i.e.*, the main screen the User sees when opening Twitter which displays a stream of tweets from accounts the User has chosen to follow) that stays near the top (*i.e.*, within the first five (5) tweets) of a User’s Twitter timeline: (1) for at least six (6) months from the effective date of the Order; (2) until the User clicks on the “Learn More about your options” button embedded in the message; or (3) until the User scrolls past the message in their timeline, whichever occurs earlier.

G. “**User**” means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent’s products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent and its Representatives, directly or through any corporation, subsidiary, division, website, mobile app, or other device, in connection with the offering of any product or service in or affecting commerce, must not misrepresent, in any manner, expressly or by implication, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

A. Respondent’s privacy and security measures to prevent unauthorized access to Covered Information;

B. Respondent’s privacy and security measures to honor the privacy choices exercised by Users;

C. Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information;

D. The extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls;

E. The extent to which Respondent makes or has made Covered Information accessible to any third parties;

F. The extent to which Respondent targets advertisements to Users or enables third parties to target advertisements to Users; or

G. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (*e.g.*, two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent’s ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

III. REQUIRED NOTICE TO CONSUMERS

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must provide a Timeline Notice to all current U.S. Users who joined Twitter prior to September 17, 2019, that states: “**Twitter’s Use of Your Personal Information for Tailored Advertising** As we stated on Oct. 8, 2019, we may have served you targeted ads based on an email address or phone number you provided to us to secure your account.”, and includes a “Learn more about your options” button that links to a webpage showing the information in Exhibit A.

IV. REQUIRED MULTI-FACTOR AUTHENTICATION OPTIONS

IT IS FURTHER ORDERED that, as of the effective date of this Order, Respondent must allow Users to utilize multi-factor authentication without providing a telephone number to access their Twitter accounts, such as by integrating authentication applications or allowing the use of security keys. The Company may use equivalent, widely-adopted industry authentication options that do not require Users to provide a telephone number and that are not multi-factor, if the person or persons responsible for the Program under Provision V.C: (1) approve(s) in writing the use of such equivalent authentication options; and (2) document(s) a written explanation of how the authentication options are widely-adopted and at least equivalent to the security provided by multi-factor authentication.

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Program;
- B. Provide the written program, and any evaluations thereof or updates thereto to Respondent’s board of directors or governing body or, if no such board or equivalent governing

body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;
2. For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;
3. For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report (“Privacy Review”) for each such new or modified product, service, or practice. The Privacy Review must:
 - (a) Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;
 - (b) Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;
 - (c) If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (*e.g.*, under security settings, in pop-up messages in the timeline, or in response to a prompt reading, “Get Better Ads!”);

- (d) Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (e) State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;
- (f) Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (g) Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;
- (h) Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;
- (i) Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;
- (j) Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;
- (k) Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;
- (l) Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;
- (m) Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and
- (n) Include any decision or recommendation made as a result of the review (e.g., whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

4. Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:
 - (a) Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;
 - (b) Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;
 - (c) Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and
 - (d) Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;
 5. Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;
 6. Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and
 7. Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. INDEPENDENT PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order titled Mandated Privacy and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to Respondent's compliance with this Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first three-hundred-and-sixty-five (365) days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were

identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Independent Program Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about Respondent's Resources(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and have visibility to Resource(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for the Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification; and
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re Twitter, Inc., FTC File No. 202-3062.”

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent’s discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- D. The number of Users whose Covered Information was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW,

Washington, DC 20580. The subject line must begin, “*In re Twitter, Inc.*, FTC File No. 202-3062.”

X. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities relating to the subject matter of this Order, and all agents and representatives who participate in any acts or practices subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XI. COMPLIANCE REPORTING AND NOTICES

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. Two-hundred and forty (240) days after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent’s businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business, including the goods and services offered and the means of advertising, marketing, and sales; (4) describes in detail whether and how Respondent is in compliance with each Provision of this Order; and (5) provides a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; (3) the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent.

C. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

D. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “In re Twitter, Inc., FTC File No. 202-3062.”

XII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person that Respondent contracts with directly and that provides services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, and any responses to such complaints;
- D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;
- E. A copy of each widely-disseminated representation by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, (1) statements relating to any change in any product, service, or practice that relates to the privacy, security, confidentiality, or integrity of such information, and (2) statements relating to: (a) Respondent’s privacy and security measures to prevent unauthorized access to Covered Information; (b) Respondent’s privacy and security measures to honor the privacy choices exercised by Users; (c) Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information; (d) the extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls; (e) the extent to which Respondent makes or has made Covered Information accessible to any third parties; (f) the extent to which Respondent allows third parties to serve advertisements to Users; or (g) the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules;

- F. All materials relied upon in making the statements in Provisions XII.D and XII.E, and copies of each materially different notice provided to Users and mechanisms for obtaining a User's consent for the collection, use, or disclosure of Covered Information (including screenshots/screencasts and User interfaces, consent flows, and paths a User must take to reach such settings);
- G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;
- H. For 5 years from the date received, copies of all subpoenas, information provided in response to such subpoenas, and all material correspondence with law enforcement, if such communication relate to Respondent's compliance with this Order;
- I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order; and
- J. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission’s website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission’s seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: May 26, 2022

Appendix 5

1
2
3
4
5
6
7
8
9
10
11
12

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

TWITTER, INC., a corporation,

Defendant.

Case No. 3:22-cv-3070 TSH

**STIPULATED ORDER FOR
CIVIL PENALTY,
MONETARY JUDGMENT, AND
INJUNCTIVE RELIEF**

13
14
15
16
17
18
19
20
21
22

**STIPULATED ORDER FOR CIVIL PENALTY, MONETARY
JUDGMENT, AND INJUNCTIVE RELIEF**

The United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission (“Commission” or “FTC”), filed its Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief (“Complaint”) in this matter pursuant to Sections 5(a) and (l), 13(b), and 16(a)(1) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a) and (l), 53(b), and 56(a)(1). Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief (“Stipulated Order”) to resolve the claims for civil penalties and injunctive relief set forth in the Complaint.

THEREFORE, IT IS ORDERED as follows:

23
24
25
26
27
28

FINDINGS

1. This Court has jurisdiction over the subject matter and all of the parties.
2. Venue is proper as to all parties in this District.
3. The Complaint states a claim upon which relief may be granted against Defendant under Sections 5(a) and (l), 13(b), and 16(a)(1) of the FTC Act, 15 U.S.C. §§ 45(a), 45(l), 53(b), and

1 56(a)(1), including for violations of Part I of the Commission’s Decision and Order in *In re*
2 *Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. Mar. 2, 2011).

3 4. Defendant’s activities are “in or affecting commerce,” as defined in Section 4 of the FTC
4 Act, 15 U.S.C. § 44.

5 5. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28
6 U.S.C. § 2412, concerning the prosecution of this action through the date of this Stipulated
7 Order, and agrees to bear its own costs and attorney’s fees.

8 6. Defendant neither admits nor denies any of the allegations in the Complaint, except as
9 specifically stated in the Decision and Order set forth in Attachment A. Only for purposes of this
10 action, Defendant admits the facts necessary to establish jurisdiction.

11 7. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the
12 validity of this Stipulated Order.

13 **I. MONETARY JUDGMENT FOR CIVIL PENALTY**

14 IT IS FURTHER ORDERED that:

15 A. Judgment in the amount of ONE HUNDRED FIFTY MILLION dollars
16 (\$150,000,000.00) is entered in favor of Plaintiff against Defendant as a civil penalty pursuant to
17 Section 5(l) of the FTC Act, 15 U.S.C. § 45(l).

18 B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the
19 United States, ONE HUNDRED FIFTY MILLION dollars (\$150,000,000.00), which, as
20 Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment
21 to Plaintiff. Such payment must be made within seven (7) days of entry of this Stipulated Order
22 by electronic fund transfer in accordance with instructions specified by a representative of
23 Plaintiff.

24 C. In the event of any default in payment, the entire unpaid amount, together with interest,
25 as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall
26 immediately become due and payable.
27
28

1 D. Defendant relinquishes dominion and all legal and equitable right, title, and interest to all
2 funds paid pursuant to this Stipulated Order. Defendant shall make no claim to or demand for
3 return of the funds, directly or indirectly, through counsel or otherwise.

4 E. Defendant agrees that the facts alleged in the Complaint will be taken as true, without
5 further proof, only in any subsequent civil litigation by Plaintiff to enforce its rights to any
6 payment or monetary judgment pursuant to this Stipulated Order.

7 F. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security
8 Numbers or Employer Identification Numbers), which Defendant has previously submitted to
9 Plaintiff, may be used for collecting and reporting on any delinquent amount arising out of this
10 Stipulated Order, in accordance with 31 U.S.C. § 7701.

11 II. MODIFICATION OF DECISION AND ORDER

12 IT IS FURTHER ORDERED that Defendant, and its successors and assigns, shall
13 consent to: (i) reopening of the proceeding in FTC Docket No. C-4316; (ii) waiver of its rights
14 under the show cause procedures set forth in Section 3.72(b) of the Commission's Rules of
15 Practice, 16 C.F.R. § 3.72(b); and (iii) modifying the Decision and Order in *In re Twitter, Inc.*,
16 C-4316, 151 FTC LEXIS 162 (F.T.C. Mar. 2, 2011), with the Decision and Order set forth in
17 Attachment A.

18 III. ADDITIONAL PROVISIONS

19 IT IS FURTHER ORDERED that Defendant shall provide to the Department of Justice
20 copies of all of the reports, assessments, notifications, certifications, and other documents
21 required or requested under the Decision and Order set forth in Attachment A as follows: Parts
22 VI.A, VI.E, VIII.A, IX, X.A, XI.A, and XI.B. Such documents shall be furnished via email to
23 Consumer.Compliance@usdoj.gov, with the subject line "United States v. Twitter, Inc., DJ 102-
24 4022." In the event that electronic mail is unavailable, the documents may be sent to the Director
25 of the Department of Justice's Consumer Protection Branch, and whomever he or she designates,
26 via overnight courier (not the U.S. Postal Service) to: Director, Consumer Protection Branch,
27 Department of Justice, 450 Fifth St. NW Ste. 6400-South, Washington, DC 20001, with the
28

1 subject line “United States v. Twitter, Inc., DJ 102-4022.” Defendant agrees that the Department
2 of Justice shall have the same rights as the Commission (as given in the Decision and Order set
3 forth in Attachment A) to request such documents under the specified parts, subject to any
4 applicable law or regulation. Within fourteen (14) days of receipt of a written request from a
5 representative of the Department of Justice’s Consumer Protection Branch related to the reports,
6 assessments, notifications, certifications, and other documents produced pursuant to the parts of
7 the Decision and Order identified in this paragraph, Defendant agrees to submit additional
8 compliance reports or other requested information, which must be sworn under penalty of
9 perjury. For purposes of this paragraph, “Defendant” shall have the same definition and scope as
10 the definition of “Respondent” in Paragraph E on page 3 of the Decision and Order set forth in
11 Attachment A.

12 **IV. CONTINUING JURISDICTION**

13 IT IS FURTHER ORDERED that this Court shall retain jurisdiction in this matter for
14 purposes of construction, modification, and enforcement of this Stipulated Order. The Clerk of
15 Court shall close the file.

16 SO ORDERED this 26th day of May, 2022.

17 
18 _____
19 THOMAS S. HIXSON
20 UNITED STATES MAGISTRATE JUDGE
21
22
23
24
25
26
27
28

1 **SO STIPULATED AND AGREED:**

2 Dated: May 25, 2022

FOR PLAINTIFF:

THE UNITED STATES OF AMERICA:

3
4 BRIAN M. BOYNTON
5 Principal Deputy Assistant Attorney General
6 Civil Division

7 ARUN G. RAO
8 Deputy Assistant Attorney General

9 GUSTAV W. EYLER
10 Director
11 Consumer Protection Branch

12 LISA K. HSIAO
13 Assistant Director

14 /s/ Zachary L. Cowan
15 ZACHARY L. COWAN
16 DEBORAH S. SOHN
17 Trial Attorneys
18 U.S. Department of Justice
19 Civil Division
20 Consumer Protection Branch
21 450 5th Street NW, Suite 6400-S
22 Washington, DC 20530
23 Telephone: (202) 451-7468
24 Zachary.L.Cowan@usdoj.gov
25 Deborah.S.Sohn@usdoj.gov

26 STEPHANIE M. HINDS
27 United States Attorney

28 MICHELLE LO
29 Chief, Civil Division

30 SHARANYA MOHAN
31 EMMET P. ONG
32 Assistant United States Attorneys
33 Northern District of California
34 450 Golden Gate Avenue
35 San Francisco, California 94102
36 Tel: (415) 436-7198
37 sharanya.mohan@usdoj.gov
38 emmet.ong@usdoj.gov

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
26
27
28

Dated: May 24, 2022

FOR THE FEDERAL TRADE COMMISSION:

JAMES A. KOHM
Associate Director
Division of Enforcement

LAURA KOSS
Assistant Director
Division of Enforcement



REENAH L. KIM
Attorney
Division of Enforcement

ANDREA V. ARIAS
Attorney
Division of Privacy and Identity Protection

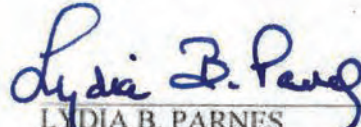
Federal Trade Commission
600 Pennsylvania Avenue, N.W.,
Mail Stop CC-9528
Washington, D.C. 20580
Tel: (202) 326-2272 (Kim); -2715 (Arias)
rkim1@ftc.gov; aarias@ftc.gov

FOR DEFENDANT TWITTER, INC.

1
2 Dated: 05/18/22


DAMIEN KIERAN
Chief Privacy Officer
Twitter, Inc.

3
4
5
6 Dated: 5/20/2022


LYDIA B. PARNES
Wilson Sonsoni Goodrich & Rosati
1700 K Street N.W., Fifth Floor
Washington, D.C. 20006
Tel: (202) 973-8800
lparnes@wsgr.com

Counsel for Twitter, Inc.

ATTACHMENT A

202-3062

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair**
 Noah Joshua Phillips
 Rebecca Kelly Slaughter
 Christine S. Wilson

In the Matter of

TWITTER, INC., a corporation.

DECISION AND ORDER

Docket No. C-4316

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed presenting the draft Complaint to the Commission. If issued, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1) and (l), 53(b), and 56(a)(1).

Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe Respondent has violated the Decision and Order the Commission previously issued in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent Twitter, Inc. (“Twitter”) is a Delaware corporation with its principal office or place of business at 1355 Market Street, Suite 900, San Francisco, CA 94103.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Provision I of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).
4. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.
5. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

DEFINITIONS

For the purpose of this Order, the following definitions apply:

- A. **“Covered Incident”** means any instance affecting 250 or more Users in which: (1) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) individually identifiable Covered Information collected or received, directly or indirectly, by Respondent, was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. “Covered Incident” does not include instances where the only unauthorized access, acquisition, or exposure was due to a User communicating through Respondent’s services (e.g., public tweets, protected tweets, retweets, or direct messages) information that was obtained from sources other than Respondent.
- B. **“Covered Information”** means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (4) a mobile or other telephone number; (5) photos and videos; (6) Internet Protocol (“IP”) address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; (7) a Social Security number; (8) a driver’s license or other government issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; or (13) any information combined with any of (1) through (12) above. “Covered Information” does not include information that a User intends to make public using Respondent’s services.
- C. **“Representatives”** means Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.
- D. **“Resources”** means networks, systems, and software.

E. “**Respondent**” means Twitter, Inc. (“Twitter”), and its successors and assigns. For purposes of Parts V and VI, Respondent means Twitter, Inc., its successors and assigns, and any business that Respondent controls directly or indirectly, except for any business that: (1) does not provide services that are offered to U.S. residents; or (2) does not collect, maintain, use, disclose, access, or provide access to the Covered Information of U.S. residents to enable Respondent’s microblogging, social networking, or communications services.

F. “**Timeline Notice**” means a message Respondent places in a User’s Twitter timeline (*i.e.*, the main screen the User sees when opening Twitter which displays a stream of tweets from accounts the User has chosen to follow) that stays near the top (*i.e.*, within the first five (5) tweets) of a User’s Twitter timeline: (1) for at least six (6) months from the effective date of the Order; (2) until the User clicks on the “Learn More about your options” button embedded in the message; or (3) until the User scrolls past the message in their timeline, whichever occurs earlier.

G. “**User**” means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent’s products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent and its Representatives, directly or through any corporation, subsidiary, division, website, mobile app, or other device, in connection with the offering of any product or service in or affecting commerce, must not misrepresent, in any manner, expressly or by implication, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

A. Respondent’s privacy and security measures to prevent unauthorized access to Covered Information;

B. Respondent’s privacy and security measures to honor the privacy choices exercised by Users;

C. Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information;

D. The extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls;

E. The extent to which Respondent makes or has made Covered Information accessible to any third parties;

F. The extent to which Respondent targets advertisements to Users or enables third parties to target advertisements to Users; or

G. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to

the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (e.g., two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

III. REQUIRED NOTICE TO CONSUMERS

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must provide a Timeline Notice to all current U.S. Users who joined Twitter prior to September 17, 2019, that states: “**Twitter’s Use of Your Personal Information for Tailored Advertising** As we stated on Oct. 8, 2019, we may have served you targeted ads based on an email address or phone number you provided to us to secure your account.”, and includes a “Learn more about your options” button that links to a webpage showing the information in Exhibit A.

IV. REQUIRED MULTI-FACTOR AUTHENTICATION OPTIONS

IT IS FURTHER ORDERED that, as of the effective date of this Order, Respondent must allow Users to utilize multi-factor authentication without providing a telephone number to access their Twitter accounts, such as by integrating authentication applications or allowing the use of security keys. The Company may use equivalent, widely-adopted industry authentication options that do not require Users to provide a telephone number and that are not multi-factor, if the person or persons responsible for the Program under Provision V.C: (1) approve(s) in writing the use of such equivalent authentication options; and (2) document(s) a written explanation of how the authentication options are widely-adopted and at least equivalent to the security provided by multi-factor authentication.

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program, and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;
2. For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;
3. For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report ("Privacy Review") for each such new or modified product, service, or practice. The Privacy Review must:
 - (a) Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;
 - (b) Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;
 - (c) If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (*e.g.*, under security settings, in pop-up messages in the timeline, or in response to a prompt reading, "Get Better Ads!");

- (d) Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (e) State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;
- (f) Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (g) Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;
- (h) Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;
- (i) Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;
- (j) Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;
- (k) Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;
- (l) Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;
- (m) Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and
- (n) Include any decision or recommendation made as a result of the review (e.g., whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

4. Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:
 - (a) Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;
 - (b) Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;
 - (c) Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and
 - (d) Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;
 5. Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;
 6. Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and
 7. Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. INDEPENDENT PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order titled Mandated Privacy and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to Respondent's compliance with this Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first three-hundred-and-sixty-five (365) days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were

identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Independent Program Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about Respondent's Resources(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and have visibility to Resource(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for the Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification; and
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062."

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- D. The number of Users whose Covered Information was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW,

Washington, DC 20580. The subject line must begin, “*In re Twitter, Inc.*, FTC File No. 202-3062.”

X. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities relating to the subject matter of this Order, and all agents and representatives who participate in any acts or practices subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XI. COMPLIANCE REPORTING AND NOTICES

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. Two-hundred and forty (240) days after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent’s businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business, including the goods and services offered and the means of advertising, marketing, and sales; (4) describes in detail whether and how Respondent is in compliance with each Provision of this Order; and (5) provides a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; (3) the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent.

C. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

D. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “In re Twitter, Inc., FTC File No. 202-3062.”

XII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person that Respondent contracts with directly and that provides services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, and any responses to such complaints;
- D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;
- E. A copy of each widely-disseminated representation by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, (1) statements relating to any change in any product, service, or practice that relates to the privacy, security, confidentiality, or integrity of such information, and (2) statements relating to: (a) Respondent’s privacy and security measures to prevent unauthorized access to Covered Information; (b) Respondent’s privacy and security measures to honor the privacy choices exercised by Users; (c) Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information; (d) the extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls; (e) the extent to which Respondent makes or has made Covered Information accessible to any third parties; (f) the extent to which Respondent allows third parties to serve advertisements to Users; or (g) the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules;

F. All materials relied upon in making the statements in Provisions XII.D and XII.E, and copies of each materially different notice provided to Users and mechanisms for obtaining a User's consent for the collection, use, or disclosure of Covered Information (including screenshots/screencasts and User interfaces, consent flows, and paths a User must take to reach such settings);

G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

H. For 5 years from the date received, copies of all subpoenas, information provided in response to such subpoenas, and all material correspondence with law enforcement, if such communication relate to Respondent's compliance with this Order;

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order; and

J. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED:

EXHIBIT A

[To appear with the Twitter logo and Twitter's standard website header]

We may have asked for your phone number or email address to secure or authenticate your account (for example, for two-factor authentication). As we [told you](#) in October 2019, we may have used these phone numbers or email addresses to deliver tailored advertising to you on Twitter until September 2019. On [date], we entered into a settlement with the Federal Trade Commission to resolve this issue.

As of September 17, 2019, we are no longer using phone numbers or email addresses collected for safety or security purposes for advertising. We never disclosed or shared your phone number or email address with advertisers. There is no action that you need to take regarding this issue.

You have a number of options to control your privacy and security when you use Twitter:

- **Control your privacy settings.** You can find out more about your privacy settings on Twitter, including how to enable or disable personalized ads, by visiting <https://myprivacy.twitter.com>.
- **Review your multi-factor authentication settings.** By requiring both a password and a secondary code or security key to access your account, multi-factor authentication can help keep your account safe. You can use an authentication app, a security key, or a phone number for multi-factor authentication. (And if you provide us a phone number for multi-factor authentication, it will not be used for advertising purposes without your consent.) You can learn about multi-factor authentication settings by visiting <https://help.twitter.com/en/managing-your-account/two-factor-authentication>.

For more details about how we protect the information you share with us and how we use that data, we encourage you to visit the [Twitter Privacy Center](#).

We are very sorry this happened. If you have questions or comments about this notice or what we do to protect your information moving forward, you may contact Twitter's Office of Data Protection through this [form](#).

[To appear with the Twitter's standard website footer]

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

TWITTER, Inc.,
a corporation.

Docket No. C-4316

DECISION

The Federal Trade Commission (“Commission”) issued a Decision and Order against Twitter, Inc. (“Twitter”) in Docket C-4316 on March 2, 2011 (“2011 order”).¹ On [INSERT DATE], the United States of America, acting upon notification and authorization to the Attorney General by the Commission, filed a complaint (“2022 complaint”) in federal district court alleging that Twitter violated the 2011 order by misrepresenting the extent to which it maintained and protected the privacy of nonpublic consumer information. The complaint also alleged that Twitter violated Section 5 of the FTC Act by misrepresenting how it would use telephone numbers and email addresses that users provided to enable a security feature.

On [INSERT DATE], Judge [INSERT JUDGE’S NAME] in the District for the Northern District of California entered a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief (“Stipulated Order”) resolving the 2022 complaint. In Section II of the Stipulated Order, Twitter consented to: (1) reopening the 2011 proceeding in FTC Docket No. C-4316; (2) waiving its rights under the show cause procedures set forth in Section 3.72(b) of the Commission’s Rules of Practice, 16 C.F.R. § 3.72(b); and (3) modifying the 2011 Order with the new Decision and Order set forth below.

In view of the foregoing, the Commission has determined that it is in the public interest to reopen the proceeding in Docket No. C-4316 pursuant to Commission Rule 3.72(b), 16 C.F.R. § 3.72(b), and to issue a new order as set forth below. Accordingly,

IT IS ORDERED that this matter be, and it hereby is, reopened; and

IT IS FURTHER ORDERED that, Twitter having consented to modifying the 2011 order as set forth below, the Commission hereby modifies the 2011 order with the attached Decision and Order.

¹ *In the Matter of Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011).

Appendix 6



To whom it may concern:

Elon Musk's takeover of Twitter will further toxify our information ecosystem and be a direct threat to public safety, especially among those already most vulnerable and marginalized.

Twitter has outsized influence in shaping both public discourse and industry-wide platform governance standards. While the company is hardly a poster-child for healthy social media, it has taken welcome steps in recent years to mitigate systemic risks, ratcheting up pressure on the likes of Facebook and YouTube to follow suit. Musk intends to steamroll those safeguards and provide a megaphone to extremists who traffic in disinformation, hate, and harassment. Under the guise of 'free speech,' his vision will silence and endanger marginalized communities, and tear at the fraying fabric of democracy.

The undersigned organizations believe that Twitter should continue to uphold the practices that serve as guideposts for other Big Tech platforms. **We call on you - Twitter's top advertisers - to commit to these standards as non-negotiable requirements for advertising on the platform:**

1. **Keep accounts including those of public figures and politicians that were removed for egregious violations of Twitter Rules - such as harassment, violence, and hateful conduct - off the platform** and continue to enforce the [civic integrity policy](#) along with the [hateful conduct policy](#). Since 2020, Twitter has applied its civic integrity policy to all users, including elected officials. Musk's statements at [Ted2022](#) last week indicate that he will roll-back permanent bans and err on the side of allowing harmful content to remain on the platform under the guise of 'free speech.' A reversal of Twitter's content moderation policies including its recently released [climate commitments](#), its protections for transgender people, and its restrictions on other forms of hate, harassment, and violence would be toxic not just for those targeted, but also for businesses advertising on the platform.
2. **Beyond algorithmic transparency, ensure algorithmic accountability, preserve people's privacy, and commit to depolarizing the algorithm.** Consider the implications of full-scale public visibility into Twitter's algorithm and put protections in place to prevent bad actors from gaming the system. Listen to [privacy experts](#) and others whose expertise includes protecting communities that are discriminated against in speaking truth to power. Continue the work of its in-house research team called [Machine Learning Ethics, Transparency and Accountability](#) that looks at potential biases in

its algorithms including published research, for instance, on whether the algorithms that automatically crop profile photos contained inadvertent bias.

3. Continue Twitter's commitment to transparency and researcher access.

Twitter stands out for its support of researchers – both internal and external to the company. From its [API for academic research](#) to its [willingness to publish critique](#) and its internal learnings, Twitter has demonstrated a commitment to transparency and access for researchers that sets an example for other Big Tech companies and allows for accountability.

As top advertisers on Twitter, your brand risks association with a platform amplifying hate, extremism, health misinformation, and conspiracy theorists.

Under Musk's management, Twitter risks becoming a cesspool of misinformation, with your brand attached, polluting our information ecosystem in a time where trust in institutions and news media is already at an all-time low. Your ad dollars can either fund Musk's vanity project or hold him to account. We call on you to demand Musk uphold these basic standards of community trust and safety, and to pull your advertising spending from Twitter if they are not.

Sincerely,

Access Now
 Accountable Tech
 Black Lives Matter Global Network Foundation
 Center for Countering Digital Hate
 Empowering Pacific Islander Communities (EPIC)
 Face the Music Collective
 Fair Vote UK
 Free Press
 Friends of the Earth
 Gender Equity Policy Institute
 GLAAD
 Global Project Against Hate and Extremism
 Indivisible Northern Nevada
 Kairos
 Media Matters for America
 MediaJustice
 NARAL Pro-Choice America
 National Hispanic Media Coalition
 Religious Coalition for Reproductive Choice
 Reproaction
 Stop Online Violence Against Women Inc
 The Sparrow Project
 UltraViolet
 Union of Concerned Scientists
 V-Day/One Billion Rising
 Women's March

Appendix 7



Office of the Chair

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Final Report 1638

May 6, 2022

The Honorable Jim Jordan
Ranking Member
Committee on the Judiciary
U.S. Houses of Representatives
Washington, D.C. 20515

Dear Ranking Member Jordan:

Thank you for your May 4, 2022, letter regarding the Open Markets Institute's April 26, 2022, issuance of a statement on the proposed acquisition of Twitter by Elon Musk. I am happy to respond to the two questions posed in your letter.

1. Did you or anyone else at the FTC solicit or play any role in drafting OMI's statement?

I did not and, as far as I am aware, nor did anyone under my supervision. It would be inappropriate for FTC staff to be in contact with the Open Markets Institute regarding the drafting or solicitation of their statement.

2. Has the FTC taken any actions in response to the statement released by OMI?

The FTC has not taken any actions in response to the statement released by the Open Markets Institute. As noted in 16 C.F.R. §§ 2.2 and 2.3, anyone is welcome to file a complaint or a request for Commission action, though the Commission acts only in the public interest. The FTC's law enforcement work is driven by the Commission, conducted by the agency's staff, and confined by our statutory authorities.

Thank you again for your letter. If you have any questions, please feel free to have your staff call [REDACTED], the Director of our Office of Congressional Relations, at [REDACTED].

Sincerely,

A handwritten signature in cursive script that reads "Lina Khan".

Lina M. Khan
Chair, Federal Trade Commission

Appendix 8

**Concurring Statement of Commissioner Christine S. Wilson
and Commissioner Noah Joshua Phillips**

Twitter

Matter No. 2023062

May 25, 2022

Today's settlement with Twitter, Inc., years in the making,¹ illustrates once again that the Federal Trade Commission takes seriously both the protection of consumers' privacy and the enforcement of Commission orders. The settlement provides meaningful relief, including a \$150 million civil penalty and extensive injunctive provisions. We thank our knowledgeable and experienced career staff who investigated this case and negotiated this order – they and their colleagues work tirelessly to make the FTC the most effective privacy enforcer in the world.

In March 2011, the Commission finalized an order with Twitter (“2011 Order”), settling allegations that it deceived consumers and put their privacy at risk by failing to (1) use reasonable and appropriate security measures to protect nonpublic user data from unauthorized access, and (2) honor consumers' privacy choices.² That 2011 Order prohibited Twitter from misrepresenting the extent to which it maintains and protects the security and privacy of nonpublic data and honors users' privacy choices. As alleged in the complaint filed today, Twitter failed to live up to its obligations. Specifically, Twitter allegedly collected telephone numbers and email addresses from consumers for security purposes, but then used that information for targeted advertisements.

When consumers hand over personal information for specific security purposes, such as multi-factor authentication, account recovery, or re-authorization, they reasonably expect the information to be deployed for those purposes. When companies use those data for non-security purposes, like advertising, they undermine trust in critical security measures to the detriment of consumers and businesses alike.

The complaint alleges that this conduct violated both the 2011 Order and Section 5 of the FTC Act. The complaint also alleges that Twitter misrepresented its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, which prohibit participants from processing personal information in a way that is incompatible with the purposes for which it was originally collected.³

¹ See Twitter, Inc., Quarterly Report (Form 10-Q) (Aug. 3, 2020), <https://sec.report/Document/0001418091-20-000158/>.

² *In the matter of Twitter, Inc.*, FTC File No. 0923093 (March 2011), <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3093-twitter-inc-corporation>.

³ This settlement demonstrates the Commission's continued commitment to take action against companies that misrepresent their compliance with Privacy Shield, any successor program, or similar agreements that protect privacy and facilitate international data transfers.

The new Twitter order employs the model that the FTC has built during two decades of vigorous privacy and data security enforcement. Observant readers will spot many injunctive remedies the Commission has employed repeatedly in its privacy and data security orders. For example, the order requires Twitter to create and implement a privacy and security program that includes privacy risk assessments, detailed privacy reviews for new or modified products, documentation, data access controls, technical measures to monitor unauthorized access, training, and certifications.

But the FTC’s enforcement model is not static; the Commission has refined and updated it to address evolving business practices and technologies. Some of the provisions in today’s order reflect recent refinements. For example, Twitter is required to use either multifactor authentication or a widely adopted mechanism that provides equivalent security.⁴ The Commission first included a requirement to use multifactor authentication in our March enforcement action against CaféPress.⁵ Today’s order also requires Twitter to design and implement both a privacy and an information security program, a dual obligation we first imposed in our 2019 enforcement action against Facebook.⁶

And, in each case, the Commission tailors its enforcement to the specific unlawful conduct and harms alleged in each case. This Twitter order includes a data use restriction tied to the core

⁴ *In the Matter of Twitter, Inc.*, C-4316, Decision and Order (May 2022) (Section IV).

⁵ See *In the Matter of CafePress*, No. 192-3209 (Mar. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Residual%20Pumpkin%20Agreement%20Containing%20Consent%20Order.pdf (Section II.E.7). This obligation builds on provisions in prior Commission orders that require encryption or other security features. See, e.g., *In the Matter of Zoom Video Communications, Inc.*, C-4731 (Feb. 2021), https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf (requiring “[p]rotections, such as encryption, tokenization, or other same or greater protections, for Covered Information collected, maintained, processed, or stored by Respondent, including in transit and at rest” (Section II.E.11)); *In the Matter of LightYear Dealer Technologies, LLC*, No. C-4687 (Sept. 2019), https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf (requiring encryption of all Social Security numbers and financial account information on Respondent’s computer networks (Section I.E.4)).

⁶ Part V of the Facebook order requires that it: “implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security of Covered Information. In addition to any security-related measures associated with Respondent’s Privacy Program under Part VII of this Order, the information security program must contain safeguards appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the Covered Information.” Part VII of the order requires that it: “establish and implement, and thereafter maintain a comprehensive privacy program (‘Privacy Program’) that protects the privacy, confidentiality, and Integrity of the Covered Information collected, used, or shared by Respondent.” *U.S. v. Facebook*, No. 1:19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf; *In the Matter of Facebook, Inc.*, C-4365 (Apr. 2020), <https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf>, see also 2019 Order Fact Sheet (Jul. 24, 2019), https://www.ftc.gov/system/files/attachments/press-releases/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook/2019_order_fact_sheet_facebook.pdf (noting that the order requires Facebook to create a comprehensive data security program and a mandated privacy program); Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson Regarding the Matter of Facebook (Jul. 24, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chairman-joe-simons-commissioners-noah-joshua-phillips-christine-s-wilson-regarding-matter> (discussing the inclusion of a requirement for both a privacy and security program).

allegation of illegality in the complaint: the company may not use for advertising any phone numbers or email addresses that had been gathered for security purposes. The 2019 Facebook order contained a similar use restriction, flowing from a similar allegation of illegality.

Precisely because this order builds on established precedent and the Commission’s expertise in privacy enforcement, it provides meaningful and effective relief. The value of these types of injunctive provisions and accountability mechanisms has long been clear to us.⁷ But strikingly similar settlements in the past have been subjected to (sometimes vitriolic) criticism⁸ for alleged failings that today’s order would share. No executives are named, or obligated personally.⁹ There is no admission of liability, or disgorgement of algorithms. There is no change to Twitter’s business model.

⁷ See Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, *In re Sunday Riley Modern Skincare, LLC*, (Nov. 6, 2020), https://www.ftc.gov/system/files?file=documents/cases/2020.11.6_sunday_riley_majority_statement_final.pdf (discussing the effectiveness of injunctive and other non-monetary relief); see also Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson Regarding the Matter of Facebook (Jul. 24, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chairman-joe-simons-commissioners-noah-joshua-phillips-christine-s-wilson-regarding-matter> (describing the breadth and scope of the non-monetary relief in the order). Commissioner Wilson also has spoken at length about the effectiveness of non-monetary relief. See, e.g., Christine S. Wilson, One Step Forward, Two Steps Back: Sound Policy on Consumer Protection, Remarks at NAD (Oct. 5, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581434/wilson_remarks_at_nad_100520.pdf; Christine S. Wilson, Remarks at Global Antitrust Institute, *FTC v. Facebook* (Dec. 11, 2019), https://www.ftc.gov/system/files/documents/public_statements/1557534/commissioner_wilson_remarks_at_global_antitrust_institute_12112019.pdf.

⁸ See, e.g., Dissenting Statement of Commissioner Rohit Chopra Regarding Zoom Video Communications, Inc. (Feb. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1586865/20210129_final_chopra_zoom_statement_0.pdf (asserting that the final order is “weak,” provides “no money” and that the injunctive relief constitutes “paperwork requirements” with no real accountability). In addition, then-Commissioner Chopra stated that the order “doesn’t fix the incentives causing these repeat privacy abuses. It doesn’t stop \$FB from engaging in surveillance or integrating platforms. There are no restrictions on data harvesting tactics — just paperwork.” Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; see also Center for Digital Democracy Press Release: Groups Join Legal Battle to Fight Ineffective FTC Privacy Decision on Facebook (Jul. 26, 2019), <https://www.democraticmedia.org/article/groups-join-legal-battle-fight-ineffective-ftc-privacy-decision-facebook> (citing several organizations that criticized and challenged the settlement). Notably, the groups stated that the settlement was “woefully insufficient,” “provides no meaningful changes to Facebook’s structure or financial incentives” and that the “fine is a mere cost of doing business,” “a parking ticket,” a “get-out-of jail free card.” *Id.*; see also Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf. See also, Dissenting Statement of Commissioner Rohit Chopra, *In the matter of Google LLC and YouTube, LLC* (Sep. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

⁹ See *FTC v. Google LLC and YouTube, LLC*, No. 1:19-cv-2642 (D.D.C. Sep. 4, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3083-google-llc-youtube-llc>; *In the matter of Facebook, Inc.*, No. 1:19-cv-02184, (D.D.C. Jul. 24, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter>; *U.S. v. Musical.ly* (now known as TikTok), No. 2:19-cv-1439 (C.D. Cal. Feb. 2, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3004-musically-inc> (naming corporate entities only).

The order in the 2019 Facebook case met with condemnation from some quarters, so it is worth comparing today’s settlement to the alleged shortcomings of the Facebook order:¹⁰

Criticism of Order	Facebook Order	Twitter Order
“Mere paperwork” requirements ¹¹	Privacy risk assessments for new or modified products	Privacy risk assessments for new or modified products
“Mere paperwork” requirements ¹²	Privacy reviews and reports	Privacy reviews and reports
“Mere paperwork” requirements ¹³	Covered incident reports	Covered incident reports
Certifications only ensure that paperwork has been completed ¹⁴	Certifications by CEO and Chief Privacy Officer	Certifications by senior corporate management or senior officer (not CEO)
No accountability for executives ¹⁵	No executives named, no IH of CEO or other executives cited in statements supporting settlement	No executives named, no IH of CEO or other executives cited in statements supporting settlement

¹⁰ The Facebook order included stronger and more sweeping provisions, and a penalty measured in the billions. The differences in approach are appropriate, as there were more Section 5 and order violations alleged in Facebook.

¹¹ Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹² Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹³ Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁴ Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁵ Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *In the matter of FTC v. Facebook* (Jul.24, 2019), https://www.system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

Penalty is a mere cost of doing business ¹⁶	\$5 billion 2018 Annual Revenues: \$55.8 billion Penalty: 9% of annual revenue	\$150 million 2021 Annual revenues: \$5.077 billion ¹⁷ Penalty: 3% of annual revenue
Company receives majority of revenue from advertising and order does nothing to change the business structure or incentives ¹⁸	Can still use data for advertising purposes; prohibited from misrepresenting the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information	Can still use data for advertising purposes; prohibited from misrepresenting the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information
Company governance unchanged ¹⁹	Board of Directors restructured to include Privacy Committee with oversight authority	No governance changes
No meaningful restrictions on ability to collect, share, and use personal information ²⁰	Use restriction for phone numbers; requirement to identify material risks to privacy of covered information and prepare privacy review statements documenting efforts to control for the risk	Use restriction for phone numbers; requirement to identify material risks to privacy of covered information and prepare privacy review statements documenting efforts to control for the risk

We support this order, which is a strong one. The Facebook order included more stringent obligations and greater relief because more egregious conduct was alleged. We reject the view that the provisions in orders like these constitute “mere paperwork” that provide no meaningful restrictions or accountability. And we reject the characterization of substantial penalties as “a slap on the wrist.” Penalties matter, then and now. And so do the privacy programs and

¹⁶ Nancy Scola and Steven Overly, “FTC strikes \$5B Facebook settlement against fierce Democratic objections,” POLITICO (July 24, 2019), <https://www.politico.com/story/2019/07/24/ftc-facebook-settlement-1428432> (quoting Representation Cicilline as stating that the \$5B fine is “disappointing” and Senator Blumenthal as stating that the penalty is “[a] tap on the wrist, not even a slap”); *see also* Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁷ *See Twitter Revenue 2011-2022* TWTR, MacroTrends, <https://www.macrotrends.net/stocks/charts/TWTR/twitter/revenue>.

¹⁸ Dissenting Statement of Commissioner Rebecca Kelly Slaughter *In the matter of FTC v. Facebook* (Jul. 24, 2019), https://www.system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁹ Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

²⁰ Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *In the matter of FTC v. Facebook* (Jul. 24, 2019), https://www.system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

assessments that orders like today's command. Both orders also create processes that require the companies to consider the risks to the privacy and security of the information they collect, evaluate the safeguards they have in place, and adjust procedures to address those risks. Both orders require assessments by third-party experts, approved by the FTC, to evaluate the companies' privacy programs and issue reports evaluating compliance with the mandated program. Both orders require executives in the company to certify to compliance. These processes force companies under order to consider privacy, account for privacy, and be accountable for failing to protect it.

The Commission recognizes that its orders are not perfect. For this reason, we approach each new order with care, fine-tuning provisions and considering alternative ways to address violations.²¹ We hope that the bipartisan approval of this order, one very much in line with prior orders, signals the beginning of a more constructive dialogue about how to continue refining our enforcement program. If this case can close the door on unfounded and gratuitous attacks on the FTC's privacy enforcement program, that closure would serve consumers, provide clarity to stakeholders, and advance the mission of the agency.

The resolution of this matter also demonstrates the general deterrent effect of Commission orders. In our July 2019 complaint and order against Facebook,²² the Commission for the first time found it unlawful for companies to collect consumer information for security purposes and then use it to target advertising. Shortly after the Facebook order was announced, in October 2019, Twitter disclosed its similar misuse of consumers' email addresses and phone numbers.²³ This timeline suggests that Twitter was paying attention to the FTC's actions and underscores the value of sending signals to the marketplace through orders like these.

A side note. In August 2020, Twitter publicly disclosed that the FTC was investigating it for potential order violations, taking an accounting reserve to pay a \$150 million fine.²⁴ Nearly two full years have passed, and Twitter now is paying the anticipated fine. An observer might ask what took so long, and why now. Despite (and because of) the coincidence in timing with

²¹ See, e.g., Statement of the Federal Trade Commission *Regarding Unixiz, Inc. d/b/a i-Dressup.com and Zhijun Liu and Xichen Zhang individually & James V. Grago, Jr. d/b/a ClixSense.com* (Apr. 2019), https://www.ftc.gov/system/files/documents/cases/2019-03-19_idressupclixsense_statement_final.pdf (announcing new requirements that go beyond requirements from previous data security orders); see also *In the Matter of LightYear Dealer Technologies, LLC*, No. C-4687 (Sept. 2019), https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf (including additional data security requirements such as encryption of all Social Security numbers and financial account information on Respondent's computer networks).

²² FTC Press Release, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, July 24, 2019, <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>.

²³ Twitter Support (@TwitterSupport), TWITTER (Oct. 8, 2019, 4:02 PM), https://twitter.com/twittersupport/status/1181661080033955840?ref_src=.

²⁴ See Kate Conger, *F.T.C. Investigating Twitter for Potential Privacy Violations*, N.Y. TIMES (Aug. 3, 2020), <https://www.nytimes.com/2020/08/03/technology/ftc-twitter-privacy-violations.html>.

unrelated headlines concerning Twitter,²⁵ it is important to be clear that this settlement has nothing to do with Twitter's potential sale or new ownership, the company's content moderation policies, or anything other than the facts alleged in the Complaint.

This settlement is about ensuring that Twitter safeguards consumer privacy and vindicates the Commission's authority through zealous enforcement of its orders. It is an excellent settlement. We commend staff on their stellar work.

²⁵ See, e.g., Cara Lombardo, Meghan Bobrowsky & Georgia Wells, *Twitter Accepts Elon Musk's Offer to Buy Company in \$44 Billion Deal*, WALL ST. J. (Apr. 25, 2022, 5:48PM), <https://www.wsj.com/articles/twitter-and-elon-musk-strike-deal-for-takeover-11650912837>.

Appendix 9

**Statement of Chair Lina M. Khan
 Joined by Commissioner Rebecca Kelly Slaughter
 In the Matter of Twitter, Inc.
 Commission File No. 2023062**

May 25, 2022

Americans increasingly find themselves having to surrender personal data to use technologies that are central to economic and social life, and many report feeling a total loss of control over how this data is used.¹ Indeed, evidence suggests that the current configuration of commercial data practices do not actually reveal how much users value privacy or security, and there is growing recognition that the “notice-and-consent” framework has notable shortcomings.² The FTC must harness its full set of tools to ensure we are keeping pace with these new realities, including by exploring the need for agency promulgated rules. In the meantime, we must also hold companies accountable for violating existing laws, including through deceptive disclosures.

According to the Complaint in this matter, Twitter obtained data from users on the pretext of harnessing it for security purposes but then ended up also using the data to target users with ads. The relief we are obtaining from Twitter for this alleged violation of both the law and a past FTC order drives home two key consumer protection principles. First, stating that data is being collected for one purpose and then using it for another purpose is deceptive. The FTC Act prohibits companies from engaging in bait-and-switch tactics with individuals’ data.³ Second, burying disclosures in lengthy privacy policies or terms of service documents does not cure deceptive statements the company makes at the time it collects users’ information. Users do not assume the responsibility of wading through privacy policies to uncover provisions that override or negate what the company told them directly.

Twitter’s Prior and Present Unlawful Practices, As Alleged in the Complaint

Consumers use passwords to access their email, social media accounts, bank accounts, medical records, and more. These credentials are a primary shield for some of our most confidential and personal information, but they are also a common target for hackers or

¹ Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CENTER (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

² See, e.g., Daniel Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 22-32 (2021).

³ Our recent order in *CafePress* stands for this proposition that consumers can bank on claims that data will be used in a limited way or for limited purposes. Agreement Containing Consent Order, *Residual Pumpkin Entity, LLC, and PlanetArt LLC (d/b/a CafePress)*, Comm’n File No. 192-3209 (Mar. 15, 2022).

malicious actors. As a result, many data breaches can be traced back to stolen or compromised consumer credentials.⁴ In response to these online threats and harms, businesses and consumers alike have adopted cybersecurity approaches, like multi-factor authentication, to protect their accounts and data from unauthorized third-party access and use. Multi-factor authentication allows consumers to use two or more forms of evidence to verify their identity when attempting to log into or otherwise access a network, device, application, or service.

In 2011, the Commission charged Twitter with violating Section 5 of the FTC Act for the company's failures to provide reasonable security safeguards to prevent unauthorized access to users' information and to honor privacy choices exercised by Twitter users. This enforcement action resulted in a consent order that barred Twitter from misrepresenting how the company handles "nonpublic consumer information," such as email addresses and phone numbers, and the security measures that it has in place.⁵

From May 2013 to September 2019 Twitter prompted users to provide a telephone number or email address for the express purpose of enabling multi-factor authentication to verify their Twitter accounts, assisting with account recovery, and re-authenticating users' accounts. According to the complaint, Twitter during this period failed to disclose that it also used the telephone numbers and email addresses that users provided for security purposes to target advertisements to those users. Although Twitter's privacy policy made reference to the fact that contact information would be used for advertising purposes,⁶ the complaint charges that this disclosure was deficient and did not remedy the misleading representations made to users when Twitter collected their personal information for security purposes. This allegedly deceptive practice potentially affected more than 140 million Twitter users, while boosting Twitter's primary source of revenue. In October 2019, Twitter publicly self-reported its misuse of users' personal information.⁷

Today's announcement of an enforcement action and resolution alleges that Twitter violated Section 5 of the FTC Act, the EU-US and Swiss-US Privacy Shield frameworks, and the FTC's 2011 Order with Twitter. The case reflects diligent work by FTC staff, and we thank the team for their efforts to hold Twitter accountable.

⁴ VERIZON, DATA BREACH INVESTIGATIONS REPORT, at 7 (2022), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/> (noting that 61% of data breaches involved credentials).

⁵ Press Release, Fed. Trade Comm'n, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2021), <https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-information-0>.

⁶ See *Twitter Privacy Policy*, TWITTER, <https://twitter.com/en/privacy#update> (effective June 10, 2022; last visited May 25, 2022).

⁷ @TwitterSupport, TWITTER (Oct. 8, 2019, 4:02 PM), https://twitter.com/twittersupport/status/1181661080033955840?ref_src=.

The Commission’s Settlement with Twitter⁸

The settlement imposes a series of requirements on Twitter. A few in particular are worth highlighting.

First, Twitter must notify affected parties of its allegedly deceptive conduct. Requiring parties to provide notice ensures that individuals and businesses can determine whether they need to take any action and decide whether they want to continue doing business with a firm that was charged with engaging in wrongdoing.

Second, Twitter must provide users with multi-factor authentication tools that do not require users to share their phone number, such as mobile authentication apps or security keys.⁹ Research shows that these alternatives provide greater security, as they can protect users against credential phishing. Ensuring that the remedies we seek reflect the latest in security research and learning is critical. We are grateful that we have been able to increase the number of technologists, security researchers, and other technical experts at the agency over the last year, and we are keen to continue building out this skillset at the FTC. Given that a growing portion of our work requires investigating digital tools and services, embedding technologists in our investigative teams can further boost the sophistication and efficacy of our enforcement work.

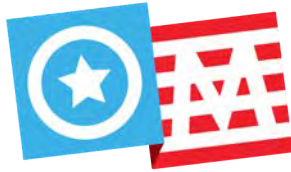
Third, Twitter must pay \$150 million in civil penalties for its alleged recidivism. Civil penalties are key for deterring law violations, and we believe the FTC must approach civil penalties with an eye to complete deterrence. We are confident that in this matter the civil penalty amount obtained ensures that Twitter is not profiting from its allegedly unlawful conduct.

We are grateful to the FTC team for the thorough investigation into Twitter’s alleged violation and the role of individual decisionmakers and for securing a strong settlement.

⁸ Our colleagues Commissioners Wilson and Phillips invite a framework of comparing enforcement resolutions in two entirely different matters—an exercise that the defense bar also frequently demands. We respectfully reject this invitation. No two law violations—or law violators—are exactly alike. Every potential action the Commission takes, whether it is to litigate or to weigh the merits of a proposed settlement, is distinct and requires close and careful consideration of several factors, including: the alleged violations, the effect of those violations on consumers and markets, the structure and incentives of the defendant’s business model, the defendant’s past history of lawbreaking, the ability of the order to affect specific and general deterrence, and the resources of the Commission. Charting and tallying may have some visual appeal, but it is no substitute for case-by-case analysis, nor can it make apples-to-apples out of oranges and bananas.

⁹ The FTC first requires this security mechanism in its March enforcement action against CafePress. *See* CafePress Decision and Order ¶ 7 (requiring use of multi-factor authentication in place of security questions and answers).

Appendix 10



OPEN MARKETS

LIBERTY ★ DEMOCRACY ★ PROSPERITY

FOR IMMEDIATE RELEASE: Tuesday, Apr. 26, 2022

CONTACT: Roberto Hylton, roberto@npagency.com

OMI STATEMENT ON ELON MUSK AND TWITTER

WASHINGTON - *In response to Elon Musk buying Twitter Open Markets Institute Director Barry Lynn issues the following statement:*

Yesterday Twitter's board agreed to sell the corporation to Elon Musk, the owner of Tesla and SpaceX. The Open Markets Institute believes the deal poses a number of immediate and direct threats to American democracy and free speech. Open Markets also believes the deal violates existing law, and that the Federal Communications Commission (FCC), the Department of Justice (DOJ), and the Federal Trade Commission (FTC) have ample authority to block it.

The most obvious problem is that the deal would give to a single man – one who already wields immense political and economic power – direct control over one of world's most important platforms for public communications and debate. As has been true from the Founding, the American people have an absolute right to ensure the full openness and neutrality of all essential public infrastructure. Specific to communications, we see this in Article I, Section 8 of the Constitution, in the Telegraph acts of 1860 and 1866, the Mann-Elkins Act of 1910, the Communications Act of 1934, and many other federal and state laws. Americans have also repeatedly used our antitrust laws to prevent concentrations of power over communications, speech, debate, and news.

Yesterday's deal also violates the law at a more technical level. Mr. Musk already controls one of the most important internet platforms in the world – in the form of the satellite communications system Starlink. Since the late 19th Century, the U.S. government has routinely acted to prevent mergers between existing essential platforms. Most recently, the DOJ in 2017 attempted to block AT&T's takeover of Time-Warner (an effort which failed because the DOJ filed a poor case, as OMI made clear at the time). This means that just as we would now expect the U.S. government to block a takeover of Twitter by Google, Facebook, Comcast, or Verizon, the same rules apply to the owners of Starlink.

Let's be clear. Elon Musk's effort to buy Twitter is not the only threat to free communications and debate in the United States. The size, scope, and business models of Facebook, Google, and Amazon also pose a wide variety of often extreme threats to American democracy and the basic rights of citizens. That's why law enforcers and Congress should view this deal as an opportunity to firmly reestablish clear bans on any manipulation of communications by essential platforms, and to eliminate all business models that rely on such manipulation.

Finally, as Open Markets made clear in [this article](#) in the Washington Monthly, it's past time for the FCC to get serious about regulating Starlink to ensure that this vital and increasingly important Internet platform serves the public interest only.

Appendix 11



Office of the Chair

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Final Report 1655

June 24, 2022

The Honorable Jim Jordan
Ranking Member
Committee on the Judiciary
U.S. Houses of Representatives
Washington, D.C. 20515

Dear Ranking Member Jordan:

Thank you for your May 24, 2022, letter regarding the proposed acquisition of Twitter by Elon Musk. Generally speaking, the goal of every FTC merger review is to determine whether the transaction violates the antitrust laws.

Below are the responses to the three informational requests presented in your letter:

1. ***All documents and communication between or among the Federal Trade Commission and any third-party organizations referring or relating to Mr. Musk's purchase of Twitter.***

The only responsive document to this request is enclosed.

2. ***All documents and communication between or among the Federal Trade Commission and members and staff of the White House Competition Council referring or relating to Mr. Musk's purchase of Twitter.***

Inter-governmental discussions generally are protected under various exemptions, including the deliberative-process privilege, attorney-client privilege, and attorney work product privilege. In addition, the Commission's longstanding policy is that if the agency receives a legally binding request that may require the disclosure of information protected by executive privilege, the FTC will inform the White House so that the President can decide whether to invoke executive privilege.

3. ***All documents and communications, including all plans, proposals, or other communications, referring, or relating to the FTC's purpose in making inquiries related to Mr. Musk's purchase of Twitter that deviate from typical reviews.***

There are no such documents or communications.

Thank you again for your letter. If you have any questions, please feel free to have your staff call [REDACTED] the Director of our Office of Congressional Relations, at [REDACTED] [REDACTED]

Sincerely,



Lina M. Khan
Chair, Federal Trade Commission

Enclosure



COMPUTER INFORMATION ALLIANCE FOUNDATION
 400 NORTH TAMPA ST, 15TH FL, TAMPA, Floor, 33602
 9544447408
 cio-alves@minixel.com
<https://oneye.us>

Federal Trade Commission. Bureau of Competition
 Office of Policy and Coordination, Room CC-5422
 Bureau of Competition, 600 Pennsylvania Ave., NW
 Washington, DC 20580, Telephone: (202) 326-3300

April 26, 2022

Dear Federal Trade Commission,

As we all know, the mission of the FTC, as defined by Congress, is *“to protect consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity.”* With the above statement in mind is that I am writing to you to respectfully demand that Citizen Elon Musk be stopped from buying and taking private the so far public company called Twitter, INC.

Your duty as a Federal Agency, is, above all, to protect the American economy from predatory actors and preclude fraud by establishing rules that make it hard to create havoc in the life of millions of investors. It happens that this operation will doom the company, and it will cause a hole of \$US 43 BN in banks, pensions funds, mutual funds, etc., but in the end, the money will be lost to the American people. How do I know this? Citizen Musk is NOT buying he company outright, with his own money, he is borrowing some \$US 43 BN, and the interest alone to service this loan is estimated to be \$US 2.5 BN/year, more than double the available Twitter’s revenue after direct operating expenses. The Commission may verify these figures against the public filings and also it may request details of the transaction from Citizen Musk. This is an absolutely unacceptable model, and the FTC must step in and forbid the actors to commit what constitutes a fraud against the American people. Furthermore, being a private company, the new Twitter, INC, will not be able to sell shares in the public market to raise capital and cover temporary operating losses. Private banks will never lend money to a business that is unable to service its existing debt. This is a Kamikaze operation and it must be stopped.

Yours truly
 Federico Alves
 President, CIAF

Appendix 12

Open Markets Institute Statement in response to Elon Musk Buying Twitter

October 27, 2022 - *Press Releases, Public Comments - Lynn's Musings*



FOR IMMEDIATE RELEASE: October 27, 2022

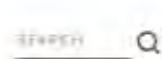
CONTACT: Ashley Woolhiser woolhisa@openmarketsinstitute.org

In response to Elon Musk buying Twitter Open Markets Institute Director Barry Lynn issues the following statement:

WASHINGTON- "The Open Markets Institute believes Elon Musk's deal to buy Twitter poses a number of immediate and direct threats to American democracy, free speech, and national security. Open Markets believes the deal violates existing law and that the Department of Justice (DOJ), Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) each have ample authority to block it. We also believe the Securities and Exchange Commission (SEC), Department of Defense (DOD), and the Committee on Foreign Investment in the U.S. (CFIUS) each have a duty to vet this takeover closely.

The most obvious problem is that the deal would give to one man – who already wields enormous economic and political power – direct control over one of world's most important platforms for public communications and debate. As has been true from the Founding, the American people have both an absolute right and responsibility to regulate all essential public communications infrastructure to ensure its full openness and neutrality, and freedom from foreign influence.

And let's be clear, Elon Musk is no run-of-the-mill billionaire. In recent months he has repeatedly meddled in delicate foreign policy issues in ways that demonstrate a seeming disregard for the security of the United States and its closest allies in a time of war and economic conflict. This includes shutting down his Starlink satellite system in certain parts of Ukraine, in ways that appear to support Russian and Chinese interests and demands. And it includes undermining U.S. policy on Taiwan at a moment when China is threatening to invade or blockade that island. In reporting these actions, the New York Times this week described Musk as a "geopolitical chaos agent."



Then there's the fact that Musk has exploited Twitter and other communications platforms to engage in fraudulent misrepresentations of his own businesses, as he admitted in 2018 in a settlement with the SEC. And just this week Reuters reported that the DOJ is investigating Tesla for fraudulent statements about its autopilot system.

Specific to domestic communications, Musk's statements on Twitter's regulation of its own platform show a basic misunderstanding of how the United States protects freedom of expression. In addition to using our antimonopoly laws to prevent concentrations of power over communications, speech, debate, and news, Americans also use both private and public regulation to ensure platforms are not used to promote violence or spread dangerous disinformation, as Donald Trump used Twitter to do.

One way law enforcers can move swiftly to block Musk's takeover of Twitter is to focus on his existing ownership of Starlink. As its use in Ukraine demonstrates, Starlink has become one the most important communications platforms in the world. Since the late 19th Century, the U.S. government has routinely acted to ensure the separation of essential platforms. This includes the 1913 order to AT&T to spin off Western Union, the 1956 consent decree with AT&T that blocked a move into publishing, and most recently, the DOJ's 2017 attempt to block AT&T's takeover of Time-Warner (an effort which failed only because the DOJ filed a poor case, as OMI made clear at the time). Just as we would now expect law enforcers to block a takeover of Twitter by Google, Facebook, Comcast, or Verizon, the same rules apply to the owners of Starlink.

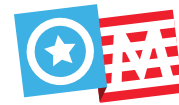
Elon Musk's effort to buy Twitter is not the only threat to free communications and debate in the United States. The size, scope, and business models of Google, Amazon, and Facebook also pose a wide variety of threats to American democracy and the basic rights of citizens. That's why law enforcers and Congress should also view this deal as a big step towards eliminating all business models that rely on the manipulation of communications, commerce, and debate."

Lynn also commented in April on Musk's initial plans to purchase the social media site, outlining why the deal would both pose risks to democracy and free speech and violate existing antitrust law. Since then Musk's reckless engagement in national security matters has made it even more clear why the public must block his effort to capture control over this essential public communications platform

###

The Open Markets Institute is a team of journalists, researchers, lawyers, economists, and advocates working together to expose and reverse the stranglehold that corporate monopolies have on our country.

Appendix 13



November 16, 2022

To: Jonathan Kanter
Assistant Attorney General, Department of Justice Antitrust Division

Jessica Rosenworcel
Chair, Federal Communications Commission

Lina Khan
Chair, Federal Trade Commission

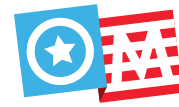
The Open Markets Institute respectfully calls on your offices to fully investigate Elon Musk’s takeover of the communications platform Twitter. The deal raises many fundamental questions about the independence and integrity of essential communications services in America.

No democracy can survive if its citizens allow one or few private individuals to seize control over the public square or public marketplace, or any platform or network essential to the ability of citizens to speak with and do business with one another. Citizens of democracies therefore have an absolute right and duty to protect the independence, neutrality, and economic wellbeing of every communications and commercial platform and network.

It is vital to move swiftly. The Twitter platform long ago proved it serves a unique and irreplaceable role in enabling citizens to communicate and to debate key issues of the day.¹ Twitter’s character as a utility is even more clear when we look at how the platform has been used during emergencies such as Hurricane Ian in Florida, earthquakes in Mexico and Japan, floods in Pakistan, and fires in Australia. In the company’s own words, “Over the years, Twitter has become a critical communication tool for responding to natural disasters.”² One way it does so is by creating a “centralized source of credible information.”³

Yet now, people in the United States and around the world are watching a single man radically alter this essential communications platform to favor his own personal interests and political views. And indeed, since Mr. Musk took control of Twitter on October 27, there are many well-documented reports that he or people working for him have interfered directly in public debate on that platform.⁴ Similarly, people across the United States and around the world are watching Mr. Musk potentially destroy – out of greed, recklessness, or incompetence – a service that has proven critical to their safety, and around which they have institutionalized entire systems of emergency response.

A second reason to move immediately is that Mr. Musk controls the satellite-based Internet service provider Starlink. Although as yet unfinished, Starlink in recent months has proven to be a highly effective technology, one that is of critical importance to the security of the United States, its citizens, and to allies such as the Ukraine and Taiwan.⁵ Over this same period,



however, Mr. Musk has repeatedly interfered in the normal operations of Starlink in ways that appear to promote his personal economic and political interests.⁶ It is therefore anything but inconceivable that Mr. Musk will manage Starlink in ways that disrupt Twitter, or vice versa.

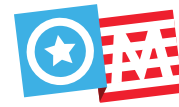
We fully understand that this deal does not fit easily into some of the categories your agencies have relied on in recent years to determine when and how to investigate takeovers or certain corporate actions. But we are very confident that each of your agencies has ample authority to fully review this takeover, and if necessary to unwind or restructure the deal and/or regulate the actions of the combined corporations. The Department of Justice played exactly such a role with America's main telephone corporation, AT&T, in 1913, 1956, and 1982.⁷ The American people created the Federal Communications Commission precisely to guarantee the independence and integrity of our communications platforms and news and entertainment media⁸ (including, in 2018, Starlink).⁹ And the Federal Trade Commission has routinely acted to ensure that industries vital to democracy are protected from the concentration and misuse of private power.¹⁰ Over the years this includes newspapers, book publishing, and online communications platforms (including, in 2011, Twitter).¹¹

Indeed, the FTC's statement on November 10, 2022 that it intends to use the original text of the Federal Trade Act of 1914 to guide enforcement of the "federal ban on unfair methods of competition" provides an excellent model for all three agencies to adopt in assessing the nature of the threats posed by Mr. Musk's takeover of Twitter, and for cataloging the many authorities available to address those threats.¹²

Ultimately, your responsibility derives from the Constitution itself. As Supreme Court Justice Anthony M. Kennedy wrote in 1994, "The First Amendment's command that government not impede the freedom of speech does not disable the government from taking steps to ensure that private interests not restrict, through physical control of the critical pathway of communication, the free flow of information and ideas."¹³

You are not alone in having a duty to review this combination and to act to protect our democracy and security. At least six other departments, agencies, and offices have a responsibility to work with you on a thorough investigation of Mr. Musk's takeover and management of Twitter, and his management of Starlink: the Committee on Investment in the United States (CFIUS), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB), the Department of Defense, the Department of Treasury, and the Federal Reserve.

That said, only your agencies have the ability to lead and coordinate this investigation. Your offices and staffs are uniquely equipped to: 1) identify threats to freedom of expression and freedom of the press posed by dangerous forms of vertical integration and arbitrary and discriminatory provision of services; 2) wield a wide and sophisticated range of regulatory tools to address such threats; 3) help other departments and agencies understand such threats and how to use their own authorities to protect democracy and the public interest; and 4) establish rules that empower citizens to safely benefit from the full promise of new technologies.



We believe the following goals should guide your work and that of the other offices in the U.S. government with whom you partner:

- Ensuring the complete independence of Twitter and Starlink from foreign interests.
- Ensuring the complete Independence of Twitter and Starlink from other business interests.
- Protecting all communications and political debates on Twitter and Starlink from any interference by Twitter and Starlink executives, board members, and employees.
- Ensuring both Twitter and Starlink establish clear terms of service for all users, and enforce those terms without prejudice or discrimination, in a completely transparent fashion.
- Ensuring that present management of Twitter and Starlink does not pose any avoidable threat to the stability and viability of Twitter Starlink.
- Protecting the interests and properties of Twitter users, who are the people who built that platform into an essential communications network.
- Protecting the privacy of every Twitter and Starlink user.
- Protecting small and medium-scale investors in Twitter, SpaceX/Starlink, and Tesla.
- Preventing any use of the Twitter and Starlink platforms to sidestep financial and monetary regulatory regimes, or to promote dangerous speculation.
- Preventing any leveraging of the monopoly nature of the Twitter and Starlink platforms to concentrate power over other businesses and markets.

There is no reasonable excuse for delay. On its own, an investigation by CFIUS into ownership of Twitter is not sufficient.¹⁴ The same is true for FTC enforcement of its consent decree with Twitter on privacy.¹⁵ The same is true The public has a right to know that the U.S. government is investigating *every* potentially troublesome aspect of this deal, and using *every* existing authority to ensure that the managers of Twitter and Starlink neither misuse nor destroy either platform.

It is important to state that our aim in writing you is not to target Mr. Musk personally. No matter who controlled Starlink and Twitter, we would call for the same close review of any deal involving these two entities.

In ending, it's worth remembering Justice Hugo Black's assurance in 1945 that enforcement of antimonopoly law against powerful communications platforms does not, in any respect, constitute regulation of speech or of the press. On the contrary, as Justice Black said, "it would be strange indeed... if the grave concern for freedom of the press which prompted adoption of the First Amendment should be read as a command that the government was without power to protect that freedom."¹⁶

Thank you.

The Open Markets Institute.



¹ As Lydia Polgreen of the *New York Times* put it, "Musk is right that the world needs a digital public square; unfortunately, he seems to have little idea that creating one involves balancing free speech against abuse, misinformation and government overreach. Twitter had just barely managed to get the hang of that difficult, important work in the past couple of years. Musk has left little doubt that rather than continue that work, he'd rather burn it all down." *If You Want to Understand How Dangerous Musk Is, Look Outside America*, NEW YORK TIMES (Nov. 14, 2022).

² *When Natural Disasters Happen, Twitter Can Be Used to Help. Here's How*, TWITTER (Oct. 13, 2022), https://blog.twitter.com/en_us/topics/company/2022/when-natural-disasters-happen-twitter-can-help-heres-how.

³ *Id.*

⁴ Barbara Ortutay, *Musk's Partisan Tweets Call Twitter Neutrality into Question*, AP NEWS (Nov. 7, 2022), <https://apnews.com/article/elon-musk-twitter-inc-technology-cbd873f1>.

⁵ See Alex Marquardt, *Musk's SpaceX Says It Can No Longer Pay For Critical Satellite Services in Ukraine, Asks Pentagon to Pick Up the Tab*, CNN (Oct. 14, 2022), <https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine>; see also Karina Tsui, *Taiwan, Looking to Ukraine, Pursues Internet Backup*, WASH. POST (Oct. 6, 2022), <https://www.washingtonpost.com/world/2022/10/06/taiwan-ukraine-satellite-interent-china-russia/>.

⁶ Mehul Srivastava et al., *Ukrainian Forces Report Starlink Outages During Push Against Russia*, FIN. TIMES (Oct. 7, 2022), <https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397>.

⁷ See Daniel A. Hanley et al., *Financing Free Speech: A Typology of Government Competition Policies in Information, Communication, and Media Markets*, CTR. FOR JOURNALISM & LIBERTY 5-6, 10-11 (Sept. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4089870.

⁸ Daniel A. Hanley, *Administrative Antimonopoly*, OPEN MARKETS INST. 7 (Feb. 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4044077.

⁹ *Why Are We Letting Monopolists Corner Space?* Luke Goldstein, Washington Monthly, Nov./Dec. 2021.

¹⁰ See generally Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 U. PA. J. BUS. L. 645 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830702.

¹¹ American citizens have used their state and federal governments to guarantee the neutrality and financial stability of electronic communications systems since passing the first laws regulating telegraph services in the mid-19th century. See RICHARD R. JOHN, NETWORK NATION: INVENTING AMERICAN TELECOMMUNICATIONS (2010); see, e.g., Act of July 1, 1862, § 15, 12 Stat. 489 (1862).

¹² *FTC Restores Rigorous Enforcement of Law Banning Unfair Methods of Competition*, FTC, Nov. 10, 2022.

¹³ *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 657 (1994).

¹⁴ *Musk's Foreign Investors in Twitter Are "Worthy" of Review*, Biden Says, Rebecca Kern, Politico, Nov. 9, 2022.

¹⁵ *In the Matter of Twitter, Inc.*, 151 F.T.C. 162 (2011).

¹⁶ *Associated Press v. United States*, 326 U.S. 1 (1945)

Appendix 14

PRESS STATEMENT DEC 21, 2022

STATEMENT: The FTC, Congress, and Advertisers Must Hold Elon Musk and Twitter Accountable, Say Progressive Groups

CONTACT



Julia Cusick

Restoring Social Trust in Democracy



Washington, D.C. — In his latest erratic behavior since buying Twitter, Elon Musk suspended several journalists, then abruptly reinstated some. In response, 14 groups issued the following statement:

As organizations deeply attached to democracy, to our freedom of expression, and to our fundamental rights, we cannot remain silent about Elon Musk's reckless decision to suspend numerous journalists' Twitter accounts. The reversal of some of these suspensions over the weekend does not diminish this attempt to silence journalists for simply doing their jobs.

Journalism is the cornerstone of free speech, and any attack on journalism is an assault on one of our fundamental pillars. While pretending to give power back to the people, Elon Musk is actually turning Twitter into an autocratic system where neo-Nazi accounts are restored while journalists' accounts are suspended. This is a dangerous turn that raises deep concerns. Journalists doing fact-based reporting have been a critical part of Twitter's success, and Elon Musk's apparent disdain for journalism and fundamental rights must be rebutted with clear shows of support from throughout civil society.

If Elon Musk is as committed to freedom of expression and democracy as he states, then it is not enough to reverse his incorrect decision; he also must guarantee appropriate safeguards to protect journalists and voices of interrogation and dissent on his platform, even and especially when he is the one they may be holding accountable.

While Musk may own Twitter, we all have a role to play in ensuring accountability on the platform:

1 All advertisers should take notice of these dangerous actions and ensure Elon Musk does not profit from dismantling one of the world's most influential communications platforms.

2 The Federal Trade Commission (FTC) should determine if any of Musk's actions since taking over Twitter—including broken public promises around the site's terms of service and efforts to protect users' privacy and safety—violate the company's existing consent decree or any other laws enforced by the commission. The commission should share those findings with the public.

3 Congress should move quickly to hold hearings on this incident and the potential for a privately held forum for national dialogue to endanger journalism and U.S. democracy. It should also explore potential remedies.

The undersigned,

Accountable Tech
AFL-CIO
American Federation of Teachers
Center for American Progress
Common Cause
Indivisible
GLAAD
Media Matters for America
MoveOn
National Education Association
National Women's Law Center
Public Citizen
Public Knowledge
SEIU

Appendix 15



November 17, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan,

We write regarding Twitter’s serious, willful disregard for the safety and security of its users, and encourage the Federal Trade Commission (FTC) to investigate any breach of Twitter’s consent decree or other violations of our consumer protection laws.

In recent weeks, Twitter’s new Chief Executive Officer, Elon Musk, has taken alarming steps that have undermined the integrity and safety of the platform, and announced new features despite clear warnings those changes would be abused for fraud, scams, and dangerous impersonation. According to media reports, in prioritizing increasing profits and cutting costs, Twitter’s executives have dismissed key staff, scaled back internal privacy reviews, and forced engineers to take on legal liability for new changes — preventing managers and staff tasked with overseeing safety and legal compliance from reviewing the product updates.¹ Moreover, key Twitter executives responsible for the platform’s privacy, cybersecurity, and integrity resigned last week, further calling into question whether personal data is adequately protected from misuse or breach while the company explores new products and monetization strategies.²

Users are already facing the serious repercussions of this growth-at-all-costs strategy. Since the launch of the verification feature over a decade ago, Twitter users have come to rely on the blue checkmark as an assurance that prominent users are who they claim to be — the most clear sign that an account is trustworthy. When Mr. Musk announced plans to open Twitter’s verification services to all paying users, experts warned the change would exacerbate the

¹ “Two Weeks of Chaos: Inside Elon Musk’s Takeover of Twitter.” New York Times.
<https://www.nytimes.com/2022/11/11/technology/elon-musk-twitter-takeover.html>

² “Twitter’s Security And Privacy Leaders Quit Amidst Musk’s Chaotic Takeover.” Forbes.
<https://www.forbes.com/sites/thomasbrewster/2022/11/10/twitter-security-privacy-compliance-leads-quit-elon-musk-takeover/>

platform’s already rampant problems with financial scams, foreign disinformation, and public safety threats.³ These misguided changes come at a time when Twitter is facing coordinated campaigns of racist, misogynistic, and antisemitic harassment, attempting to exploit the change in ownership to spread hate and vitriol.⁴

Despite these warnings, Mr. Musk pressed ahead and launched the feature, resulting in fake accounts impersonating President Biden, Senators, athletes, companies, and others.⁵ Of particular concern, these fake accounts included scammers impersonating companies and celebrities for cryptocurrency schemes, identity theft, and other financial crimes.⁶ Twitter knew in advance that there was high likelihood the Twitter Blue product could be used for fraud, and still it took no action to prevent consumers from being harmed until this rampant impersonation became a public relations crisis.⁷

We are concerned that the actions taken by Mr. Musk and others in Twitter management could already represent a violation of the FTC’s consent decree, which prohibits misrepresentation and requires that Twitter maintain a comprehensive information security program. The FTC was already on notice, even prior to Mr. Musk’s acquisition, about Twitter’s recent inadequate security practices based on whistleblower disclosures by Twitter’s former Security Lead Peiter “Mudge” Zatkó.⁸ Earlier this year, Twitter agreed to pay \$150 million to settle allegations by the FTC and the Department of Justice that Twitter violated the Federal Trade Commission Act and its 2011 consent decree with the FTC by deceiving users about the company’s privacy and security practices.⁹ We fear that Mr. Musk’s reported changes to internal reviews and data security practices further put consumers at risk and could directly violate the

³ “Elon Musk wants Twitter users to pay to be verified. It could create a new set of headaches for the company.” CNN. <https://www.cnn.com/2022/11/03/tech/elon-musk-twitter-verification-plans>

⁴ “Antisemitic campaign tries to capitalize on Elon Musk’s Twitter takeover.” New York Times. <https://www.nytimes.com/2022/10/28/technology/musk-twitter-antisemitism.html>

⁵ Letter from Senator Markey to Twitter Chief Executive Officer Elon Musk. <https://www.markey.senate.gov/news/press-releases/senator-markey-demands-answers-from-twitter-on-disinformation-and-fake-accounts>

For \$8, Twitter Blue users create a wave of checkmarked imposter accounts. Ars Technica. <https://arstechnica.com/gaming/2022/11/twitter-scammers-use-musks-paid-checkmarks-to-spread-official-looking-fake-news/>

⁶ “Elon Musk’s Twitter Is a Scammer’s Paradise.” Wired. <https://www.wired.com/story/twitter-blue-check-verification-buy-scams/>

⁷ “Elon Musk wants Twitter users to pay for their blue checks. What could possibly go wrong?” NBC News. <https://www.nbcnews.com/think/opinion/elon-musk-just-changed-meaning-twitters-coveted-blue-check-rcna55121>

⁸ Letter from Senator Blumenthal to the Federal Trade Commission. <https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-calls-on-ftc-to-investigate-twitter-whistleblower-claims>

⁹ “Twitter to pay \$150 million penalty for allegedly breaking its privacy promises – again.” Federal Trade Commission. <https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again>

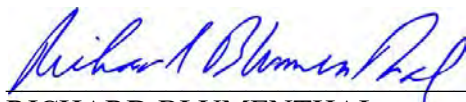
“Twitter Agrees with DOJ and FTC to Pay \$150 Million Civil Penalty and to Implement Comprehensive Compliance Program to Resolve Alleged Data Privacy Violations.” Department of Justice. <https://www.justice.gov/opa/pr/twitter-agrees-doj-and-ftc-pay-150-million-civil-penalty-and-implement-comprehensive>.

requirements of the consent decree. One Twitter lawyer was concerned enough about potential legal violations and management’s attitude toward the consent decree that they advised colleagues to seek legal counsel.¹⁰

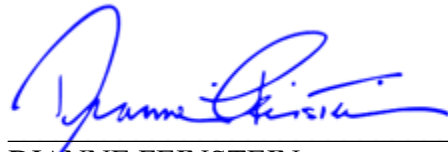
We urge the Commission to vigorously oversee its consent decree with Twitter and to bring enforcement actions against any breaches or business practices that are unfair or deceptive, including bringing civil penalties and imposing liability on individual Twitter executives where appropriate. As you recently noted in Senate testimony, “no CEO or company is above the law, and companies must follow our consent decrees.”¹¹

Thank you for your attention to this important matter.

Sincerely,



RICHARD BLUMENTHAL
United States Senate



DIANNE FEINSTEIN
United States Senate



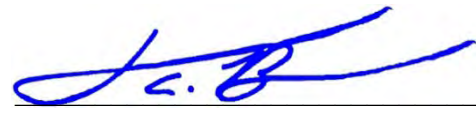
BEN RAY LUJÁN
United States Senate



ELIZABETH WARREN
United States Senate



EDWARD J. MARKEY
United States Senate



CORY A. BOOKER
United States Senate



ROBERT MENENDEZ
United States Senate

¹⁰ “Elon Musk is putting Twitter at risk of billions in fines, warns company lawyer.” The Verge.

<https://www.theverge.com/2022/11/10/23451198/twitter-ftc-elon-musk-lawyer-changes-fine-warning>

¹¹ FTC Chair Lina M. Khan Testifies Before Senate Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights. Federal Trade Commission. <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-chair-lina-m-khan-testifies-senate-judiciary-subcommittee-antitrust-competition-policy-consumer-rights>



The Weaponization of the Federal Trade Commission Part II: Harassment of Elon Musk

Interim Staff Report of the
Committee on the Judiciary
U.S. House of Representatives



October 28, 2024

EXECUTIVE SUMMARY

The Committee on the Judiciary has been investigating the politicization of the Federal Trade Commission (FTC) under far-left Chair Lina Khan. This report details new information about the weaponization of the Biden-Harris FTC, under Chair Khan’s direction, against Elon Musk following his acquisition of social media platform Twitter.¹ Based on new documents obtained from the FTC, the evidence is stark that—contrary to Chair Khan’s denials—the FTC finalized a consent decree against Twitter due to Musk’s pending acquisition. Documents show that although the FTC had been considering potential enforcement for years prior to the acquisition, Chair Khan called for an immediate vote to finalize the consent decree only days after Twitter’s board announced the deal. One contemporaneous email from an attorney advisor to Chair Khan makes the FTC’s motivation crystal clear: “The urgency is due to Elon Musk’s purchase of the company this week.”²

This report builds on the Committee’s growing body of evidence that Chair Khan has politicized the FTC, centralized power and control in her office, and made decisions that undermine the credibility and legitimacy of the FTC as a nominally independent federal agency. In March 2023, the Committee issued a report detailing how the FTC used its consumer protection authority and an ongoing consent decree as a pretext to harass Twitter in the months following Elon Musk’s acquisition of the company.³ The Committee exposed how the Biden-Harris FTC sought detailed information about journalists working to “expose abuses by Big Tech and the federal government.”⁴ With Chair Khan’s support, FTC staff sought sensitive operational information about every department in Twitter, regardless of whether the department had anything to do with privacy or data security, among other burdensome demands.⁵ The Committee documented how the FTC’s effort was an inherently politically motivated attempt to stifle Twitter at a time when Musk was taking steps to “reorient Twitter around free speech.”⁶

In a separate report in February 2024, the Committee detailed how Chair Khan has neglected and mismanaged the agency “in furtherance of her personal pursuit of political and ideological aims.”⁷ After reviewing documents produced by the FTC and interviewing career managers who revealed major leadership deficits at the FTC, the Committee reported that Chair Khan consolidated power in the Chair’s Office, ignored warnings from career staff, and limited operational transparency within the agency.⁸ The Committee also found that Chair Khan’s indecision on important, time-sensitive cases along with her tendency to make decisions “for

¹ In April 2023, Twitter, Inc. was renamed “X Corp.” For simplicity, this report refers to the company as Twitter throughout because that was the name of the company at the time of the events in question. See Derek Saul, *Twitter Tells Corporate Partners It’s Now X Corp Amid Switch To ‘Everything App’*, FORBES (Apr. 18, 2023).

² FTC-TW000000875.

³ THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION: AN AGENCY’S OVERREACH TO HARASS MUSK’S TWITTER, INTERIM STAFF REPORT, COMM. ON THE JUDIC., U.S. HOUSE OF REPRESENTATIVES (Mar. 7, 2023) (hereinafter “2023 TWITTER HOUSE STAFF REPORT”).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ ABUSE OF POWER, WASTE OF RESOURCES, AND FEAR: WHAT INTERNAL DOCUMENTS AND TESTIMONY FROM CAREER EMPLOYEES SHOW ABOUT THE FTC UNDER CHAIR LINA KHAN, INTERIM STAFF REPORT, COMM. ON THE JUDIC., U.S. HOUSE OF REPRESENTATIVES (Feb. 22, 2024).

⁸ *Id.*

headlines” not only harmed the ability for the FTC to win cases and enforce the antitrust laws, but also cast into doubt whether a bipartisan competition enforcement agency can exist absent significant legislative overhaul.⁹ This oversight helped to inform the Committee’s consideration of legislative reforms to help address Chair Khan’s overreach.¹⁰

In this report, the Committee outlines how the FTC’s attacks on Elon Musk began immediately after Twitter’s board accepted Musk’s offer to buy the company.¹¹ New, nonpublic documents and information produced by the FTC provide a clear timeline of the FTC’s actions against Twitter both before and after Musk’s acquisition. They show that, after an agreed-upon consent decree was in place in March 2021 to provide additional privacy and security protections, the Biden-Harris FTC did not act for more than a year to finalize the consent decree.¹² Further, documents reveal that even though Republican Commissioners sought updates on the status of the Twitter consent decree, Chair Khan’s senior leadership withheld information about the agreed-upon consent decree from them until the days after Musk’s planned acquisition of the company was made public.¹³

On April 25, 2022, Twitter accepted Musk’s offer to acquire the company.¹⁴ Three days later, on April 28, 2022, an attorney advisor for Chair Khan sent an email to the other Commissioners’ offices requesting that they immediately vote the following day to approve a consent decree with Twitter and impose a modified privacy order on the company.¹⁵ Prior to this email, Chair Khan had not circulated a copy of the consent decree or a memorandum with FTC staff recommendations to the Republican Commissioners—despite having the consent decree all but finalized for over a year.¹⁶ In addition, despite repeated requests, FTC staff had not briefed the Republican Commissioners about contents of the proposed consent decree.¹⁷ In rushing to schedule the vote, Chair Khan sought to ignore the traditional three-week timeline to provide Commissioners sufficient time to understand all the information required for the vote, and instead proposed only a one-day review due to what her staff called “new developments.”¹⁸ When asked why Chair Khan demanded the immediate vote after months of inaction, other Commissioners were told that “[t]he urgency” that Chair Khan required “[was] due to Elon Musk’s purchase of the company [that] week.”¹⁹

⁹ *Id.*

¹⁰ See e.g. H.R. 7737, the One Agency Act, 118th Cong. (2024).

¹¹ *Infra* Section III.

¹² *Infra* Section II.

¹³ *Infra* Section III.

¹⁴ Press Release, Twitter, Inc., Elon Musk to Acquire Twitter (Apr. 25, 2022).

¹⁵ FTC-TW000003049.

¹⁶ Letter from James Kohm, Ass’t Dir., Enforcement Div., Bureau of Consumer Protection, Fed. Trade Comm’n to Douglas Geho, Chief Counsel for Administrative L., H. Comm. on the Judic. (May 12, 2023).

¹⁷ FTC-TW000003049. Chair Khan routinely applied this tactic, in a break from the long tradition of the FTC, which acted to both undermine staff morale and reduce efficiency in the agency. See, e.g. ABUSE OF POWER, WASTE OF RESOURCES, AND FEAR, *supra* note 7 at 9.

¹⁸ FTC-TW000003049.

¹⁹ *Id.*

FTC consent decrees settle claims of wrongdoing and impose specific requirements on a company.²⁰ A consent decree may last a period of ten years or more, require annual reporting on a company's compliance with the consent decree, impose fines on the company, and require certain actions by the company to correct the alleged violation of law.²¹ FTC lawyers can demand information from companies that have entered consent decrees and these companies must respond within a short period of time.²²

The consent decree, at that time, had been nearly three years in the making. In October 2019, Twitter self-reported a violation of its existing consent decree with the FTC and cooperated with a six-month investigation into its security practices.²³ By March 2021, Twitter and the FTC had tentatively agreed to a settlement to resolve the FTC's security and privacy concerns, but Acting-Chair Rebecca Slaughter did not act to finalize the consent decree.²⁴ When Chair Khan took over in June 2021, she ordered FTC staff to start again and renegotiate the consent decree.²⁵ In March 2022, after six additional months of renegotiation, Twitter and FTC staff again tentatively agreed to a consent decree that was virtually identical to the one from 2021.²⁶ The consent decree then sat dormant for an additional month before Twitter announced its sale to Musk,²⁷ which Chair Khan's advisor said prompted Chair Khan's demand for an immediate vote to finalize the settlement.²⁸

After the FTC voted to approve the consent decree, Chair Khan's FTC began harassing Twitter. As the Committee has previously documented, within the first three months of Musk's ownership of Twitter, the FTC sent a dozen letters containing 350 demands for documents and information—demands, such as every communication in the company by or about Elon Musk, that had little to do with the recently agreed-to consent decree. Musk sought a meeting with Chair Khan to better understand the nature of the FTC's concerns, but Chair Khan refused until Twitter fully complied with *all* the FTC's demands.²⁹ That is, Chair Khan refused to consider meeting with Musk absent Twitter's full compliance, even when, for example, Twitter's attorneys pointed out that not every communication to, from, or about Musk could reasonably contain information about Twitter's data security and privacy program.³⁰ The FTC claimed that Twitter was required to produce this material, because any "company-wide communications sent by or at the direction of Musk may contain relevant information," but it did not explain how it may be relevant to privacy and data security.³¹ The only reasonable explanation, then, for requiring *all* communications remotely related to Musk would be as a tool for the FTC to harass Musk.

²⁰ J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, *Consent Decrees: Is the Public Getting Its Money's Worth?*, Remarks before the XVIIIth St. Gallen International Competition Law Forum (Apr. 7, 2011), at 8.

²¹ *See, e.g., id.* *See also* Damien Kieran, *FTC Settlement: Our Commitment to Protecting Your Privacy and Security*, TWITTER (May 25, 2022).

²² *Division of Enforcement*, FED. TRADE COMM'N, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-enforcement> (last accessed Oct. 22, 2024).

²³ Letter from James Kohm, *supra* note 16.

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ FTC-TW000003049.

²⁹ FTC-TW000000849.

³⁰ FTC-TW000001636.

³¹ *Id.*

The FTC ultimately found nothing to give the Commission reason to believe Twitter, under Musk, failed to honor its compliance requirements pursuant to the consent decree or engaged in any other conduct to warrant further investigation.³² This is not surprising because, as Chair Khan should have been aware, early in his tenure as owner of Twitter, Musk relayed to every staff member at Twitter that “Twitter will do whatever it takes to adhere to both the letter and spirit of the FTC consent decree.”³³ Despite investigating Twitter’s compliance with the consent decree for more than a year, and despite Chair Khan’s barrage of harassing letters, the FTC found that Musk’s Twitter honored that commitment.³⁴

Evidence available to the Committee also suggests that Chair Khan misled the Committee. Chair Khan claimed in correspondence to the Committee that the Committee was “incorrect in asserting” that her decision to finalize the consent decree “was a result of Elon Musk’s anticipated acquisition of the company.”³⁵ Internal, contemporaneous FTC email correspondence proves otherwise.³⁶ Chair Khan also defended the rushed vote by asserting that “Twitter’s counsel urged the [FTC] to approve the order expeditiously.” This assertion, too, is misleading. Twitter initially expected the deal to be finalized in three to six months.³⁷ When Twitter sought to resolve the consent decree quickly following the announcement of Musk’s acquisition, it made the request to the Bureau of Consumer Protection, which did not relay the message to the Chair’s office until more than half a day *after* Chair Khan demanded an immediate vote on the consent decree.³⁸ It is therefore simply not accurate to assert that Chair Khan’s demand for an urgent vote on Twitter’s consent decree came at Twitter’s request because the evidence suggests Chair Khan did not know of Twitter’s preference until after she scheduled the vote.

The evidence shows that the Biden-Harris FTC finalized and adopted the stronger consent decree with Twitter, after a year of delay, only *after* news broke that Twitter’s board had accepted Musk’s offer to buy the social media company. The Biden-Harris FTC could have acted on the new consent decree earlier if it was simply good policy or if the FTC wanted to strengthen consumer protections on the platform. Instead, the evidence suggests that Chair Khan pressured her fellow Commissioners to finalize the consent decree with “the urgency required” solely because Elon Musk was taking over Twitter.

³² Cat Zakrzewski, *Employees Prevented Musk from Breaking Federal Twitter Order; FTC Finds*, WASH. POST (Feb. 21, 2024).

³³ FTC-TW000001638.

³⁴ Cat Zakrzewski, *supra* note 32.

³⁵ See Letter from Lina Khan, Chair, Fed. Trade Comm’n to Jim Jordan, Chair, H. Comm. on the Judic. (Jun. 22, 2023).

³⁶ FTC-TW000003049.

³⁷ FTC-TW000002155.

³⁸ *Id.*

TABLE OF CONTENTS

I. Background..... 6

II. FTC And Twitter: 2011 to 2022 9

III. Chair Khan’s Rushed Vote: “The urgency is due to Elon Musk’s purchase of the company this week.”..... 12

IV. Chair Khan’s False Excuses About the Consent Decree Vote..... 15

V. The FTC’s Continued Harassment of Musk’s Twitter Under Chair Khan 18

VI. Chair Khan’s Disregard for Congressional Oversight 21

VII. Conclusion..... 24

I. BACKGROUND

On March 7, 2023, the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government released a staff report documenting the FTC’s push, under Chair Lina Khan, to harass Elon Musk in the wake of his acquisition of Twitter.³⁹ The Committee had learned that, as soon as Musk acquired Twitter in October 2022, the FTC began an aggressive campaign to harass and undermine Twitter during the transition to Musk’s leadership.⁴⁰ The FTC’s overly aggressive salvos at Twitter following Musk’s acquisition mirrored other efforts by the Biden-Harris Administration to target Musk:⁴¹ the DOJ is investigating Tesla⁴² and SpaceX,⁴³ the SEC is policing his personal speech on Twitter,⁴⁴ and the FCC unilaterally revoked funding from Musk’s Starlink satellite business.⁴⁵ Musk’s sin, in the eyes of the Biden-Harris Administration, was a rededication of Twitter to fundamental free speech principles and a rejection of the growing embrace on the radical left of censorship.⁴⁶

The Committee obtained nonpublic information consisting of over a dozen letters sent by the FTC to Twitter within the first three months following Musk’s takeover of the company.⁴⁷ The Biden-Harris FTC used these letters to impose more than 350 different demands for documents and information, including a significant number of demands that fell outside the scope of the FTC’s consent decree.⁴⁸

This regulatory assault by the FTC appeared to be politically motivated.⁴⁹ As the Committee recounted, when Musk took steps to “reorient Twitter around free speech, the FTC regularly followed soon thereafter with a new demand letter.”⁵⁰ The FTC demanded every communication to, from, or about Elon Musk, and required that Twitter turn over information about every department in the company, regardless of whether the department had anything to do with user privacy or data security—the topics at issue in the consent decree.⁵¹ The FTC even demanded detailed information about Twitter’s work with independent journalists who were working to “expose abuses by Big Tech and the federal government.”⁵² “The FTC’s harassment of Twitter,” the Committee concluded, “is likely due to one fact: Musk’s self-described ‘absolutist’ commitment to free expression in the digital town square.”⁵³

³⁹ 2023 TWITTER HOUSE STAFF REPORT, *supra* note 3.

⁴⁰ *Id.*

⁴¹ *See generally*, Editorial Board, *The Harassment of Elon Musk*, WALL ST. J. (Sep. 22, 2023).

⁴² Tom Krisher, *Tesla Says Justice Department is Expanding Investigations and Issuing Subpoenas for Information*, AP (Oct. 23, 2023).

⁴³ Stuart Anderson, *SpaceX Court Win Could End DOJ Immigrant Lawsuits*, FORBES (Nov. 28, 2023).

⁴⁴ Lawrence Hurley, *Supreme Court Rejects Elon Musk’s Challenge to SEC Agreement to Vet His Social Media Posts*, NBC NEWS (Apr. 29, 2024).

⁴⁵ Editorial Board, *The FCC Ambushes Musk’s Starlink*, WALL ST. J. (Dec. 14, 2023).

⁴⁶ Liz Peek, *Biden’s Alarming Harassment of Elon Musk*, THE HILL (Dec. 15, 2023) (When asked about Musk’s acquisition of Twitter, Biden said the acquisition “is worth being looked at.”).

⁴⁷ 2023 TWITTER HOUSE STAFF REPORT, *supra* note 3 at 4.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.* at 1.

⁵¹ *Id.* at 2.

⁵² *Id.* at 5.

⁵³ *Id.* at 2.

Following the issuance of the Committee’s report revealing the weaponization of the FTC against Twitter, the Committee requested documents and information related to the FTC’s interactions with Twitter.⁵⁴ For nearly a year, the Committee faced significant pushback from Chair Khan and the Biden-Harris FTC.⁵⁵ Despite producing some limited documents, the FTC has continued to refuse to produce the highest priority documents that the Committee requested and still withholds its staff recommendation memoranda—the key documents that would directly inform the Committee’s oversight.⁵⁶ The Committee has made significant accommodations to facilitate the FTC’s production of this narrow set of materials, but Chair Khan still stubbornly refuses to make available the FTC staff recommendation memoranda that would provide the best, contemporaneous evidence for why the FTC targeted Musk’s Twitter.

Separately, the Committee has been investigating serious allegations of a toxic FTC work environment under Chair Khan. The Committee detailed how mismanagement at the FTC from current leadership harmed the ability of FTC staff to win cases and enforce the antitrust laws.⁵⁷ After reviewing documents produced by the FTC and interviewing career managers, the Committee found that Chair Khan neglected the FTC’s mission and mismanaged the agency “in furtherance of her personal pursuit of political and ideological aims.”⁵⁸ One manager candidly wrote: “I’m not sure being successful (or doing things well) is a shared goal, as the Chair wants to show that we can’t meet our mission mandate without legislative change.”⁵⁹ Another career manager wrote that Chair Khan “has a knee-jerk negative reaction to” FTC staff’s work, and staff is afraid to “say things or recommend outcomes because it will upset” the Chair.⁶⁰ Further, “managers expressed concerns about Chair Khan ‘directing complaint allegations against the evidence’ and sending staff into court ‘unprepared.’”⁶¹

Chair Khan’s mismanagement of the FTC has real-world consequences for Americans. During the Trump administration, the FTC initiated investigations and cases against the “largest and arguably most powerful companies in the world.”⁶² However, during the Biden-Harris Administration, the Committee found that:

Chair Khan’s radicalism, inexperience, and imprudence squandered the [Trump FTC’s] momentum and continues to hamper the ability of the FTC and career federal civil servants to do their jobs well on behalf of the American people. The documents and other information highlighted in this interim staff report show how the FTC under Chair Lina Khan is in chaos.⁶³

⁵⁴ Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm’n (Mar. 10, 2023).

⁵⁵ *See infra* Section VI.

⁵⁶ *Id.*

⁵⁷ ABUSE OF POWER, WASTE OF RESOURCES, AND FEAR, *supra* note 7.

⁵⁸ *Id.* at 1.

⁵⁹ *Id.* at 3.

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² *Id.* at 5.

⁶³ *Id.* at 5.

The FTC’s harassment of Twitter in the wake of Elon Musk’s acquisition is one plank in the left’s multi-faceted response to heightened attention of the censorship-industrial complex, which was first exposed by the Twitter Files journalists in December 2022.⁶⁴ Following his takeover of Twitter, Musk allowed journalists to expose the “lead role” that the government played in pressuring Twitter and other technology companies, such as Meta, to censor speech online.⁶⁵ Through its robust oversight of the Biden-Harris Administration’s censorship efforts, the Committee found that the Administration—up to and including White House employees—pressured technology companies to “change their content moderation policies,”⁶⁶ in large part because the technology companies had “other policy concerns” before the Administration.⁶⁷

⁶⁴ See THE CENSORSHIP-INDUSTRIAL COMPLEX: HOW TOP BIDEN WHITE HOUSE OFFICIALS COERCED BIG TECH TO CENSOR AMERICANS, TRUE INFORMATION, AND CRITICS OF THE BIDEN ADMINISTRATION, INTERIM STAFF REPORT, COMM. ON THE JUDIC., U.S. HOUSE OF REPRESENTATIVES (May 1, 2024) (hereinafter “INTERIM STAFF REPORT”).

⁶⁵ *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 Judic.*, 118th Cong. (Mar. 9, 2023) (testimony of Matt Taibbi); see also Letter from Mark Zuckerberg, CEO, Meta Platforms to Jim Jordan, Chair, H. Comm. on the Judic. (Aug. 26, 2024).

⁶⁶ INTERIM STAFF REPORT, *supra* note 64 at 2.

⁶⁷ *Id.* at 4.

II. FTC AND TWITTER: 2011 TO 2022

To understand how Chair Lina Khan and the Biden-Harris FTC weaponized its regulatory authority against Elon Musk and Twitter, it is necessary to examine the sequence of events that first subjected Twitter to the FTC's enforcement regime. The FTC's enforcement of Twitter's security and privacy policies began in 2011 when Twitter entered into a consent decree with the FTC.⁶⁸ The FTC's initial investigation followed two reports alleging that Twitter's privacy and data security policies were not sufficient to prevent hackers from gaining access to Twitter's administrative controls.⁶⁹ This 2011 consent decree "resolved charges that Twitter deceived consumers and put their privacy at risk by failing to safeguard their personal information."⁷⁰ As part of the consent decree, the FTC required an independent assessor to audit Twitter's privacy and data security protocols annually for 10 years.⁷¹

In October 2019, Twitter self-reported a violation of the 2011 consent decree to the FTC and agreed to fully cooperate with the FTC to investigate and resolve the situation.⁷² Twitter reported improper use of user information arising from instances where some user email addresses and phone numbers, collected to bolster account security, "may have been inadvertently used for advertising."⁷³

The Trump FTC undertook a six-month investigation to assess the scope of the breach, the risks of additional breaches, and the effectiveness of the remedies currently in place.⁷⁴ By May 2020, FTC's career staff completed the investigation and was prepared to recommend modifications to the 2011 consent decree that would require Twitter to meet higher privacy and security standards than those previously required.⁷⁵

In general, FTC consent decrees settle claims of wrongdoing and impose specific requirements on a company when the FTC "has reason to believe" that the party to the consent decree has violated the FTC Act.⁷⁶ In exchange for the FTC ceasing any litigation or an ongoing investigation against a company, the company can enter into a consent decree that imposes specific requirements on the company for a period of time.⁷⁷ For example, a consent decree may last a period of ten years or more, require annual reporting on a company's compliance with the consent decree, impose fines on the company, and require certain actions by the company to correct the alleged violation of law.⁷⁸ Additionally, FTC lawyers can demand information from

⁶⁸ Press Release, Fed. Trade Comm'n., FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2011).

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² Letter from James Kohm, *supra* note 16.

⁷³ Damien Kieran, *FTC Settlement: Our Commitment to Protecting Your Privacy and Security*, TWITTER (May 25, 2022).

⁷⁴ Letter from James Kohm, *supra* note 16.

⁷⁵ *Id.*

⁷⁶ J. Thomas Rosch, *supra* note 20.

⁷⁷ *Id.*

⁷⁸ *See, e.g., id. See also* Damien Kieran, *supra* note 73.

companies that have entered into consent decrees and the company must respond to these demands within a short period of time.⁷⁹

At that time, career staff briefed then-FTC Chair Joseph Simons and the other Commissioners, and in July 2020 the FTC authorized career staff to engage with Twitter to negotiate a settlement.⁸⁰ Twitter requested, and the FTC granted, a pause to the settlement discussions during the 2020 election.⁸¹ Negotiations resumed following the election and by March 2021, FTC staff and Twitter tentatively agreed to a new consent decree that would impose greater reporting requirements.⁸² Shortly thereafter, FTC staff recommended the new consent decree to the new Biden-Harris FTC leadership team for Commission approval.⁸³

In January 2021, Chair Joseph Simons resigned from the FTC,⁸⁴ and Commissioner Rebecca Slaughter, a Democrat appointee, became the Acting Chair of the Biden-Harris FTC.⁸⁵ For more than three months, Acting Chair Slaughter took no action to finalize the new consent decree. On June 15, 2021, immediately after she was confirmed by the Senate as a commissioner, President Biden elevated Lina Khan to be the Chair of the FTC.⁸⁶

According to information provided by the FTC, when Chair Khan assumed leadership of the Commission, she demanded that FTC staff renegotiate the new consent decree to obtain additional concessions from Twitter.⁸⁷ These renegotiation efforts were not a result of additional information collected by the FTC, new feedback from Commissioners, or any additional findings that the new consent decree was inadequate to remedy any privacy and data security concerns—Chair Khan simply ordered staff to renegotiate it.⁸⁸

Despite Chair Khan’s claims that the FTC won additional concessions through reopening negotiations, suggesting that her actions led to a stronger settlement, the individual leading the Twitter negotiations told the Committee that the negotiations did not lead to a stronger settlement.⁸⁹ According to James Kohm, the Associate Director of the Bureau of Consumer Protection’s Enforcement Division, “the FTC staff determined that [the FTC] was unable to obtain additional relief” from the reopened negotiations and staff briefed the Chair about the lack of success in January 2022.⁹⁰

On March 7, 2022, nearly a year after initially reaching an agreement, Twitter agreed to the revised consent decree, which was virtually identical to the tentative agreement from March

⁷⁹ *Division of Enforcement, supra* note 22.

⁸⁰ Letter from James Kohm, *supra* note 16.

⁸¹ *Id.*

⁸² *Id.*

⁸³ *Id.*

⁸⁴ Press Release, Fed. Trade Comm’n, FTC Chairman Simons Announces his Resignation and the Departure of Senior Staff (Jan. 19, 2021).

⁸⁵ Press Release, Fed. Trade Comm’n, FTC Commissioner Rebecca Kelly Slaughter Designated Acting Chair of the Agency (Jan. 21, 2021).

⁸⁶ Press Release, Fed. Trade Comm’n, Lina M. Khan Sworn in as Chair of the FTC (Jun. 15, 2021).

⁸⁷ Letter from James Kohm, *supra* note 16.

⁸⁸ *Id.*

⁸⁹ *Compare* Letter from Lina Khan, *supra* note 35 with Letter from James Kohm, *supra* note 16.

⁹⁰ Letter from James Kohm, *supra* note 16.

2021.⁹¹ On March 16, 2022, the new consent decree was sent to the Director of the Bureau of Consumer Protection for review, where it sat until news broke that Twitter's board had accepted Musk's offer to acquire the company on April 25, 2022.⁹²

The timeline is instructive in showing that the FTC had no urgency in attempting to enforce its consent decree with Twitter until after Musk bought the company. The FTC and Twitter had tentatively agreed to the terms of the new consent decree by March 2021, but the FTC did not move to settle the matter until over a year later. This slow pace stands in stark contrast with the sudden urgency following Musk's acquisition.

⁹¹ *Id.*

⁹² *Id.*

**III. CHAIR KHAN’S RUSHED VOTE:
“THE URGENCY IS DUE TO ELON MUSK’S PURCHASE OF THE COMPANY THIS WEEK.”**

On Monday, April 25, 2022, news broke that Musk entered an agreement to acquire Twitter, a major social media platform used worldwide.⁹³ The news prompted an immediate and vitriolic backlash from top Democrats.⁹⁴ For example, Senator Elizabeth Warren wildly claimed that “Musk purchasing Twitter is dangerous for our democracy.”⁹⁵ The Open Markets Institute, Chair Khan’s former employer, opposed the deal, going so far as to urge the FTC to “block” Musk from purchasing Twitter.⁹⁶ Shortly after Twitter accepted the terms, it was reported that the FTC was investigating whether the deal somehow violated the antitrust laws—even though Musk had no controlling holdings in any competing social media company.⁹⁷

Three days later, on the morning of April 28, 2022, the Secretary of the FTC distributed to the Commission the FTC’s Bureau of Consumer Protection recommendation memorandum concerning the revised consent decree with Twitter.⁹⁸ As a general matter, the staff recommendation memoranda contain in-depth legal and factual analyses, along with recommendations on options for proceeding, which include discussions of legal and policy risks for taking different courses of action. The recommendation memorandum often also includes additional evidence, such as economic analysis or business documents, as necessary to support the staff’s recommendations.

Prior to Chair Khan’s takeover, the practice of withholding information from Commissioners until the last second was extraordinarily rare, if not unprecedented. Traditionally, unless otherwise instructed by statute,⁹⁹ the FTC had afforded at least three weeks to allow Commissioners and their staff to review recommendation memoranda and related evidence and to receive any requested briefings so that their decisions can be fully informed.¹⁰⁰ Although Republican Commissioners had repeatedly requested—but had not received—the recommendation memorandum and the proposed consent decree, Chair Khan, through her attorney advisor, demanded an immediate vote to adopt the consent decree against Twitter.¹⁰¹

Documents obtained by the Committee reflect how Chair Khan sought to rush a decision on Twitter without allowing her fellow commissioners adequate time to review the material. Commissioner Noah Phillips was one of the commissioners who had previously asked about the status of the consent decree and sought access to the staff recommendation memos.¹⁰² By email,

⁹³ See Max Zahn, *A Timeline of Elon Musk’s Tumultuous Twitter Acquisition*, ABC NEWS (Nov. 11, 2022).

⁹⁴ Alexander Bolton, *Musk Buying Twitter Alarms Democrats*, THE HILL (Apr. 26, 2022).

⁹⁵ *Id.*

⁹⁶ Press Release, Open Market’s Institute, OMI Statement on Elon Musk and Twitter (Apr. 26, 2022).

⁹⁷ *Musk’s \$44 bln Buyout of Twitter Faces U.S. Antitrust Review*, REUTERS (May 5, 2022).

⁹⁸ FTC-TW000000875.

⁹⁹ For example, the Commissioners are bound by the timeline set forth in the Hart-Scott-Rodino Act when reviewing merger filings. See *Premerger Notification and the Merger Review Process*, FED. TRADE COMM’N, <https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/mergers/premerger-notification-merger-review-process> (last accessed Sep. 27, 2024).

¹⁰⁰ See FTC-TW000003049.

¹⁰¹ *Id.*

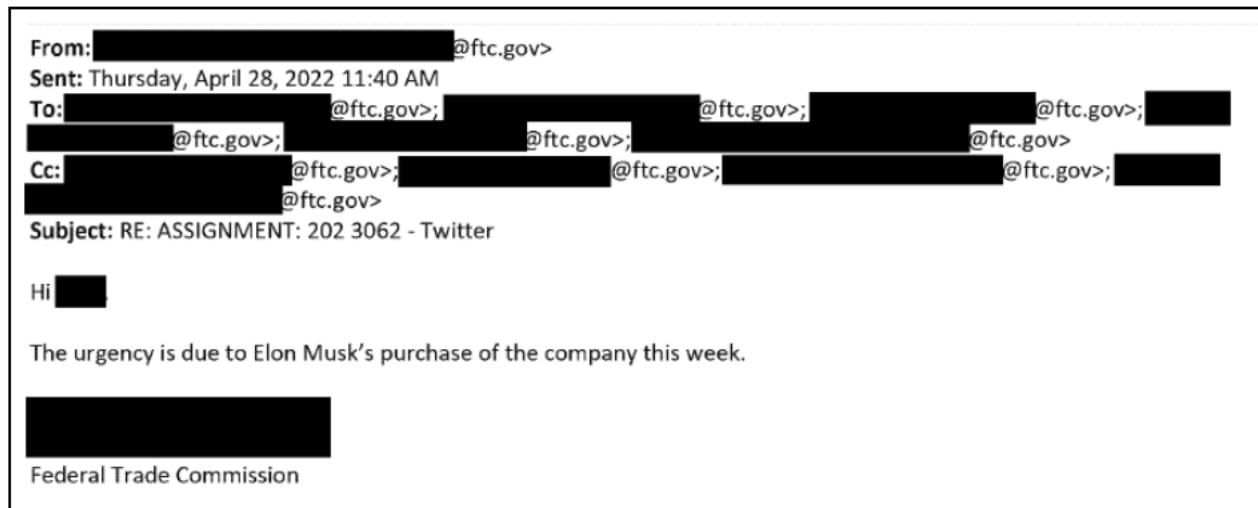
¹⁰² FTC-TW000000875.

Phillips’s attorney advisor asked for an explanation for Chair Khan’s sudden rush to vote, explaining that Commissioner Phillips had been regularly requesting to see a recommendation memo.¹⁰³ The attorney advisor for Commissioner Phillips wrote:

Given that this matter has been open for quite a while, what’s the urgency? Commissioner Phillips has been very interested in seeing this [recommendation] package and has been regularly asking about it in his meetings with [the Bureau of Consumer Protection], so he’d like to understand the issues that require an accelerated review. It’s an important case and he will want time to get any questions he might have answered and give it thoughtful consideration.¹⁰⁴

An attorney advisor for Commissioner Christine Wilson expressed similar concerns, writing: “We have repeatedly asked the Bureau about the status of this matter and for updates. This is an important matter for the Commission and she wants sufficient time to review it carefully and discuss with staff.”¹⁰⁵ According to her attorney advisor, Commissioner Wilson had been asking about the matter since at least late 2020.¹⁰⁶

Chair Khan’s attorney advisor replied to the group that “[t]he urgency is due to Elon Musk’s purchase of the company this week.”¹⁰⁷



Commissioner Phillips’s attorney advisor promptly responded seeking further explanation: “I am not trying to be dense, but could you spell that out a bit?”¹⁰⁸ The Chair’s office offered no substantive response and ultimately reiterated the Chair’s demand for quick action: “In light of new developments, this matter still requires urgent action . . . While I can

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ FTC-TW000003049.

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

understand there may be some frustration regarding prior delays with this matter, I hope that all [of the Commissioner’s] offices can cooperate and accommodate the urgency required here.”¹⁰⁹

From: ██████████@ftc.gov>
Sent: Thursday, April 28, 2022 11:45 AM
To: ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>
Cc: ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>; ██████████@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

██████████ handling for our office. I spoke with Commissioner Wilson and she will not be ready to vote tomorrow. She too has been in discussions with staff and BCP front office about this matter since Andrew Smith was Bureau Director. We have repeatedly asked the Bureau about the status of this matter and for updates. This is an important matter for the Commission and she wants sufficient time to review it carefully and discuss with staff.

As I understand it, resolution of this matter involves a number of steps – referral to DOJ, approval by a court, and then an amendment to the admin order by the Commission. As a result, it’s going to take some time so it would be helpful to understand how the Chair envisions the timeline for this matter.

Thanks,
 ██████████

That same day, the attorney advisor for Commissioner Wilson wrote that Wilson anticipated needing the “traditional three weeks to thoroughly review this matter,”¹¹⁰ to which Commissioner Phillips’s attorney advisor agreed and requested the standard timeline to review the proceedings.¹¹¹

Chair Khan’s attorney advisor seemed to ignore these concerns, and continued to pursue the expedited vote timeline, indicating that the latest date that Chair Khan would accommodate for a vote would be May 13, 2022—less than the customary three weeks.¹¹² On May 13, the FTC voted to accept the settlement agreement and referred the complaint to the Department of Justice (DOJ) as required by the FTC Act.¹¹³ On May 25, the DOJ filed the complaint in federal court on behalf of the FTC,¹¹⁴ and on May 26, the consent decree became effective.¹¹⁵

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ Letter from James Kohm, *supra* note 16.

¹¹⁴ Press Release, U.S. Dep’t of Just., Twitter Agrees with DOJ and FTC to Pay \$150 Million Civil Penalty and to Implement Comprehensive Compliance Program to Resolve Alleged Data Privacy Violations (May 25, 2022).

¹¹⁵ Letter from James Kohm, *supra* note 16.

IV. CHAIR KHAN'S FALSE EXCUSES ABOUT THE CONSENT DECREE VOTE

Throughout the Committee's investigation, Chair Khan has repeatedly claimed two things about the FTC's actions against Twitter, both of which are false based on documents produced to the Committee. First, Chair Khan claimed that the timing of Commission's vote on the revised consent decree was not because of Musk's planned acquisition of Twitter.¹¹⁶ Second, Chair Khan claimed that Twitter—and not the FTC—was the reason for the expedited finalization of the consent decree in advance of closing on the transaction with Musk.¹¹⁷

With respect to the role of Musk's acquisition in the timing of the FTC's actions, Chair Khan claimed that the Committee was “incorrect in asserting that the recommendation [to finalize the consent decree] was a result of Elon Musk's anticipated acquisition of the company.”¹¹⁸ However, Chair Khan's assertion that Musk's acquisition of Twitter did not impact the timing and urgency to finalize the consent decree is patently false: as her attorney advisor explained in an email, the only reason Chair Khan was seeking to adopt the consent decree on April 28, 2022, was “due to Elon Musk's purchase of the company” This contemporaneous document is directly contrary to Chair Khan's assertion to the Committee. To date, the FTC has not provided any evidence to demonstrate that Chair Khan intended to finalize the consent decree at all until immediately after Twitter announced Musk would purchase the company.

Chair Khan also claimed that the statement by two Republican Commissioners about the consent decree proves that the consent decree was not targeting Musk.¹¹⁹ When writing a statement about the settlement, Commissioners Phillips and Wilson observed that the *content* of the consent decree, in their opinion, had nothing to do with Musk's announced takeover of Twitter.¹²⁰ This statement about the substance is not surprising, given that the negotiated consent decree was all but finalized for over a year before Chair Khan decided to act. Commissioners Phillips and Wilson warned, however, that an “observer might ask what took so long, and why now.”¹²¹ As Commissioner Phillips and Wilson warned, it now appears that the *timing* of the consent decree was a result of an ulterior motive.

Chair Khan has also claimed that the FTC considered the expedited timeline at the behest of Twitter. In a letter to the Committee, Chair Khan represented:

On April 28, 2023, [*sic*¹²²] . . . Twitter's counsel urged the Commission to approve the order expeditiously, to resolve the outstanding issues in the interest of facilitating the acquisition and change in ownership to proceed smoothly. As is customary with companies, going through ownership changes, we considered

¹¹⁶ Letter from Lina Khan, *supra* note 35.

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ See Christine S. Wilson & Noah Joshua Phillips, Comm'rs, Fed. Trade Comm'n, *Concurring Statement: Twitter* (May 25, 2022).

¹²² Although Chair Khan indicated the year to be 2023, the consent decree was finalized in 2022.

whether it was possible to accommodate the request on an expedited timeframe.¹²³

Chair Khan's assertions, however, are not supported by the documents that the FTC produced to the Committee. At 10:10 a.m. on April 28, the Bureau of Consumer Protection staff working on the Twitter investigation and consent decree received notification that Chair Khan wanted to vote the next day to finalize the consent decree. Thirty minutes later, at 10:40 a.m., Chair Khan's attorney advisor informed the other Commissioners that Chair Khan wanted to vote the next day.¹²⁴ At 11:27 a.m., a Bureau of Consumer Protection staffer on the Twitter investigation team relayed a conversation the staffer had with Twitter's outside counsel that morning to other Bureau of Consumer Protection staffers, writing:

I spoke to [Twitter's outside counsel] this morning, and she said they plan to convey to DOJ during this afternoon's call that Twitter is especially anxious to get everything wrapped up soonest, given the recent Elon Musk developments. She said Twitter's goal is for this new FTC order to be entered and all done before Musk formally takes over (which is expected to happen in 3-6 months).¹²⁵

A couple of hours after this message, at 1:33 p.m., Monica Vaca, Deputy Director for the FTC's Bureau of Consumer Protection, wrote James Kohm asking to relay the message from Twitter's outside counsel to Chair Khan's office. Vaca wrote:

Can I convey to the Chair's office the conversation that [redacted] describes, below? They are trying to get a vote within a short period of time, i.e. a week, but Commissioner Phillips is asking for 3 weeks. This information about Twitter's time pressure could be relevant. What do you think?¹²⁶

The FTC has not provided any documents to the Committee showing that Kohm responded to Vaca's email.

Based on the FTC's documents, it is unlikely that Chair Khan knew about Twitter's request to finalize the consent decree at the time that demanded the immediate FTC vote.¹²⁷ The FTC has produced no documents reflecting that Twitter's outside counsel spoke directly with Chair Khan's office about the FTC's vote to finalize the consent decree on the morning of April 28. In addition, the contents of the emails that the FTC did produce would make no sense if Twitter had contacted the Chair's office directly. First, it would be unlikely that Twitter's outside counsel would indicate an intention to communicate with DOJ about the company's desire to "get everything wrapped up soonest" but fail to mention that Twitter had already spoken to the Chair's office. Second, Vaca's email at 1:33 p.m. asking for permission to inform the Chair's

¹²³ Letter from Lina Khan, *supra* note 35.

¹²⁴ FTC-TW000003049.

¹²⁵ FTC-TW000002155.

¹²⁶ *Id.*

¹²⁷ See Letter from Lina Khan, *supra* note 35; see also FTC-TW000003049.

office would be unnecessary if Twitter had already done so directly. Finally, the FTC itself represented to the Committee that the Chair's office did not routinely interact with Twitter during the investigation, signifying that Chair's office would only learn of developments in the investigation from the Bureau of Consumer Protection.¹²⁸

These contemporaneous emails appear to undercut Chair Khan's assertions to the Committee. Twitter's request cannot be the reason for Chair Khan's urgency that the FTC hold a vote for the day immediately following the circulation of the recommendation memorandum. Documents produced by the FTC show that Chair Khan's demand for an expedited vote came *before* Twitter's request to wrap up the revised consent decree. Other emails suggest that Chair Khan's office did not know of Twitter's preference for an expedited timeline until *after* she requested an expedited vote timeline from the other Commissioners.

Based on the documents that the FTC has produced, Chair Khan demanded that the FTC follow the expedited timeline because Twitter agreed to sell the company to Musk. Chair Khan would later use this new consent decree to harass Musk and Twitter, including questions targeting journalists that could act to chill First Amendment rights including the work of journalists to expose collusion between Big Tech and the federal government to censor Americans' speech online.

¹²⁸ Non-public briefing by James Kohm before Committee staff (May 8, 2023) (notes on file with the Committee).

V. THE FTC'S CONTINUED HARASSMENT OF MUSK'S TWITTER UNDER CHAIR KHAN

With the consent decree in place, Chair Khan's harassment of Musk and Twitter was set to begin. The burdensome demands for documents and information began on October 27, 2022, the day that Musk took over control of Twitter. On that day, the FTC sent a letter to Twitter outlining deficiencies with prior document requests and demanded Twitter's immediate compliance.¹²⁹ The FTC sent 12 more letters containing more than 350 additional demands for documents and information, before the end of 2022.¹³⁰

At the time of the takeover, Musk committed to complying with the consent decree. In an email to all Twitter employees, Musk wrote: "I cannot emphasize enough that Twitter will do whatever it takes to adhere to both the letter and spirit of the FTC consent decree. Anything you read to the contrary is false."¹³¹ Then, shortly after taking over Twitter, Musk attempted to meet with Chair Khan to "better understand the issues and to show [Bureau of Consumer Protection staff] and [the FTC] the genuineness of his commitment" to effectively comply with the consent decree as Twitter's new CEO.¹³² Chair Khan, however, refused to meet with Musk until "Twitter came into compliance with its discovery obligations," which she continuously augmented by sending new demand letters to Twitter.¹³³

The FTC defended Chair Khan's refusal to meet with Musk by claiming that Chair Khan and other politically accountable officials are not involved in the handling of the Twitter investigation. In a briefing to the Committee, Kohm represented that the Bureau of Consumer Protection Front Office, the Chair's office, or Commissioners' offices do not get involved in investigations into consent decree violations.¹³⁴

However, contrary to Kohm's assertion, documents provided to the Committee show that the FTC's political leadership was involved in the investigation of Twitter. On November 15, 2022, the director of the Bureau of Consumer Protection, Samuel Levine, sent Kohm an email with the subject line "Twitter/Musk taking down two-factor authentication?" and wrote "[t]his was just flagged for me but I've not dug in" and added a link to a news story.¹³⁵ Kohm replied: "Working on it."¹³⁶ Further on January 4, 2023, Kohm received an email with the subject line "Twitter" and was told that Chair Khan "praised [the Twitter] team's assertiveness and momentum in its Twitter investigation" and suggested that "it would be helpful for [the Twitter] team to connect with [the Bureau of Competition]."¹³⁷ In other words, Chair Khan was aware of FTC staff's work and was encouraging it. These emails demonstrate that the politically appointed staff members at the FTC were continuously checking in and directing the investigation into Twitter and attempted to marshal FTC resources from both the Bureau of Consumer Protection and the Bureau on Competition to intimidate and harass Elon Musk and Twitter.

¹²⁹ FTC-TW000001705.

¹³⁰ See 2023 TWITTER HOUSE STAFF REPORT, *supra* note 3.

¹³¹ FTC-TW000001638.

¹³² FTC-TW000002077.

¹³³ FTC-TW000000849.

¹³⁴ Non-public briefing by James Kohm, *supra* note 128.

¹³⁵ FTC-TW000001773.

¹³⁶ *Id.*

¹³⁷ FTC-TW000001553.

Additionally, the Biden-Harris FTC sought information that extended far beyond the limits of the consent decree and refused to accept reasonable discovery limitations. For example, and as detailed by the Committee previously, the FTC sent a letter to Twitter requesting, among other things, *every* communication from any Twitter employee sent to, from, or about Musk.¹³⁸ Despite Chair Khan’s claim that Twitter could “undertake the routine step of calling FTC staff” to “clarify” the FTC’s demands,¹³⁹ when Twitter’s attorney’s explained that the request was overly broad and that most communications related to Musk do not relate to data security or privacy, the FTC refused to negotiate.¹⁴⁰ The FTC, in an email sent to Twitter’s attorneys, continued to demand that Twitter produce all company-wide communications related to Musk, regardless of the privacy, data protection, or information security contents, because “company-wide communications sent by or at the direction of Elon Musk may contain relevant information even where they do not relate to Twitter’s privacy, data protection, or information security functions.”¹⁴¹

Despite Chair Khan’s claim that Twitter could reach out to the FTC for clarity, the Biden-Harris FTC refused to engage Twitter’s reasonable requests and did not “clarify” why it deemed such information to be relevant. This is another example of where Chair Khan told the Committee one thing—that the FTC is open to holding constructive conversations about demanded documents—and in reality, neither Chair Khan nor the Biden-Harris FTC were willing to engage in even the most “routine” discovery discussions with Twitter once owned by Elon Musk.

Finally, FTC staff discussed using Twitter’s disclosure of information to journalists as a way to get around Twitter’s privilege claim for withholding documents from the FTC. On December 12, 2022, an FTC staff member wrote:

We probably need to press further on understanding with greater certainty and detail exactly what types of access Musk is granting outside journalists, both as a potential argument about their privilege waiver and also as a basic privacy/security access issue. . . .¹⁴²

In this case, the FTC was considering an argument that if Twitter gave certain documents to journalists, then Twitter’s privilege claims could be nullified, and the FTC would be entitled to access information about the journalists who ultimately uncovered the censorship regime perpetrated by the Biden-Harris Administration,¹⁴³ including their identities and the documents and information they accessed.

Despite the onerous demands for documents and continued harassment after Musk took over operations of Twitter, the FTC found nothing. Chair Khan claimed that the FTC was

¹³⁸ See 2023 TWITTER HOUSE STAFF REPORT, *supra* note 3.

¹³⁹ Letter from Lina Khan, Chair, Fed. Trade Comm’n to Jim Jordan, Chair, H. Comm. on the Judic. (Feb. 21, 2024).

¹⁴⁰ FTC-TW000001636.

¹⁴¹ *Id.*

¹⁴² FTC-TW000002095.

¹⁴³ See ABUSE OF POWER, WASTE OF RESOURCES, AND FEAR, *supra* note 7.

required to investigate Twitter’s compliance with the consent decree because the “broad access to [Twitter’s] systems, communications, and other information” that Musk gave to the journalists investigating the Twitter Files “triggered legal scrutiny” and because “Twitter may have disclosed consumers’ personal information . . . in violation of the FTC’s [consent decree]”¹⁴⁴ However, the FTC came to find that “Twitter employees took appropriate measures to protect consumers’ private information,”¹⁴⁵ rendering the FTC’s investigation unnecessary. As *The Washington Post* reported in February 2024, “[a]fter investigating his handling of the ‘Twitter Files’ for more than a year, the agency found no evidence the company violated the consent order.”¹⁴⁶

Further, the FTC investigated the personnel decisions at Twitter following Musk’s takeover of the company because the “workforce reductions significantly impacted the Twitter teams charged with protecting key user data.”¹⁴⁷ However, the FTC has not provided the Committee with any evidence to conclude that workforce reductions led to any violations of the consent decree. Finding nothing, the FTC appears to have closed its investigation into Twitter earlier this year after months of investigating and wasting significant public and private resources.¹⁴⁸

¹⁴⁴ Letter from Lina Khan, *supra* note 139.

¹⁴⁵ *Id.*

¹⁴⁶ Cat Zakrzewski, *supra* note 32.

¹⁴⁷ Letter from Lina Khan, *supra* note 139.

¹⁴⁸ *Id.*

VI. CHAIR KHAN'S DISREGARD FOR CONGRESSIONAL OVERSIGHT

Throughout the Committee's investigation, Chair Khan has displayed a flagrant disregard for congressional oversight. Under her leadership, the FTC has slow-walked producing documents, resisted good-faith efforts at accommodation, and outright refused to produce key documents.

On March 10, 2023, the Committee wrote to Chair Khan raising concerns that the FTC was abusing its authority in its conduct toward Twitter.¹⁴⁹ After failing to produce any documents and only providing cursory responses to questions posed by the Committee,¹⁵⁰ including during a public hearing,¹⁵¹ on April 12, 2023, the Committee issued a subpoena to compel the FTC to produce documents and information related to the FTC's harassment of Twitter.¹⁵²

After failing to comply with the subpoena, and as an accommodation to the FTC, on June 8, 2023, the Committee prioritized the immediate production of "all recommendation memoranda" related to the FTC's investigation into Twitter's compliance with 2011 consent decree.¹⁵³ The Committee requested that the FTC make it a priority to produce the recommendation memoranda because they provide the best evidence of the rationale behind the FTC's actions with respect to Twitter, including the legal and policy analysis at the time when the memoranda were circulated.

In response, Chair Khan initially claimed that the recommendation memoranda were outside the scope of the Committee's subpoena. She wrote to the Committee:

In a June 8, 2023, letter, the Committee made additional requests beyond what was requested in the April 2023 subpoena; specifically, it asked for recommendation memoranda and documents relating to the timing of the FTC's investigation. There have been no recommendation memoranda or discussions of timing with regard to Twitter's compliance with the May 2022 Order that is the subject of the Committee's April subpoena.¹⁵⁴

However, despite Chair Khan's claim that the recommendation memoranda are outside the scope of the subpoena, the FTC produced emails that contained the recommendation memoranda as attachments while omitting the memoranda. Numerous emails produced to the Committee show that the Secretary's Office at the FTC circulated to the Commission a document entitled "RECOMMENDATION TO REFER A COMPLAINT TO THE DEPARTMENT OF JUSTICE AND APPROVE A CONSENT IN SETTLEMENT OF THE COURT ACTION," with

¹⁴⁹ Letter from Jim Jordan, Chairman, H. Comm. on the Judic., & Ted Cruz, Ranking Member, S. Commerce Comm. to Lina Khan, Chair, Fed. Trade Comm'n (Mar. 10, 2023).

¹⁵⁰ Letter from Lina Khan, Chair, Fed. Trade Comm'n, to Hon. Jim Jordan, Chair, H. Comm. on the Judic. (Mar. 27, 2023).

¹⁵¹ *Compliance with Committee Oversight: Hearing Before the Subcomm. on Responsiveness & Accountability to Oversight of the H. Comm. on the Judic.*, 118th Cong. (Mar. 29, 2023).

¹⁵² Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm'n (Apr. 12, 2023).

¹⁵³ Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm'n (June 8, 2023).

¹⁵⁴ Letter from Chair Khan, *supra* note 35.

the “Matter Name: Twitter” on April 28, 2022.¹⁵⁵ The Committee has asked for, and the FTC has refused to produce, this or any other recommendation memoranda. Chair Khan cannot withhold the recommendation memoranda on the basis that they are outside the scope of the subpoena while simultaneously producing, pursuant to the subpoena, documents that reference and attach the memoranda.

Further, the Committee’s request for the recommendation memoranda is well within the scope of the subpoena. Among other things, the subpoena requested “items in your possession, custody, or control, from April 1, 2022, to present, in unredacted form: 1. All documents and communications between or among Federal Trade Commission (FTC) officials or employees referring or relating to the FTC’s investigation(s) of Twitter, Inc.”¹⁵⁶ These recommendation materials are important documents to inform the Committee about the FTC’s handling of Twitter because the recommendation memoranda and packages contain important legal and policy analysis prepared by FTC career staff. The recommendation memoranda are the essential resources relied upon by the Commissioners when rendering decisions about how to vote. Given that the FTC has produced documents showing that these recommendation memoranda were distributed to the Commissioner’s offices on April 28, 2022, and that attorney advisors for Commissioners Wilson and Phillips claimed that the Commissioners were carefully reviewing the documents in advance of the vote to finalize the consent decree following a lengthy investigation into Twitter, the recommendation memoranda clearly fall within the subpoena’s specification of documents between FTC officials or employees related to the FTC’s investigation of Twitter.

The FTC’s justification for withholding the recommendation memoranda for being outside of the scope of the subpoena is not only facially wrong but is an inconsistent exclusion relative to responsive material that the FTC has already produced. The recommendation memoranda are documents related to the FTC’s Twitter investigation and fall within the date range required by the subpoena. The FTC effectively conceded the responsiveness of the recommendation memoranda by producing emails where the recommendation memoranda are clearly shown to exist.

The Committee attempted to reasonably accommodate the Biden-Harris FTC from the beginning, but under Chair Khan’s leadership, the FTC has refused to fully comply with the Committee’s subpoena and has imposed inappropriate restrictions on Committee staff throughout this process. The Committee accommodated the FTC by prioritizing the production of the recommendation memoranda, and the FTC refused to produce them.¹⁵⁷ The Committee accommodated the FTC by agreeing to review some “highly sensitive” documents *in camera* instead of insisting on their production¹⁵⁸—however, the FTC demanded that Committee attorneys and staff not take notes or produce any work product related to the documents reviewed *in camera*.¹⁵⁹ The Committee agreed to the FTC’s demand on the condition that the

¹⁵⁵ FTC-TW000002811; FTC-TW000000875; FTC-TW000003049.

¹⁵⁶ Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm’n (Apr. 12, 2023).

¹⁵⁷ Email from FTC staff to Committee staff (Jun. 21, 2024) (Indicating that the FTC does not intend to produce the recommendation memoranda to the Committee).

¹⁵⁸ Email from Committee staff to FTC staff (May 14, 2024).

¹⁵⁹ Email from Committee staff to FTC staff (Jun. 5, 2024).

recommendation memoranda be available for review, but when Committee staff reviewed the documents under the FTC’s onerous conditions, the FTC refused to allow Committee access to the recommendation memoranda.¹⁶⁰

Aside from withholding the most important documents necessary for the Committee’s oversight and imposing onerous restrictions on the Committee’s document review, the FTC has produced only 1,448 documents related to the Twitter matter, which lasted several years and included many FTC employees. Very few of these documents produced by the FTC provide substantive insight into the decision-making around the vote on the consent decree. In addition, there is evidence that the FTC has destroyed many documents related to the Twitter investigation. In an email sent on June 14, 2022, the FTC staff that worked on the Twitter investigation that led to the May 2022 consent decree received an email instructing them to “dispose of all materials relating to this matter . . .”¹⁶¹ Because of this destruction of critical documents related to the FTC’s investigation into Twitter, the Committee and the public may never know the true extent of the political harassment of Twitter.

The Biden-Harris FTC has engaged in a sustained effort to obstruct the Committee’s oversight.¹⁶² Even after the Committee issued a subpoena, the FTC refused to comply, and only began to do so under the threat of contempt.¹⁶³ The FTC continues to withhold the internal recommendation memoranda from the Committee.¹⁶⁴

The FTC’s obstruction of the Committee’s oversight fits an unfortunate pattern. Chair Khan has already misled Congress about her compliance with ethics recommendations;¹⁶⁵ obstructed the Committee’s investigation related to FTC staff morale, forcing the Committee to seek interviews with career staff to obtain any information;¹⁶⁶ misrepresented the agency’s results in merger enforcement;¹⁶⁷ and refused to provide the Committee with recommendation memoranda related to its unlawful non-compete rulemaking.¹⁶⁸ The consistent attempt to limit transparency has undermined Chair Khan’s credibility as an enforcer, and undermined the ability of the FTC to accomplish its mission.

¹⁶⁰ Email from FTC staff to Committee staff, *supra* note 157.

¹⁶¹ FTC-TW000003019.

¹⁶² See Email from FTC staff to Committee staff (Nov. 13, 2023) (Indicating that the FTC does not intend to produce internal documents responsive to the subpoena); see also Email from FTC staff to Committee staff, *supra* note 157.

¹⁶³ See Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm’n (Feb 23, 2024).

¹⁶⁴ Email from FTC staff to Committee staff (Apr. 5, 2024).

¹⁶⁵ Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm’n (Sep. 5, 2023)

¹⁶⁶ Letter from Jim Jordan, Chair, H. Comm. on the Judic. to Lina Khan, Chair, Fed. Trade Comm’n (Jul. 28, 2023).

¹⁶⁷ Letter from Jim Jordan, Chair, H. Comm. on the Judic. & Thomas Massie, Chair, Subcomm. on the Administrative State, Regulatory Reform, and Antitrust to Lina Khan, Chair, Fed. Trade Comm’n (Feb. 27, 2024).

¹⁶⁸ Email from FTC staff to Committee staff (April 5, 2024).

VII. CONCLUSION

This report adds to the Committee’s findings that the FTC, under Chair Lina Khan, has engaged in blatant political harassment of Musk and Twitter. Despite Chair Khan’s denials,¹⁶⁹ contemporaneous FTC documents make explicit the reason behind the FTC’s urgency to finalize its action against Twitter. As Chair Khan’s own attorney advisor wrote: “The urgency is due to Elon Musk’s purchase of the company this week.”¹⁷⁰ This unequivocal declaration runs counter to Chair Khan’s assertions to the Committee. It reveals Chair Khan’s enforcement priorities are not to serve the best interest of the American public, but rather to run her agency as a politically weaponized extension of the Biden-Harris Administration.

The First Amendment protection of freedom of speech is a fundamental freedom that is the cornerstone of American democracy. The Biden-Harris Administration has demonstrated time and again a willingness to stifle speech that runs contrary to the prevailing narrative. Amazingly, the Biden-Harris Administration see free speech advocates, such as Elon Musk, as dangerous and worthy of harassment. As the Committee has detailed in this report, Chair Khan’s efforts to punish Twitter and Musk for exposing the Biden-Harris Administration’s censorship apparatus extend to the very moment that the world learned that Musk would transform Twitter into a platform centered around free speech.

¹⁶⁹ Letter from Lina Khan, *supra* note 35.

¹⁷⁰ FTC-TW000003049.

VIII. Appendix

Appendix Table of Contents

Exhibit 1: FTC-TW000000875 Email between Chair Khan’s attorney advisor and the attorney advisors for the other FTC Commissioners (April 28, 2022)	3
Exhibit 2: FTC-TW000003049 Email between Chair Khan’s attorney advisor and the attorney advisors for the other FTC Commissioners (April 28-May 9, 2022)	9
Exhibit 3: FTC-TW000002155 Email conversation between Monica Vaca and James Kohm (April 28, 2022)	17
Exhibit 4: FTC-TW000003019 Internal email between FTC staff, including James Kohm (June 14, 2022).....	20
Exhibit 5: FTC-TW000001705 Letter from the FTC to Twitter (October 27, 2022)	22
Exhibit 6: FTC-TW000002811 Letter from the FTC to Twitter (November 10, 2022)	28
Exhibit 7: FTC-TW000002077 Email conversation between an FTC employee to Twitter’s outside counsel (November 11 and 14, 2022).....	32
Exhibit 8: FTC-TW000001773 Email conversation between Samuel Levine to James Kohm (November 14-15, 2022).....	35
Exhibit 9: FTC-TW000002095 Internal email between FTC staff (December 12, 2022).....	37
Exhibit 10: FTC-TW000001636 Email conversation from an FTC employee to Twitter’s outside counsel (December 27, 2022).....	39
Exhibit 11: FTC-TW000001553 Email from Rebecca Unruh to James Kohm (January 4, 2023)	46

Exhibit 12: FTC-TW000000849 Email from James Kohm to FTC employee

(March 30, 2023) 48

Exhibit 1
FTC-TW000000875
Email between Chair Khan's attorney
advisor and the attorney advisors for the
other FTC Commissioners
(April 28, 2022)

Message

From: Wilson, Christine [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=3625456A8500420490D8687DC48095 [REDACTED]]
Sent: 4/28/2022 1:07:40 PM
To: [REDACTED]@ftc.gov]
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Let's discuss later.

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:55 AM
To: Wilson, Christine [REDACTED]@ftc.gov>
Subject: FW: ASSIGNMENT: 202 3062 - Twitter

See below and also attached response to [REDACTED] I can respond that you want the tradition three weeks but just wanted to send you the info.

Thanks,
[REDACTED]

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:49 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi [REDACTED]

As my last email indicated we are amenable to identifying another vote date if other offices require more time but in order to propose another timeline we need clear communication regarding how much time Commissioner Wilson requires in order to vote. A proposed date or estimated timeframe (e.g. 3 business days) is preferred.

- [REDACTED]

[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:45 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

I am handling for our office. I spoke with Commissioner Wilson and she will not be ready to vote tomorrow. She too has been in discussions with staff and BCP front office about this matter since Andrew Smith was

Bureau Director. We have repeatedly asked the Bureau about the status of this matter and for updates. This is an important matter for the Commission and she wants sufficient time to review it carefully and discuss with staff.

As I understand it, resolution of this matter involves a number of steps – referral to DOJ, approval by a court, and then an amendment to the admin order by the Commission. As a result, it’s going to take some time so it would be helpful to understand how the Chair envisions the timeline for this matter.

Thanks,

[REDACTED]

Thanks,

[REDACTED]

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:42 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

I am not trying to be dense, but could you spell that out a bit?

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:40 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi [REDACTED]

The urgency is due to Elon Musk’s purchase of the company this week.

[REDACTED]

Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:38 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Good morning,

I'm handling this for our office. Given that this matter has been open for quite a while, what's the urgency? Commissioner Phillips has been very interested in seeing this package and has been regularly asking about it in his meetings with BCP, so he'd like to understand the issues that require an accelerated review. It's an important case and he will definitely want time to get any questions he might have answered and give it thoughtful consideration.

Best,

From: [REDACTED]@ftc.gov>

Sent: Thursday, April 28, 2022 11:11 AM

To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

DOJ is in the loop and is aware of the urgency regarding this matter, but the case team is going to reach out to DOJ to stress urgency. Are you going to handle for your office [REDACTED]? Also please let me know if you (or any other offices) need more time to review. I proposed a 1 day vote given the urgency but I can propose a new date if offices require more time to review but it will be helpful to communicate how much time you need so we can move expeditiously.

[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>

Sent: Thursday, April 28, 2022 10:53 AM

To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

This matter is getting referred to DOJ so have we talked to them – are they likely to move quickly?

Thanks,

From: [REDACTED]@ftc.gov>

Sent: Thursday, April 28, 2022 10:43 AM

To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

That's me. I think we can do it.

From: [REDACTED]@ftc.gov>

Sent: Thursday, April 28, 2022 10:40 AM

To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Cc: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Subject: FW: ASSIGNMENT: 202 3062 - Twitter

Hi All,

In light of recent events that affect this matter, I am proposing tomorrow as a vote date? Please let us know who is handling for your office and if this vote date works.

[redacted]
Federal Trade Commission

From: [redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 6:59 AM
To: [redacted]@ftc.gov>
Subject: ASSIGNMENT: 202 3062 - Twitter

The assignment package referenced above (Related Document [redacted]) is available at:
[redacted]

ASSIGNMENT

The attached document is assigned to
Chair Khan
for review and presentation to the Commission.

Assignment Date: 04/28/2022

Document Number: [redacted]

Matter Name: Twitter

Matter Number: 2023062 Issue Number: 1

Staff Contact: [redacted]

Document Title: RECOMMENDATION TO REFER A COMPLAINT TO THE
DEPARTMENT OF JUSTICE AND APPROVE A CONSENT IN
SETTLEMENT OF THE COURT ACTION

In the transfer of information from this sheet to a Commission circulation form, please note that the document number shown above should be entered on the Commission circulation form as the RELATED DOCUMENT NUMBER. In addition, please note that the document title shown above should NOT be identical to the document title on the circulation form. Instead, the document title on the circulation form should begin with one of the following three phrases:

- *Motion to*
- *For information circulation of* OR

April J. Tabor

[redacted]

[redacted]
Federal Trade Commission

[REDACTED]@ftc.gov

Exhibit 2
FTC-TW000003049
Email between Chair Khan's attorney
advisor and the attorney advisors for the
other FTC Commissioners
(April 28-May 9, 2022)

Message

From: [REDACTED]@ftc.gov]
Sent: 5/9/2022 2:10:11 PM
To: [REDACTED]@ftc.gov]
CC: [REDACTED]@ftc.gov]; [REDACTED]@ftc.gov]; [REDACTED]@ftc.gov]
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

I'll get one for you.

[REDACTED]
[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Monday, May 9, 2022 2:07 PM
To: [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi [REDACTED]

I'm putting together the motion for Friday's vote and wanted to see if you by chance had a redline of the revised complaint that you attached below. (We sometimes hear complaints when there isn't a redline in the motion, though perhaps others can weigh in on whether this is strictly a necessity.) That said, if you think that there will be more edits this week, feel free to hold off and I can just attach the redline of any future versions.

Thanks so much!

[REDACTED]

From: [REDACTED]@ftc.gov>
Sent: Monday, May 2, 2022 5:04 PM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hello All,

Circulating a revised complaint in this matter that [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Friday, April 29, 2022 1:39 PM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>

Cc: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi, we will try to make that date work.

Thanks,

From: [redacted]@ftc.gov>

Sent: Friday, April 29, 2022 11:32 AM

To: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Cc: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

This works for our office.

From: [redacted]@ftc.gov>

Sent: Friday, April 29, 2022 11:32 AM

To: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Cc: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hello,

A gentle reminder to respond to the revised vote date proposal below and I'm still available to chat with anyone who would like more information about recent developments.

[redacted]
Federal Trade Commission

From: [redacted]

Sent: Thursday, April 28, 2022 2:56 PM

To: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Cc: [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>; [redacted]@ftc.gov>

Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi All,

Thanks for these updates. In light of new developments, this matter still requires urgent action so I propose a new vote date of May 13th. I recognize that this does not fully accommodate the requests below but BCP is willing and able to work with all offices to aid review and consideration of this matter. I'm also happy to speak offline with any office that seeks more information about recent developments that warrant expeditious action (I can be reached at [redacted] and I'm available for the remainder of the afternoon except 4-4:30pm). While I can understand there may be some

frustration regarding prior delays with this matter, I hope that all offices can cooperate and accommodate the urgency required here. Please let us know if your office can accommodate the revised vote date.

Best,

[Redacted]
[Redacted]
Federal Trade Commission

From: [Redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 12:31 PM
To: [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>
Cc: [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>
Subject: Re: ASSIGNMENT: 202 3062 - Twitter

Hi,
I'm handling for our office. Like Commissioner Wilson, Commissioner Phillips needs time for careful review and consideration. Using the standard timeline works for us. Also, we will definitely let everyone know if we're ready sooner.

[Redacted]

Get [Outlook for iOS](#)

From: [Redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 12:28:05 PM
To: [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>
Cc: [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Thanks [Redacted] I'll propose a new vote date after we hear from Commissioner Phillip's office.

[Redacted] - Can you confirm who is handling for your office and specify how much time you need to review?

[Redacted]
[Redacted]
Federal Trade Commission

From: [Redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 12:26 PM
To: [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>
Cc: [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>; [Redacted]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Commissioner Wilson anticipates needing the traditional three weeks to thoroughly review this matter but we can let you know if we will be ready sooner.

Also she notes that as we're clearing backlogs of old cases, we should announced [REDACTED]

Thanks,
[REDACTED]

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:49 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi [REDACTED]

As my last email indicated we are amenable to identifying another vote date if other offices require more time but in order to propose another timeline we need clear communication regarding how much time Commissioner Wilson requires in order to vote. A proposed date or estimated timeframe (e.g. 3 business days) is preferred.

[REDACTED]

[REDACTED]
[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:45 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

[REDACTED] handling for our office. I spoke with Commissioner Wilson and she will not be ready to vote tomorrow. She too has been in discussions with staff and BCP front office about this matter since Andrew Smith was Bureau Director. We have repeatedly asked the Bureau about the status of this matter and for updates. This is an important matter for the Commission and she wants sufficient time to review it carefully and discuss with staff.

As I understand it, resolution of this matter involves a number of steps -- referral to DOJ, approval by a court, and then an amendment to the admin order by the Commission. As a result, it's going to take some time so it would be helpful to understand how the Chair envisions the timeline for this matter.

Thanks,
[REDACTED]

Thanks,
[REDACTED]

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:42 AM

To: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov>
Cc: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

I am not trying to be dense, but could you spell that out a bit?

From: [redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 11:40 AM
To: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov>
Cc: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Hi [redacted]

The urgency is due to Elon Musk’s purchase of the company this week.

[redacted]
[redacted]
Federal Trade Commission

From: [redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 11:38 AM
To: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov>
Cc: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

Good morning,

I’m handling this for our office. Given that this matter has been open for quite a while, what’s the urgency? Commissioner Phillips has been very interested in seeing this package and has been regularly asking about it in his meetings with BCP, so he’d like to understand the issues that require an accelerated review. It’s an important case and he will definitely want time to get any questions he might have answered and give it thoughtful consideration.

Best,
[redacted]

From: [redacted]@ftc.gov>
Sent: Thursday, April 28, 2022 11:11 AM
To: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov>
Cc: [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]@ftc.gov; [redacted]
[redacted]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

DOJ is in the loop and is aware of the urgency regarding this matter, but the case team is going to reach out to DOJ to stress urgency. Are you going to handle for your office [REDACTED] Also please let me know if you (or any other offices) need more time to review. I proposed a 1 day vote given the urgency but I can propose a new date if offices require more time to review but it will be helpful to communicate how much time you need so we can move expeditiously.

[REDACTED]
[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 10:53 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

This matter is getting referred to DOJ so have we talked to them – are they likely to move quickly?

Thanks,
[REDACTED]

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 10:43 AM
To: [REDACTED]@ftc.gov>; [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED] <[REDACTED]@ftc.gov>
Cc: [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED], [REDACTED]@ftc.gov>
Subject: RE: ASSIGNMENT: 202 3062 - Twitter

That's me. I think we can do it.

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 10:40 AM
To: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Subject: FW: ASSIGNMENT: 202 3062 - Twitter

Hi All,

In light of recent events that affect this matter, I am proposing tomorrow as a vote date? Please let us know who is handling for your office and if this vote date works.

[REDACTED]
[REDACTED]
Federal Trade Commission

From: [REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 6:59 AM

To: [REDACTED]@ftc.gov>

Subject: ASSIGNMENT: 202 3062 - Twitter

The assignment package referenced above (Related Document #604460) is available at:
MARSID-501634618-556571

ASSIGNMENT

The attached document is assigned to
Chair Khan
for review and presentation to the Commission.

Assignment Date: 04/28/2022

Document Number: 604460

Matter Name: Twitter

Matter Number: 2023062 Issue Number: 1

Staff Contact: [REDACTED]

Document Title: RECOMMENDATION TO REFER A COMPLAINT TO THE
DEPARTMENT OF JUSTICE AND APPROVE A CONSENT IN
SETTLEMENT OF THE COURT ACTION

In the transfer of information from this sheet to a Commission
circulation form, please note that the document number shown above
should be entered on the Commission circulation form as the RELATED
DOCUMENT NUMBER. In addition, please note that the document title
shown above should NOT be identical to the document title on the
circulation form. Instead, the document title on the circulation
form should begin with one of the following three phrases:

- *Motion to*
- *For Information Circulation of* OR

April J. Taber

Target Motion Date: 05/30/2022

[REDACTED]
Federal Trade Commission
[REDACTED]@ftc.gov

Exhibit 3
FTC-TW000002155
Email conversation between Monica Vaca
and James Kohm
(April 28, 2022)

Message

From: Vaca, Monica E. [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=621B1719408345DBB2C3C5239949348-]
Sent: 4/28/2022 1:33:14 PM
To: Kohm, James A. [REDACTED]@ftc.gov]
Subject: FW: Twitter

Hi Jim,

Can I convey to the Chair's office the conversation that [REDACTED] describes, below? They are trying to get a vote within a short period of time, i.e. a week, but Commissioner Phillips is asking for 3 weeks. This information about Twitter's time pressure could be relevant. What do you think?

Monica

From: [REDACTED] <[REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:27 AM
To: [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED], [REDACTED] <[REDACTED]@ftc.gov>
Cc: [REDACTED] <[REDACTED]@ftc.gov>
Subject: RE: Twitter

DOJ and Twitter ([REDACTED] at Wilson Sonsini) have already been negotiating over the DOJ discovery provision that DOJ is insisting on adding. They're scheduled to have another call this afternoon. I spoke to [REDACTED] earlier this morning, and she said they plan to convey to DOJ during this afternoon's call that Twitter is especially anxious to get everything wrapped up soonest, given the recent Elon Musk developments. She said Twitter's goal is for this new FTC order to be entered and all done before Musk formally takes over (which is expected to happen in 3-6 months).

+ [REDACTED] - [REDACTED] says she's been talking to [REDACTED] at DOJ. Don't know if Jim thinks it'd make sense for him to reach out to [REDACTED] separately on this.

From: [REDACTED] <[REDACTED]@ftc.gov>
Sent: Thursday, April 28, 2022 11:21 AM
To: [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED], [REDACTED] <[REDACTED]@ftc.gov>
Subject: RE: Twitter

Great! I think the vote is scheduled for next week (checking on which date). Can we check with DOJ to see if they can move quickly on this? Not sure if they plan on negotiating still?

From: [REDACTED] <[REDACTED]@ftc.gov>
Sent: Thursday, [REDACTED] 28, 2022 10:22 AM
To: [REDACTED], [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED] <[REDACTED]@ftc.gov>
Subject: RE: Twitter

No objections from Enforcement either. Jim supports the quickest vote date possible.

Thanks

- [REDACTED]

From: █████, █████ <█████@ftc.gov>
Sent: Thursday, April 28, 2022 10:12 AM
To: █████ <█████@ftc.gov>; █████ <█████@ftc.gov>
Subject: RE: Twitter

No objection here.

From: █████ <█████@ftc.gov>
Sent: Thursday, █████ 28, 2022 10:10 AM
To: █████ <█████@ftc.gov>; █████, █████ <█████@ftc.gov>
Subject: Re: Twitter

Update - Chair's office wants to propose tomorrow. Any objections if I tell her we support the soonest vote date that still gives the Commission sufficient time to review?

Get [Outlook for iOS](#)

From: █████ <█████@ftc.gov>
Sent: Thursday, April 28, 2022 9:24:22 AM
To: █████ <█████@ftc.gov>; █████, █████ <█████@ftc.gov>
Subject: Fwd: Twitter

Any preference on a vote date?

Get [Outlook for iOS](#)

From: █████ <█████@ftc.gov>
Sent: Thursday, April 28, 2022 9:17:49 AM
To: █████ <█████@ftc.gov>
Subject: Twitter

Hi █████

I wanted to check in about the vote date for the settlement package. Given the urgency with this matter I wanted to confirm what the case team wants as a vote date?

Best,

█████

████████████████████

Attorney Advisor to the Chair
Federal Trade Commission

Exhibit 4
FTC-TW000003019
Internal email between FTC staff,
including James Kohm
(June 14, 2022)

Exhibit 5
FTC-TW000001705
Letter from the FTC to Twitter
(October 27, 2022)



United States of America
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION
600 PENNSYLVANIA AVENUE NW, CC-6316
WASHINGTON, DC 20580

██████████
Division of Enforcement

██████████
██████████@ftc.gov

October 27, 2022

VIA ELECTRONIC MAIL

██████████ Esq. (██████████@wsgr.com)
██████████, Esq. (██████████@wsgr.com)
██████████, Esq. (██████████@wsgr.com)
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW, Fifth Floor
Washington, DC 20006

Re: *In the Matter of Twitter, Inc.*, Docket No. C-4316

Dear Counsel:

We write regarding Twitter's October 17, 2022, responses to the FTC's September 15, 2022, demand letter, which are incomplete and non-responsive in many respects. Twitter must correct these deficiencies by **November 10, 2022**, by providing a true and accurate written report, sworn under penalty of perjury, that fully addresses the issues outlined below.

Request 1

In response to Request 1.b., You¹ stated that engineers with a "base level of access" who are not members of the specific groups granted "full access" to Tweetypic or Gizmoduck do not have access to "these services or systems that would allow them to easily take over or send Tweets from any user's Twitter account. In order to perform such unauthorized actions, an engineer who is not a member of these groups would have to violate Twitter's policies by creating and running code that seeks to imitate a valid internal service to then communicate with Tweetypic or Gizmoduck to take over or send Tweets from a user's Twitter account." Oct. 17, 2022, resp. at 3.

¹ For purposes of this letter, "You" and "Your" shall mean Twitter, Inc., its successors and assigns, and any business it controls directly or indirectly, and all directors, officers, members, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

October 27, 2022

Page 2

- State whether You have any technical controls or other safeguards (other than internal Twitter policies) to detect any such unauthorized actions (i.e., employee with base level access creating and running code that imitates a valid internal service to interact with the Tweetypic or Gizmoduck service and take over or send tweets from any user’s account, using the target account’s user ID) and prevent those unauthorized actions from occurring.
- If so, describe those controls and safeguards in detail.
- State what “full access” means with respect to these systems.
- State what other tiers of access Twitter engineers may have to these systems, and how many individuals have these tiers of access.

Request 1.d asked You to describe in detail Your access controls and technical safeguards, if any, that limit the access Twitter employees have to the Company’s internal production systems, data, services, and tools. Specifically, it asked that You address a series of detailed questions (1.d.i. through 1.d.vi.) for each HDFS or other network or distributed filesystem, database, and Remote Procedure Call (RPC) service You use. Your October 17 response described current practices relating to Your access controls and safeguards for internal production systems generally, rather than on a service-by-service basis, and did not include information about historical practices at the requested level of detail.

We need more information on these issues. To focus Your response efforts, we ask that You provide complete answers to every subpart of 1.d. (i. through vi.) with respect to each of the following services:

- Any service You identified as implicating “cornerstone” or “high-risk data” (see Appendix 2 to the October 17 response);
- Any service that implicates “medium+ sensitivity data” (see Appendix 5 to the October 17 response); and
- Any service involving APIs that could be used to “side-channel compromise” a service that handles “medium+ sensitivity data” (see Appendix 5 to the October 17 response).

For each such service, Your responses to 1.d.i. through vi. must cover the period from June 6, 2022, to the present.

Request 2

Your response to Request 2.c. lists “Server-to-Server Authorization (S2S AuthZ)” among “Areas of Improvement” the Company is addressing as part of the AAA workstreams. Oct. 17, 2022, resp. at 12.

October 27, 2022

Page 3

- For the period from June 6, 2022 to the present, describe in detail any authorization checks in place for interacting with an internal Twitter service or system. As part of Your response, describe how requests from human users (i.e., rather than machine or service identities) are authorized, including whether any authorization checks are performed to limit which authenticated identities may perform specific actions or access particular data.

Request 4

In response to Request 4.b., You stated that in certain circumstances, Twitter may retain Covered Information² it has collected or obtained from or about an individual user beyond 30 days after the user has chosen to deactivate their account. Specifically, in addition to records Twitter may retain for safety and security purposes or to comply with legal requirements (e.g., those relating to law enforcement investigations, litigation holds, or confirmed cases of abuse), Twitter may retain user data, copies of user data, or non-anonymized aggregated user data that has not yet been annotated through the Company's Project Eraser efforts. Oct. 17, 2022, resp. at 16-17.

For all such Covered Information that is not being retained for safety and security purposes or to comply with legal requirements, and has not been annotated to enable Twitter to fully delete data subject to a deletion request or requirement across all of its systems:

- State whether Twitter collected or obtained the Covered Information before or after June 6, 2022;
- Describe where the Covered Information is stored (i.e., for cases where Twitter is not retaining individual user data for safety and security purposes or to comply with legal requirements, but may be retaining Covered Information as a result of its inability to fully delete user data subject to a deletion request or requirement across all of its systems) and whether it is stored in encrypted form; and
- State whether the Covered Information is accessible or available to any person or entity inside or outside of the Company and, if so, describe the circumstances in which this occurs and for what purpose(s).

Request 6

In response to Request 6.a., You generally described a process by which, once a user account becomes eligible for deletion, automated tooling begins an irreversible account deletion process across "all known data" for that user. You stated that "automated tooling initiates the process of reaching out to identified internal services and systems that house the user's personal data and executing a series of deletion tasks to remove the user's personal data from the systems

² For purposes of this letter, "Covered Information" has the same meaning as Definition B in the 2022 Order.

October 27, 2022

Page 4

where automated deletion has been enabled.” You further stated certain data “may continue to exist in Twitter systems pending the completion of [Project Eraser.]” Oct. 17, 2022, resp. at 20-21.

- Clarify what You meant when stating that the irreversible account deletion process is performed across “all known data” for a user who deactivated their account. What Covered Information falls outside the scope of a user’s “known data”?
- Explain what You meant by “identified” internal services and systems housing the user’s personal data on which the automated tooling process is initiated. What are the services and systems housing user personal data that have not been “identified,” and how does Twitter ensure the timely deletion of user personal data that is kept on these other internal services and systems?
- For data that may continue to exist in Twitter’s systems pending the completion of Project Eraser,³ state whether any such information associated with a user’s deleted account remains available or accessible to Company personnel – including information that is stored on a hard drive or other location in a datacenter or datastore within Your possession, custody or control, and information You store or maintain on a third-party cloud server. If so, explain for how long the information remains available or accessible to Company personnel and for what purpose(s). For example, state whether any email addresses, telephone numbers, device IDs, or IP addresses associated with a deleted account remain available or accessible to any business or product team, and if so, for how long and for what purpose(s).

Request 7

In response to Request 7.a., You explained that approximately 52% of the Project Eraser work is complete as of October 17, 2022, and Twitter estimates that approximately 80% of the project will be completed by the end of Q4 2022, with the remaining work being completed by the end of Q3 2023. You further explained the work has been staged to focus on the highest priority systems and data first (i.e., online storage systems that support Twitter’s services), while leaving lower priority systems and data (i.e., offline storage systems not actively used to support Twitter’s services) to be addressed last. Oct. 17, 2022, resp. at 22.

- Specify what percentage of Twitter’s highest priority systems and data have either already completed the Project Eraser work or are expected to complete Project Eraser by the end of Q4 2022.

³ For purposes of this response, exclude any cases where Twitter is retaining user personal data for safety and security reasons or to comply with legal requirements.

October 27, 2022

Page 5

- Of the systems and data for which Twitter expects it will not complete Project Eraser until the end of Q3 2023, specify what percentage fall within Twitter’s “lower priority” systems and data.
- For the systems and data scheduled to complete Project Eraser in 2023, describe where the data is stored; whether it is stored in encrypted form; and whether it is anonymized, de-identified, and/or aggregated.
- For the systems and data scheduled to complete Project Eraser in 2023, state whether the Covered Information is accessible or available to any person or entity inside or outside of the Company and, if so, describe the circumstances in which this occurs and for what purpose(s).

* * * * *

Please have a responsible corporate officer or manager of Twitter certify under penalty of perjury that the written report(s) submitted in response to this letter is complete and accurate, and that the report and accompanying document production(s) represent all information responsive to the FTC’s requests.

All information provided in response to these requests must be submitted in an electronic format agreed upon by a Commission representative in writing prior to the submission. So that the FTC has the capability of reading and using the data, please ensure that the submission of Electronically Stored Information (“ESI”) complies with the attached Production Instructions, and contact us in advance to arrange for the electronic submission of materials via SFTP. Please send an electronic copy of your responses to the Commission at [REDACTED]@ftc.gov, with copies to [REDACTED]@ftc.gov.

Finally, Twitter should suspend any routine procedures for document destruction and take other measures to preserve all records relating to the matters addressed in this letter, including electronically stored records that are stored on backup media and all physical records stored offsite, in a form that includes the complete record.

Sincerely,

[REDACTED]

[REDACTED]

cc: [REDACTED], USDOJ
[REDACTED], USDOJ
[REDACTED], USDOJ

Exhibit 6
FTC-TW000002811
Letter from the FTC to Twitter
(November 10, 2022)



United States of America
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION
600 PENNSYLVANIA AVENUE NW, CC-9528
WASHINGTON, DC 20580

Final Report 1726

Division of Enforcement

@ftc.gov

November 10, 2022

VIA ELECTRONIC MAIL

[REDACTED] Esq. [REDACTED]@quinnemanuel.com)
[REDACTED] Esq. [REDACTED]@quinnemanuel.com)
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005

Re: *In the Matter of Twitter, Inc., Docket No. C-4316*

Dear Counsel:

According to recent press reports, Twitter laid off thousands of employees on or about November 4, 2022, approximating half of its workforce. Within days, it subsequently sought to rehire some of the terminated employees who are essential to ensure the Company's continued operations, including engineering resources needed to launch new products and features.¹

We are concerned these staff reductions impair Twitter's ability to protect consumers' information and comply with the Federal Trade Commission's May 26, 2022, Order in the above-referenced matter ("Order"). Accordingly, pursuant to Part XIII of the Order, we ask that Twitter submit by **November 25, 2022**, a true and accurate written report, sworn under penalty of perjury, that contains responses to the following requests:

¹ See, e.g., Barr, K. (2022, Nov. 7), *Musk's Twitter Looks to Rehire Some of the Staff it Booted Last Week*, Gizmodo, <https://gizmodo.com/musk-twitter-layoffs-1849751286>; Tabahrity, S. (2022, Nov. 6), *Some laid off Twitter employees say they're being asked to come back to Twitter after mass layoffs*, Insider, <https://www.businessinsider.com/some-tweeps-already-being-asked-to-come-back-to-twitter-2022-11>.

November 10, 2022

Page 2

1. State how many employees and contractors Twitter has terminated since October 27, 2022, both as an absolute number and as a percentage of total workforce. As part of Your² response:
 - a. Identify the departments, divisions, and/or teams in which the terminated personnel worked (e.g., Corporate Security, Application Security, Detection and Response Team (DART), Data Management, Enterprise Security, IT, Internal Audit, Privacy & Data Protection, Platform Security, Security Risk Management, Security Governance – Risk and Compliance, Security Architecture and Engineering);
 - b. State how many personnel were terminated from each department, division, and/or team, both as an absolute number and as a percentage of the total headcount in that particular department, division, and/or team; and
 - c. Describe the job functions that the terminated personnel performed.³
2. State whether, in connection with the recent terminations, You performed any reorganization or restructuring of any teams with job duties or responsibilities relating to privacy or information security and, if so, explain how this was done.
3. State whether You can properly protect consumers' information and comply with the Order – including Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information – despite the recent workforce reduction, and explain the basis for Your response.

* * * * *

Please have a responsible corporate officer or manager of Twitter certify under penalty of perjury that the written report(s) submitted in response to this letter is complete and accurate, and that the report and accompanying document production(s) represent all information responsive to the FTC's requests.

All information provided in response to these requests must be submitted in an electronic format agreed upon by a Commission representative in writing prior to the submission. So that the FTC has the capability of reading and using the data, please ensure that the submission of Electronically Stored Information ("ESI") complies with the attached Production Instructions, and contact us in advance to arrange for the electronic submission of materials via SFTP. Please

² For purposes of these requests, "You" and "Your" shall mean Twitter, Inc., its successors and assigns, and any business it controls directly or indirectly, and all directors, officers, members, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

³ For purposes of this request, You may indicate whether any personnel subsequently agreed to return to work for the Company at Twitter's request following their termination.

November 10, 2022

Page 3

send an electronic copy of your responses to the Commission at [REDACTED]@ftc.gov, with copies to [REDACTED]@ftc.gov.

Finally, Twitter should suspend any routine procedures for document destruction and take other measures to preserve all records relating to the matters addressed in this letter, including electronically stored records that are stored on backup media and all physical records stored offsite, in a form that includes the complete record.

Sincerely,

A large black rectangular redaction box covering the signature area.

Encl.

cc: [REDACTED] USDOJ
[REDACTED] USDOJ
[REDACTED] USDOJ

Exhibit 7
FTC-TW000002077
Email conversation between an FTC
employee to Twitter's outside counsel
(November 11 and 14, 2022)

Message

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=3CE3822C7B3F4059A0E6E735E691D02C-[REDACTED].]
Sent: 11/14/2022 8:15:31 AM
To: [REDACTED] [REDACTED]@ftc.gov]; Kohm, James A. [REDACTED]@ftc.gov]
Subject: Twitter - Musk reply

Per below, I responded to Musk's lawyer and received their reply

[REDACTED]
 Bureau of Consumer Protection – Division of Enforcement
 Federal Trade Commission
 600 Pennsylvania Avenue NW, CC-6316
 Washington DC 20580
 t: [REDACTED]@ftc.gov

From: [REDACTED]@quinnemanuel.com>
Sent: Monday, November 14, 2022 8:11 AM
To: [REDACTED] <[REDACTED]@ftc.gov>
Cc: [REDACTED]@quinnemanuel.com>; [REDACTED]@quinnemanuel.com>
Subject: Re: Cd

Understood
 Safe travels
 [REDACTED]

From: [REDACTED] <[REDACTED]@ftc.gov>
Sent: Monday, November 14, 2022 8:10:33 AM
To: [REDACTED]@quinnemanuel.com>
Cc: [REDACTED]@quinnemanuel.com>; [REDACTED]@quinnemanuel.com>
Subject: RE: Cd

[EXTERNAL EMAIL from [REDACTED]@ftc.gov]

[REDACTED] – Thanks for your message. We look forward to receiving Twitter's complete responses to all three outstanding demand letters (October 27th + two letters both dated November 10th) by the November 25 deadline. I'm heading out of the country shortly and will remain out of the office until November 28 – will follow up with you when I return.

Regards,
 [REDACTED]

[REDACTED]
 Bureau of Consumer Protection – Division of Enforcement
 Federal Trade Commission
 600 Pennsylvania Avenue NW, CC-6316
 Washington DC 20580

t: [REDACTED] / [REDACTED]@ftc.gov

From: [REDACTED]@quinnemanuel.com>

Sent: Friday, November 11, 2022 7:06 PM

To: [REDACTED] <[REDACTED]@ftc.gov>

Cc: [REDACTED]@quinnemanuel.com>; [REDACTED]@quinnemanuel.com>

Subject: Cd

[REDACTED] - hope all is well. As we have discussed, and was discussed prior to Mr. Musk taking control of the company mere days ago, we are committed to abiding by the consent decree and the law.

As was expected, there has been turnover and changes at the company - but despite this, we will be in compliance and will be responding as requested to your letter by 11-25.

In this same spirit, Mr. Musk has requested if he could join personally to meet with your office. He hopes to better understand the issues and to show you and your agency the genuineness of his commitment.

Thank you in advance for your consideration. My personal cell is [REDACTED] should anything time sensitive ever arise please feel free to call.

Thank you,

[REDACTED]

Exhibit 8
FTC-TW000001773
Email conversation between Samuel
Levine to James Kohm
(November 14-15, 2022)

Message

From: Levine, Samuel [REDACTED]@ftc.gov]
Sent: 11/15/2022 8:53:07 AM
To: Kohm, James A. [REDACTED]@ftc.gov]; [REDACTED]@ftc.gov]
CC: Unruh, Rebecca [REDACTED]@ftc.gov]; Vaca, Monica E. [REDACTED]@ftc.gov]
Subject: Re: Twitter/Musk taking down two-factor authentication?

Thanks Jim.

From: Kohm, James A. [REDACTED]@ftc.gov>
Sent: Tuesday, November 15, 2022 8:49:20 AM
To: Levine, Samuel [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: Unruh, Rebecca [REDACTED]@ftc.gov>; Vaca, Monica E. [REDACTED]@ftc.gov>
Subject: RE: Twitter/Musk taking down two-factor authentication?
Working on it.

From: Levine, Samuel [REDACTED]@ftc.gov>
Sent: Monday, November 14, 2022 4:53 PM
To: Kohm, James A. [REDACTED]@ftc.gov>; [REDACTED]@ftc.gov>
Cc: Unruh, Rebecca [REDACTED]@ftc.gov>; Vaca, Monica E. [REDACTED]@ftc.gov>
Subject: Twitter/Musk taking down two-factor authentication?
This was just flagged for me but I've not dug in:
<https://www.androidauthority.com/twitter-sms-2fa-3234698/>

Exhibit 9
FTC-TW000002095
Internal email between FTC staff
(December 12, 2022)

Message

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=3CE3822C7B3F4059A0E6E735E691D02C-[REDACTED]]
Sent: 12/12/2022 12:08:34 PM
To: [REDACTED] [REDACTED@ftc.gov]; [REDACTED] [REDACTED@ftc.gov]; [REDACTED] [REDACTED@ftc.gov]; [REDACTED] [REDACTED@ftc.gov]
Subject: Twitter - access to journalists

We probably do need to press further on understanding with greater certainty and detail exactly what types of access Musk is granting to outside journalists, both as a potential argument about their privilege waiver and also as a basic privacy/security access issue: <https://techcrunch.com/2022/12/09/twitter-gdpr-reporter-data-access/>

[REDACTED]
Bureau of Consumer Protection – Division of Enforcement
Federal Trade Commission
600 Pennsylvania Avenue NW, CC-6316
Washington DC 20580
[REDACTED]

Exhibit 10
FTC-TW000001636
Email conversation from an FTC
employee to Twitter's outside counsel
(December 27, 2022)

Message

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=3CE3822C7B3F4059A0E6E735E691D02C [REDACTED]]
Sent: 12/27/2022 9:45:35 AM
To: [REDACTED]@quinnemanuel.com]; [REDACTED] [REDACTED]@ftc.gov]; [REDACTED] [REDACTED]@quinnemanuel.com]; [REDACTED] [REDACTED]@quinnemanuel.com]; [REDACTED] [REDACTED]@quinnemanuel.com]
CC: [REDACTED] [REDACTED]@ftc.gov]; [REDACTED] [REDACTED]@ftc.gov]; [REDACTED] [REDACTED]@ftc.gov]
Subject: RE: Twitter - FTC Document and Information Requests

Thanks for your email, [REDACTED]

REQUEST 17, NOVEMBER 30 DEMAND. Can you please provide us with a hit report or other information that would demonstrate a need for adding (/50 (“privacy” OR “data” OR “infosec” OR “information security” OR “seceng” OR “security”)) to those 18 terms we proposed in our December 6 letter.

REQUEST 7, NOVEMBER 10 DEMAND. I can confirm that, for the time being, Request 7 of the November 10 demand is superseded by Request 4 of the December 6 demand. We reserve all rights to seek further communications that fall within the scope of November 10 > Request 7 as appropriate.

REQUEST 6, DECEMBER 6 DEMAND. We do not agree to your proposed limitation that Twitter would produce only “company-wide communications that broadly concern or relate to Twitter’s privacy, data protection, or information security functions,” in addition to the November 10 and November 16 emails specifically called out in our request. While we would agree that Company-wide communications regarding the open enrollment season for insurance benefits, for example, could reasonably be excluded, we believe that Company-wide communications sent by or at the direction of Elon Musk may contain relevant information even where they do not apparently concern or relate to Twitter’s privacy, data protection, or information security functions. For instance, we would consider Company-wide communications sent by or at the direction of Mr. Musk instructing personnel to search for and get rid of any apparent impersonation accounts following the November 9 launch of Twitter Blue Verified to be relevant – as would any Company-wide communications sent by or at the direction of Mr. Musk that reflect Musk’s stated priorities, which may focus on subscription services and other revenue generators, or place an emphasis on cost-cutting measures, without mentioning Twitter’s privacy, data protection, or information security functions.

Regards,
[REDACTED]

[REDACTED]
Bureau of Consumer Protection – Division of Enforcement
Federal Trade Commission
600 Pennsylvania Avenue NW, CC-6316
Washington DC 20580
t: [REDACTED]@ftc.gov

From: [REDACTED]@quinnemanuel.com>
Sent: Monday, December 26, 2022 5:22 PM
To: [REDACTED] <[REDACTED]@ftc.gov>

Cc: [REDACTED] <[REDACTED]@ftc.gov>; [REDACTED]@quinnemanuel.com>; [REDACTED]@quinnemanuel.com>; [REDACTED]@quinnemanuel.com>

Subject: Twitter - FTC Document and Information Requests

Dear [REDACTED]

Thank you for our call last Thursday to discuss the Commission's document and information requests. As we reiterated, we are working hard to identify and provide responsive documents and information to the Commission as expeditiously as possible, and we appreciate being able to have an open dialogue with the Commission regarding the status of the requests.

We set out in the chart below the current status and anticipated timeline for the first priority requests identified in your December 16, 2022, email. As to the second priority requests, we will let you know this week if there are aspects of the requests for which we need some clarification or that otherwise create concerns for us.

Finally, regarding your question about the custodial documents of [REDACTED], [REDACTED], and [REDACTED] that we have produced, our data vendor confirmed that these documents were de-duplicated prior to production.

Request	Description	Comments/Anticipated Timeline
November 30, 2022 demand, request 17	Produce all communications (including but not limited to emails, memos, and Slack communications) relating to Elon Musk, including any communications sent to any Twitter personnel by or at the direction of, or received by, Musk since October 27, 2022, as well as all other communications discussing communications, instructions, or directives from Musk.	<p>With respect to the communications of other individuals "relating" to Mr. Musk, we propose to add (/50 ("privacy" OR "data" OR "infosec" OR "information security" OR "seceng" OR "security")) to the following terms you proposed in your December 6 letter:</p> <ul style="list-style-type: none"> • job • left • true • truth • verif* • approv* • deny* • control* • incident* • authenticat* • authorizat* • deploy* • launch* • release* • Audit • Threat • Unauthorized • Complaint
December 6, 2022 demand, request 1.b.	Produce organizational charts (or other documents showing the organization of	The Company responded to Request 1.b.(i) by producing TWTRFTC_00020176 on

	<p>individual job positions in departments, divisions, groups, and/or teams) for Twitter that show the Company’s organizational structure (i) as of September 30, 2022; (ii) as of the date You complete the organizational changes referenced in Your November 25 response; and (iii) any interim organizational charts that are or were in effect at any point between October 27, 2022 and the present.</p>	<p>December 20, 2022, which shows the Company’s organizational structure as of September 30, 2022.</p> <p>With respect to Request 1.b.(ii), as we stated in our December 20, 2022, letter and explained during our call last Thursday, the Company does not have any interim organizational charts in effect.</p> <p>With respect to Request 1.b.(iii), as we stated in our December 20, 2022, letter and explained during our call last Thursday, the Company will provide an updated response to the Commission when its organizational changes are finalized.</p>
<p>November 10, 2022 demand, request 7</p>	<p>Produce all Slack communications (whether on a Slack channel or via direct message on Slack) post-dating October 26, 2022, that include, respond to, or reference communications involving the terms “FTC,” “Federal Trade Commission,” “privacy,” “data protection,” “DP,” “security,” “infosec,” or “seceng.”</p>	<p>We believe, and as you initially confirmed during our call last Thursday, this request has been superseded by Request 4 of the Commission’s December 6, 2022, demand letter.</p>
<p>December 6, 2022 demand, request 4a., b., c., d.</p>	<p>Reserving all rights to seek further Slack communications that fall within the scope of this request, we ask that You conduct additional searches for responsive Slack communications post-dating October 26, 2022 that include, respond to, or reference communications involving the terms “FTC,” “Federal Trade Commission,” “privacy,” “data protection,” “DP,” “security,” “infosec,” “or seceng,” and meet one or more of the following conditions:</p> <ul style="list-style-type: none"> a. Slack communications addressed to all Twitter personnel; b. Slack communications within channels used by the Privacy and Data Protection team formerly led by [REDACTED]; c. Slack communications within channels used by the information security organization and teams formerly led by [REDACTED]; d. Slack communications authored by or sent at the direction of Elon Musk; 	<p>We are diligently working to identify the relevant Slack channels that may contain responsive communications for this request. At this time, however, given the breadth of the request and the technical challenges we have encountered with Slack communications, we are unable to provide a definitive date for completion of this production. We are exploring technical solutions that might enable us to respond more quickly. But in the meantime, we anticipate being able to begin producing responsive non-privileged documents in January, and we are aiming to complete production by the second quarter of 2023. However, the projected timeline may change depending on the quantity of documents for review. We will promptly update the Commission about any changes in the projected timeline.</p> <p>With respect to 4(a), as we discussed, this request is focused on the #social-watercooler channel (in which a former Twitter attorney made a post that was reported in The Verge) as well as #team, Twitter’s designated company-wide channel of which all Twitter employees are members.</p>

December 6, 2022 demand, request 6	All Company-wide communications sent since October 26, 2022, including but not limited to the November 10, 2022, communication by Elon Musk referenced in Your November 25, 2022, response to request 3 of the FTC's November 10, 2022, demands (in which Mr. Musk reportedly stated to the entire Company: "I cannot emphasize enough that Twitter will do whatever it takes to adhere to both the letter and spirit of the FTC consent decree. Anything you read to the contrary is absolutely false. The same goes for any other government regulatory matters where Twitter operates.") and a Company-wide email sent on or about November 16, 2022, in which Mr. Musk reportedly told all Twitter personnel that they would need to be "extremely hardcore" going forward, "working long hours at high intensity," and directing them to reply by the next day to convey their commitment or resign with severance pay.	By the first week of January, we will produce a November 10, 2022, email from Elon Musk to the entire Company stating, "I cannot emphasize enough that Twitter will do whatever it takes to adhere to both the letter and spirit of the FTC consent decree. Anything you read to the contrary is absolutely false. The same goes for any other government regulatory matters where Twitter operates"; as well as a November 16, 2022, email from Elon Musk to the entire Company stating, "Going forward, to build a breakthrough Twitter 2.0 and succeed in an increasingly competitive world, we will need to be extremely hardcore. This will mean working long hours at high intensity. Only exceptional performance will constitute a passing grade." Additionally, we anticipate producing other company-wide communications that broadly concern or relate to Twitter's privacy, data protection, or information security functions. Happy to discuss further once you've seen our production.
November 10, 2022 demand, request 4	Produce all notes, documentation, and recordings of or relating to all calls placed to the Twitter Ethics Hotline [REDACTED] since October 27, 2022.	We anticipate producing any additional non-privileged documents and a privilege log in response to this request by the first week of January.
November 10, 2022 demand, request 5	Produce copies of all reports, complaints, and communications made to [REDACTED] since October 27, 2022.	We anticipate producing any additional non-privileged documents and a privilege log in response to this request by the first week of January.
November 10, 2022 demand, request 8.c.	Produce screenshots of all representations You make or have made to consumers regarding Twitter Blue, including but not limited to: all Tweets by Elon Musk or other Twitter personnel; in-product pop-ups, promotions, notices, banners, and other notifications; app store descriptions; Help Center articles; Company blog posts; consent flows; and all other user interfaces involved in the promotion, enrollment, and cancellation of Twitter Blue.	We anticipate producing any additional documents in response to this request by the end of January.
November 21, 2022 demand, request 3.c.	Produce screenshots of all representations You make or have made to consumers regarding Blue Verified, including but not limited to: all Tweets by Elon Musk or other Twitter personnel; in-product pop-ups,	We anticipate producing any additional documents in response to this request by the end of January.

	promotions, notices, banners, and other notifications; app store descriptions; Help Center articles; Company blog posts; consent flows; and all other user interfaces involved in the promotion, enrollment, and cancellation of Blue Verified.	
December 13, 2022 demand, request 2.	Provide screenshots of all consent flows or permission screens users previously saw and currently see since November 8, 2022, when: <ul style="list-style-type: none"> a. signing up for Twitter Blue (also known as Twitter Verified); and b. when remaining part of the Twitter Blue subscription. 	We anticipate producing documents in response to this request by the end of January.
December 13, 2022 demand, request 3.b.	Provide documents sufficient to show each materially different claim or statement made to consumers relating to the collection of phone numbers in connection with Twitter Blue, including advertisements, representations, claims, statements, screenshots of consent flows or permission screens, privacy policies, terms of use agreements, tweets, help pages, and blog posts.	We anticipate producing documents in response to this request by the end of January.
December 13, 2022 demand, request 10	Provide documents sufficient to show each materially different claim or statement made to consumers since November 8, 2022, relating to the privacy, security, and confidentiality of Twitter Blue (also known as Twitter Verified), including advertisements, representations, claims, statements, screenshots of consent flows or permission screens, privacy policies, terms of use agreements, tweets, help pages, and blog posts.	We anticipate producing any additional documents in response to this request by the end of January.
December 9, 2022 demand, request 7	Provide all representations You made between June 6, 2022 to November 8, 2022 regarding the blue Verified badge, including but not limited to screenshots, pop-up notices or explanations, and Help Center articles and text. To the extent those representations changed over time, specify the application time periods for each such screenshot, notice, explanation, article, and text.	We anticipate producing documents in response to this request by the end of January.

Best,





Associate

Quinn Emanuel Urquhart & Sullivan, LLP

1300 I Street, NW, Suite 900
Washington, D.C. 20005
[REDACTED] Direct
202-538-8000 Main Office Number
[REDACTED] FAX
[REDACTED]@quinnemanuel.com
www.quinnemanuel.com

NOTICE: The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and/or work product and as such is privileged and confidential. If the reader of this message is not the intended recipient or agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.

Exhibit 11
FTC-TW000001553
Email from Rebecca Unruh to James
Kohm
(January 4, 2023)

Message

From: Unruh, Rebecca [REDACTED]@ftc.gov]
Sent: 1/4/2023 3:28:41 PM
To: Kohm, James A. [REDACTED]@ftc.gov]
CC: [REDACTED] [REDACTED]@ftc.gov]
Subject: Twitter

Hi Jim – We had our regular mtg with the Chair this afternoon and relayed [REDACTED]'s update on Twitter. I think your team is already aware of this, but the Chair flagged that [REDACTED] (It's not yet scheduled.) The Chair thought it would be helpful for your team to connect with BC's – and she praised your team's assertiveness and momentum in its Twitter investigation.

Rebecca M. Unruh
Acting Deputy Director, Bureau of Consumer Protection
[REDACTED] | cell [REDACTED]

Exhibit 12
FTC-TW000000849
Email from James Kohm to FTC employee
(March 30, 2023)

Message

From: Kohm, James A. [REDACTED]@ftc.gov]
Sent: 3/30/2023 12:23:42 PM
To: [REDACTED]@ftc.gov]
Subject: FW: Urgent NYT inquiry

It is not true that the Chair refused to meet with Mr. Musk. She said she would meet with him when Twitter came into compliance with its discovery obligations. The second two are privileged and we shouldn't comment. I'll assume you're getting back to him unless I hear otherwise. Thanks

From: [REDACTED]@nytimes.com>
Sent: Thursday, March 30, 2023 12:21 PM
To: Kohm, James A. [REDACTED]@ftc.gov>
Subject: Urgent NYT inquiry

Hi Jim,

We are getting ready to publish a story that mentions you by name, so I wanted to run it by you. We are planning to report the following later today.

- Elon Musk tried to meet with Chair Khan in connection with your division's investigation into whether Twitter has violated its F.T.C. consent decree. She rejected the request after consulting with your division.
- Mr. Musk did speak with Commissioner Wilson. At some point, you were added to the call.
- Commissioner Wilson requested the demand letters that the F.T.C. sent to Twitter.

Please let me know if you have any comment or can share anything about the conversation between Commissioner Wilson and Mr. Musk.

I expect we will publish this in the next couple of hours. Please let me know if I can answer any questions. My number is [REDACTED]

Thanks,
[REDACTED]

--

[REDACTED]
Reporter
The New York Times



**CENSORSHIP'S NEXT FRONTIER: THE FEDERAL GOVERNMENT'S ATTEMPT
TO CONTROL ARTIFICIAL INTELLIGENCE TO SUPPRESS FREE 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



December 18, 2024

EXECUTIVE SUMMARY

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 social media and technology companies and other intermediaries to censor lawful speech.¹ As part of this oversight, the Committee and Select Subcommittee have examined the risk that the federal government’s involvement in and regulation of artificial intelligence (AI) can pose to free speech.² Previously, the Committee and Select Subcommittee uncovered that the Biden-Harris Administration is funding the development of AI-powered speech-monitoring tools that could enable the mass censorship of American speech.³ This interim staff report details threats to the free and open development of AI, identifies the free speech risks associated with the federal government’s current involvement in AI development, and recommends approaches that Congress should take to protect Americans’ fundamental First Amendment rights.

Throughout the 118th Congress, the Committee’s and Select Subcommittee’s oversight has demonstrated that the executive branch regularly abuses new technologies—and regulatory power over these technologies—to censor protected American speech. Most recently, the executive branch has coerced and colluded with social media companies to censor true information, opinions, jokes, and satire about elections, COVID-19, and other matters of public importance.⁴ This campaign to silence Americans is a frontal assault on the First Amendment: as the Supreme Court has stated, “speech concerning public affairs is more than self-expression; it is the essence of self-government.”⁵

¹ See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

² See, e.g., 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 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); *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024).

³ *Id.*

⁴ See, e.g., 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., *ELECTION INTERFERENCE: HOW THE FBI “PREBUNKED” A TRUE STORY ABOUT THE BIDEN FAMILY’S CORRUPTION IN ADVANCE OF THE 2020 PRESIDENTIAL ELECTION* (Comm. Print Oct. 30, 2024); 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); 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 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 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 WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023); Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“In 2021, senior officials from the Biden Administration, including the White House, repeatedly pressured our teams for months to censor certain COVID-19 content, including humor and satire, and expressed a lot of frustration with our teams when we didn’t agree.”).

⁵ *Garrison v. Louisiana*, 379 U.S. 64, 74-75 (1964).

Now, the federal government’s censorship campaign has moved to a new frontier: AI. The Biden-Harris Administration has regulated new AI models directly and indirectly, pressuring private companies to “advance equity,”⁶ stop “algorithmic discrimination,”⁷ and “mitigate the production of harmful and biased outputs.”⁸ These regulations provide the means for the federal government to monitor, suppress, and ultimately censor views and information disfavored by the government. AI companies, aware of the power that federal regulators have over their future, have raced to comply with the government’s directives, even allowing the government to inspect new AI models before they are released to the public.⁹ Meanwhile, the executive branch has used taxpayer dollars to fund the development of AI-powered censorship tools to police online speech at a scale never seen before.¹⁰

The burgeoning federal chokehold on AI innovation could have profound negative effects for our nation. If allowed to develop in a free and open manner, AI could dramatically expand Americans’ capacity to create knowledge and express themselves. However, needless regulation from political actors in the executive branch could enable, if not compel, government-preferred bias to become ingrained in AI models, thereby undermining Americans’ First Amendment right to free expression. As one expert testified to the Select Subcommittee in February 2024, “[a] regulatory panic could result in a small number of Americans deciding for everyone else what speech, ideas, and even questions are permitted in the name of ‘safety’ or ‘alignment.’”¹¹ Ultimately, Congress holds the keys: by rejecting censorship and embracing open, decentralized AI innovation, the United States can encourage AI development in a way that respects the First Amendment.

⁶ SELECT COMM. ON A.I. OF THE NAT’L SCI. AND TECH. COUNCIL, EXEC. OFF. OF THE PRESIDENT, NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN UPDATE (May 2023).

⁷ *FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, THE WHITE HOUSE (July 21, 2023).

⁸ SELECT COMM. ON A.I. OF THE NAT’L SCI. AND TECH. COUNCIL, EXEC. OFF. OF THE PRESIDENT, NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN UPDATE (May 2023).

⁹ Press Release, Nat’l Inst. of Standards & Tech., U.S. AI Safety Institute Signs Agreements Regarding AI Safety Research, Testing and Evaluation with Anthropic and OpenAI (Aug. 29, 2024), <https://www.nist.gov/news-events/news/2024/08/us-ai-safety-institute-signs-agreements-regarding-ai-safety-research>.

¹⁰ See, e.g., 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 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); *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024).

¹¹ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (testimony of Greg Lukianoff).

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
TABLE OF CONTENTS	3
I. WHAT’S PAST IS PROLOGUE: THE EXECUTIVE BRANCH’S PREVIOUS EFFORTS TO CENSOR SPEECH ONLINE	4
II. THE THREAT OF AI CENSORSHIP	5
A. There are two distinct AI censorship threats.....	6
B. Regulations limiting private expressive uses of AI will impair AI development and are presumptively unconstitutional.....	7
III. CURRENT AI REGULATORY EFFORTS WILL LEAD TO GOVERNMENT CENSORSHIP	8
A. The federal government is coercing AI developers to censor new models.	8
B. The federal government is funding AI-powered censorship tools.....	13
C. American regulators want to copy the European Union’s onerous AI regulations.	14
IV. CONGRESS CAN PREVENT AI-POWERED CENSORSHIP	15

I. WHAT'S PAST IS PROLOGUE: THE EXECUTIVE BRANCH'S PREVIOUS EFFORTS TO CENSOR SPEECH ONLINE

The Committee's and Select Subcommittee's oversight has revealed how the executive branch has abused new technologies—most recently social media—to censor Americans' free speech, often by covertly coercing or colluding with private companies.¹² Over the past several years, individuals at every level of the federal government have used veiled threats of retaliation to coerce social media companies to silence the voices of American citizens. The world's largest platforms mostly went along with it, trading away free speech on their platforms to try to satisfy the powerful agencies within the executive branch.

The White House. In the name of combatting vaccine hesitancy, the Biden-Harris White House coerced and colluded with the world's largest tech companies—including Facebook, YouTube, and Amazon—to censor true information, satire, and opinions, and successfully pressured them to change their content moderation policies and enforcement practices.¹³

The Department of Homeland Security and the State Department. In the name of combatting alleged election “misinformation” and foreign malign influence, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the State Department's Global Engagement Center (GEC) partnered with Stanford University and “disinformation” pseudo-scientists to create the Election Integrity Partnership (EIP), which worked to censor Americans' online speech before and after the 2020 election.¹⁴ The EIP worked directly with social media companies' content moderation teams, who gave the EIP's censorship requests priority.¹⁵ The EIP submitted specific censorship recommendations to social media companies to remove or demote thousands of Americans' online posts, including true information, jokes, and political opinions.¹⁶

¹² See Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).

¹³ 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); Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“In 2021, senior officials from the Biden Administration, including the White House, repeatedly pressured our teams for months to censor certain COVID-19 content, including humor and satire, and expressed a lot of frustration with our teams when we didn't agree.”).

¹⁴ 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 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 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 WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS* (Comm. Print June 26, 2023).

¹⁵ *Id.*; Transcribed Interview by H. Comm. of the Judiciary of Senior Manager on YouTube's Gov't Affairs & Public Policy Team (June 6, 2024), at 89 (on file with the Comm.).

¹⁶ 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 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 Federal Bureau of Investigation. In the name of combatting a potential “Russian hack-and-leak operation,” the FBI repeatedly met with Big Tech in the lead-up to the 2020 presidential election, priming the companies to censor true information about the Biden family’s influence peddling.¹⁷ In the years following the 2020 election, the FBI continued to directly pressure social media companies to take down posts and censor certain views.¹⁸ The FBI and other federal agencies, including CISA, restarted their meetings with these companies to discuss alleged “misinformation” and “disinformation” in the lead-up to the 2024 election.¹⁹

The National Science Foundation. In the name of combatting “misinformation,” the National Science Foundation (NSF) poured millions of taxpayer-funded grant dollars into the development of AI-powered tools to mass monitor and censor online content.²⁰ One NSF-funded project aimed to automate the flagging of “bad posts” and bragged about helping social media platforms “[e]xternaliz[e] the difficult responsibility of censorship.”²¹

These examples demonstrate the breadth of the executive branch’s efforts to monitor and suppress speech and viewpoints disfavored by those in power. The extent of this censorship regime signals that the federal government will likely seek to do the same with respect to AI companies.

II. THE THREAT OF AI CENSORSHIP

Government involvement in AI development presents a dual threat. First, as the Committee and Select Subcommittee have previously warned, AI offers government bureaucrats and government-partnered intermediaries the ability to mass monitor and mass censor speech at unprecedented speed and scale.²² Second, government censorship of AI training data, algorithms,

¹⁷ 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., ELECTION INTERFERENCE: HOW THE FBI “PREBUNKED” A TRUE STORY ABOUT THE BIDEN FAMILY’S CORRUPTION IN ADVANCE OF THE 2020 PRESIDENTIAL ELECTION (Comm. Print Oct. 30, 2024); Letter from Mark Zuckerberg, CEO, Meta, to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Aug. 26, 2024) (“[T]he FBI warned us about a potential Russian disinformation operation about the Biden family and Burisma in the lead up to the 2020 election. That fall, when we saw a *New York Post* story reporting on corruption allegations involving then-Democratic presidential nominee Joe Biden’s family, we sent that story to fact-checkers for review and temporarily demoted it while waiting for a reply. It’s since been made clear that the reporting was not Russian disinformation, and in retrospect, we shouldn’t have demoted the story.”).

¹⁸ See, e.g., 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 FBI’S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH (Comm. Print July 10, 2023).

¹⁹ Kevin Collier & Ken Dilanian, *FBI Resumes Outreach to Social Media Companies Over Foreign Propaganda*, NBC NEWS (Mar. 20, 2024).

²⁰ 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 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) at 1, 11-13, 15-16; U.S. National Science Foundation, *Track F: WiseDex // Phase 1 Project Video*, YOUTUBE (June 17, 2022), <https://www.youtube.com/watch?v=18gNRQaQtfw>.

²¹ *Id.*

²² See, e.g., 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 WEAPONIZATION OF THE NATIONAL SCIENCE FOUNDATION: HOW NSF IS FUNDING THE DEVELOPMENT OF AUTOMATED TOOLS TO CENSOR ONLINE

and outputs can lead to woke, biased, and inaccurate AI-generated results. Both forms of censorship rob the United States of AI’s knowledge-building and expressive capabilities.

A. There are two distinct AI censorship threats.

AI-powered censorship. AI-powered content moderation tools enable Big Tech to censor disfavored viewpoints at a far greater scale than was previously possible using only human moderators and earlier-generation, rule-based algorithms. As investigative journalist Lee Fang testified to the Select Subcommittee in February 2024, “the rapid development of artificial intelligence tools, in particular, offers powerful entities the unprecedented ability to monitor, flag, and censor billions of individuals at a scale and scope never before conceivable.”²³ Indeed, companies and non-profits, some funded by the federal government, are already developing AI tools to automatically mass monitor and flag content to be censored.²⁴ Armed with AI-powered content moderation tools, Big Tech can more fully and quickly comply with the government’s censorship demands.²⁵

For example, the Committee and Select Subcommittee found that Stanford University created the Election Integrity Partnership (EIP)—a consortium of “disinformation” pseudo-scientists who monitored and flagged Americans’ social media posts for censorship—in 2020 “at

SPEECH “AT SCALE” AND TRYING TO COVER UP ITS ACTIONS (Comm. Print Feb. 5, 2024); *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (written testimony of Lee Fang) (“Moderna also employed the services of the artificial intelligence firm Talkwalker to monitor vaccine-related conversations across 150 million websites, including social media and gaming platforms like Steam . . . Logically, a British artificial intelligence firm that has expanded into the U.S. market . . . is now competing for contracts to monitor and remove alleged social media misinformation in the upcoming 2024 presidential election . . . The United Kingdom government awarded Logically multi-million-dollar contracts to combat misinformation about the COVID-19 pandemic. The company instead surveilled activists and academics who expressed legitimate forms of speech, including thoughtful concerns about pandemic lockdowns and vaccine passports, according to a recent watchdog report on the firm’s activities. Logically previously boasted of a special partnership with Meta, the parent company of Facebook and Instagram, to automatically suppress and label content they deemed as misinformation, giving the company immense influence over content moderation decisions.”).

²³ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (submitted written testimony of Lee Fang).

²⁴ See, e.g., 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 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) at 15-16 (The federal government funded the development of an AI-powered tool that “harnesses the wisdom of crowds and AI techniques to help flag more posts,” helping social media companies to achieve “more comprehensive, equitable, and consistent enforcement, significantly reducing the spread of misinformation.”); Lee Fang, *Logically.AI of Britain and the Expanding Global Reach of Censorship*, REALCLEARINVESTIGATIONS (Jan. 25, 2024) (“During the 2021 local elections in the U.K., Logically monitored up to ‘one million pieces of harmful content,’ some of which they relayed to government officials, according to a document reviewed by RealClearInvestigations. The firm claimed to spot coordinated activity to manipulate narratives around the election, information they reported to tech giants for takedowns.”).

²⁵ *Id.*; see also Allie Funk et al., *The Repressive Power of Artificial Intelligence*, FREEDOM HOUSE (Oct. 4, 2023) (“In at least 22 countries, social media companies were required—either explicitly or indirectly through the imposition of tight deadlines for the removal of banned material—to use automated systems for content moderation.”).

the request of DHS/CISA.”²⁶ With over 100 staff, the EIP targeted *thousands* of posts by Americans for censorship.²⁷ Armed with AI-powered tools—some of which are funded by the government²⁸—a successor to the EIP operating during future election cycles could monitor and flag *tens of millions* of Americans’ election-related posts for censorship.

Censored AI. Generative AI models involve a combination of training data and machine learning algorithms. If a bad actor wanted to prevent an AI model from providing certain information to a user, it could train the model on carefully selected data, omitting certain information so that if a user ever asked for that information, the AI model would be unable to provide it.²⁹ Alternatively, a bad actor could program an AI model to censor certain outputs regardless of the training data by manipulating the model’s machine learning algorithm. For example, a bad actor could insert code into the model’s machine learning algorithm instructing it not to produce certain outputs, even if the available data responsive to the user’s prompt suggests it should.³⁰ In either case, government involvement in an AI model’s development presents an opportunity for government-directed censorship.

B. Regulations limiting private expressive uses of AI will impair AI development and are presumptively unconstitutional.

Permitting the expressive use of AI, outside the control of the government, will benefit the United States. As free speech advocate Greg Lukianoff testified to the Select Subcommittee, AI “empowered by First Amendment principles, including freedom to code, academic freedom, and freedom of inquiry” could dramatically accelerate “the development of new knowledge.”³¹ America can be home to this AI-driven knowledge revolution, but “tying the hands of the greatest programmers in the world would be to lose our advantage to our most determined foreign adversaries.”³² It is an economic and national security imperative that the U.S. leads AI

²⁶ 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 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.

²⁷ *Id.*

²⁸ 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 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) at 15; U.S. National Science Foundation, *Track F: WiseDex // Phase 1 Project Video*, YOUTUBE (June 17, 2022), <https://www.youtube.com/watch?v=18gNRQaQtfw>.

²⁹ See, e.g., Allie Funk et al., *The Repressive Power of Artificial Intelligence*, FREEDOM HOUSE (Oct. 4, 2023) (“Early research indicates that chatbots’ outputs reflect the censorship embedded in their training data, a reminder that generative AI tools influenced by state-controlled information sources could serve as force multipliers for censorship . . . The Chinese government has sought to regulate training data directly: Chinese consumer-facing generative AI products, like Baidu’s ERNIE Bot and Alibaba’s Tongyi Qianwen, are required to implement stringent content controls and ensure the ‘truth, accuracy, objectivity, and diversity’ of training data, as defined by the CCP. Indeed, chatbots produced by China-based companies have refused to engage with user prompts on sensitive subjects like Tiananmen Square and have parroted CCP claims about Taiwan.”).

³⁰ See, e.g., Jacob Mchangama & Jules White, *The Future of Censorship Is AI-Generated*, TIME (Feb. 26, 2024).

³¹ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (testimony of Greg Lukianoff).

³² *Id.*

development worldwide. Strict regulation of AI and burdensome government censorship demands will make this less likely.

Moreover, legislation or regulation broadly restricting expressive uses of AI, including writing, editing, and design, violates the First Amendment.³³ AI creators' editorial decisions about which data they use to train their AI models and which user prompts their AI models will respond to are protected by longstanding and well-developed First Amendment doctrine.³⁴ While existing exceptions to the First Amendment, including incitement, true threats, and defamation, should apply to AI-generated content, Congress and executive branch regulators should treat AI models like other forms of speech and guarantee creators and users the broadest possible berth to express themselves.³⁵

III. CURRENT AI REGULATORY EFFORTS WILL LEAD TO GOVERNMENT CENSORSHIP

The Biden-Harris Administration's current regulatory approach threatens to stifle American AI innovation while supercharging the federal government's ability to censor AI models and outputs—precisely the opposite of what America needs. The Biden-Harris Administration has pushed to censor new and developing AI models, funded the development of AI-powered censorship tools, and collaborated with foreign nations to import onerous European-style AI regulations to the U.S.

A. The federal government is coercing AI developers to censor new models.

Just as the Biden-Harris Administration pressured social media companies to censor protected speech, it is now coercing AI companies to develop “woke” AI models that comply with government censorship demands. Through ostensibly voluntary “frameworks,” “blueprints,” and “resources,” the Biden-Harris Administration has given AI companies a clear warning: censor your AI models, or else. Big Tech, mindful of the federal government's power to kill AI in its infancy, has so far complied. The timeline below outlines the Biden-Harris Administration's coercive scheme:

- **2021-2022:** The National Institute of Standards and Technology (NIST) worked with Big Tech to develop an AI Risk Management Framework (AI RMF) urging companies to manage “harmful bias”³⁶ and “incorporate trustworthiness considerations into the design, development, use, and evaluation of AI.”³⁷

³³ *Artificial Intelligence, Free Speech, and the First Amendment*, FOUND. FOR INDIVIDUAL RIGHTS AND EXPRESSION, <https://www.thefire.org/research-learn/artificial-intelligence-free-speech-and-first-amendment> (last accessed Aug. 23, 2024).

³⁴ *Id.*

³⁵ *Id.* (Under current constitutional law, “any government restriction on the expressive use of AI needs to be narrowly tailored to serve a compelling governmental purpose, and the regulation must restrict as little expression as is necessary to achieve that purpose.”).

³⁶ NAT'L INST. OF STANDARDS & TECH., NO. AI 100-1, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0), at 2-3, 12, 17-18, 36, 38-39 (Jan. 2023).

³⁷ *AI RMF Development*, NIST, <https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development> (created July 28, 2021; last updated Jan. 2, 2024).

- **October 2022:** The Biden-Harris White House issued a Blueprint for an AI Bill of Rights, calling on AI companies to “take proactive and continuous measures” against “algorithmic discrimination,” including “proactive equity assessments” and “pre-deployment and ongoing disparity testing and mitigation.”³⁸
- **May 2023:** The Biden-Harris White House issued an updated National AI R&D Strategic Plan, advocating for (1) “research into language models and other generative AI systems to mitigate the production of harmful and biased outputs”; (2) expanded public-private partnerships that focus on “equity” in “AI design, development, and deployment”; and (3) the establishment of AI standards and benchmarks to detect and avoid “inappropriate bias” and to audit and monitor the “trustworthiness of AI systems.”³⁹
- **July 2023:** The Biden-Harris White House obtained “voluntary” commitments from seven of the world’s largest AI companies, including Google, Meta, Microsoft, Amazon, and OpenAI, to mitigate “harmful bias” and “algorithmic discrimination” while promoting “responsible innovation.”⁴⁰
- **September 2023:** Eight more AI companies made the same “voluntary” commitments to the Biden-Harris White House.⁴¹
- **October 2023:** President Biden signed an Executive Order (EO) on the “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” (1) requiring AI companies to report to the federal government on an ongoing basis about how they train and develop certain “dual-use foundation models”; (2) calling for the establishment of “consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems”; and (3) directing the Department of Justice to prevent and address “algorithmic discrimination” in AI.⁴²
- **November 2023:** Two days after President Biden signed the EO, NIST announced the creation of a U.S. AI Safety Institute (USAISI) to “facilitate the development of standards for safety, security, and testing of AI models” and “align and coordinate

³⁸ OFFICE OF SCI. AND TECH. POLICY, EXEC. OFF. OF THE PRESIDENT, BLUEPRINT FOR AN AI BILL OF RIGHTS at 23 (Oct. 2022).

³⁹ SELECT COMM. ON A.I. OF THE NAT’L SCI. AND TECH. COUNCIL, EXEC. OFF. OF THE PRESIDENT, NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN UPDATE, at 13, 22, 32 (May 2023).

⁴⁰ *FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, THE WHITE HOUSE (July 21, 2023). The seven signatories were Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI. *Id.*

⁴¹ *FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI*, THE WHITE HOUSE (Sept. 12, 2023) The eight signatories were Adobe, Cohere, IBM, Nvidia, Palantir, Salesforce, Scale AI, and Stability. *Id.*

⁴² Exec. Order 14110, 88 Fed. Reg. 75191 §§ 4.1(a), 4.2(a), 7.1(a) (Oct. 30, 2023).

work” with the UK’s AI Safety Institute,⁴³ which has made addressing “misinformation” a key part of its mission.⁴⁴

- **February 2024:** President Biden appointed his former economic policy adviser Elizabeth Kelly to lead the USAISI, and NIST announced the creation of a U.S. AI Safety Institute Consortium (AISIC) to “unite” 200+ AI companies and organizations with the federal government to “establish[] the foundations for a new measurement science in AI safety”⁴⁵ and “[d]evelop guidance and benchmarks for identifying and evaluating AI capabilities, with a focus on capabilities that could potentially cause harm.”⁴⁶
- **July 2024:** NIST published a “companion resource” for its AI Risk Management Framework, recommending that AI companies “integrate tools” to “[i]dentify patterns associated with misinformation or manipulation” and “[e]ngage in due diligence to analyze GAI [generative AI] output for harmful content” and “potential misinformation.”⁴⁷ The Biden-Harris White House also announced that Apple had agreed to its “voluntary” commitments.⁴⁸
- **August 2024:** OpenAI and Anthropic, two of the nation’s largest AI companies, signed an agreement with NIST allowing the federal government to “receive access to major new models from each company prior to and following their public release.”⁴⁹
- **October 2024:** The Biden-Harris White House issued a National Security Memorandum (NSM) on AI (1) “formally designat[ing] the AI Safety Institute as U.S. industry’s primary port of contact in the U.S. Government” for “pre- and post-public deployment testing for safety, security, and trustworthiness of frontier AI models”; (2) “lay[ing] out strengthened and streamlined mechanisms for the AI Safety Institute to partner with national security agencies”; (3) directing the AISI to “issue guidance for AI developers on how to test, evaluate, and manage risks to

⁴³ Press Release, U.S. Dep’t of Commerce, At the Direction of President Biden, Department of Commerce to Establish U.S. Artificial Intelligence Safety Institute to Lead Efforts on AI Safety (Nov. 1, 2023), <https://www.commerce.gov/news/press-releases/2023/11/direction-president-biden-department-commerce-establish-us-artificial>.

⁴⁴ Press Release, UK Gov’t, Prime Minister launches new AI Safety Institute (Nov. 2, 2023), <https://www.gov.uk/government/news/prime-minister-launches-new-ai-safety-institute> (“The Institute will carefully test new types of frontier AI before and after they are released to address the potentially harmful capabilities of AI models, including exploring all the risks, from social harms like *bias and misinformation*.”) (emphasis added).

⁴⁵ Press Release, Nat’l Inst. of Standards & Tech., Biden-Harris Administration Announces First-Ever Consortium Dedicated to AI Safety (Feb. 8, 2024), <https://www.nist.gov/news-events/news/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated-ai>.

⁴⁶ Artificial Intelligence Safety Institute Consortium, 88 Fed. Reg. 75276, 75277 (Nov. 2, 2023).

⁴⁷ NAT’L INST. OF STANDARDS & TECH., NO. AI 600-1, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK: GENERATIVE ARTIFICIAL INTELLIGENCE PROFILE AT 28, 40 (July 2024).

⁴⁸ *FACT SHEET: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitment on AI*, THE WHITE HOUSE (July 26, 2024).

⁴⁹ Press Release, Nat’l Inst. of Standards & Tech., U.S. AI Safety Institute Signs Agreements Regarding AI Safety Research, Testing and Evaluation with Anthropic and OpenAI (Aug. 29, 2024), <https://www.nist.gov/news-events/news/2024/08/us-ai-safety-institute-signs-agreements-regarding-ai-safety-research>.

safety, security, and trustworthiness” posed by their models, including “[h]ow to develop mitigation measures to prevent malicious or improper use of models”; (4) directing federal agencies to “prioritize research” and “pursue partnerships” with the private sector to “advance AI safety and trustworthiness,” including “to address the malicious use of AI to generate misleading videos or images [] of political or public figures”; and (5) “direct[ing] the creation of a Framework to Advance AI Governance and Risk Management in National Security,” which “require[s] agencies to monitor, assess, and mitigate AI risks” related to “bias and discrimination” and “ensure future AI applications are responsible[.]”⁵⁰

- **November 2024:** Consistent with the NSM, NIST’s USAISI established a taskforce comprised of federal agencies—including the Departments of Defense (DoD) and Homeland Security (DHS), the National Security Agency (NSA), and the National Institutes of Health (NIH)—to “collaborate on the development of new AI evaluation methods and benchmarks” as part of the Biden-Harris Administration’s “whole-of-government approach to AI safety.”⁵¹

These “frameworks,” “blueprints,” and “resources,” are not truly “voluntary.” In reality, they are coercive attempts to require AI companies to give government a toehold in the development of new AI systems so that it can control the flow of information in and out of AI models. As the Committee has previously demonstrated, terms like “harmful bias” and “misinformation” are vague and readily weaponized to promote censorship.⁵² Like the social media companies before them, AI developers are likely mindful that the powerful executive branch could cripple their businesses with regulatory retaliation, leaving practically no choice but to comply with the Biden-Harris Administration’s demands.⁵³

The Biden-Harris Administration has not merely attempted to censor AI covertly—it has also regulated AI directly. In October 2023, President Biden issued a sweeping executive order (1) requiring AI companies to share information about how they train and develop certain “dual-use foundation models” with the federal government; (2) calling for the establishment of “consensus industry standards, for developing and deploying safe, secure, and trustworthy AI

⁵⁰ *FACT SHEET: Biden-Harris Administration Outlines Coordinated Approach to Harness Power of AI for U.S. National Security*, THE WHITE HOUSE (Oct. 24, 2024); THE WHITE HOUSE, MEMORANDUM ON ADVANCING THE UNITED STATES’ LEADERSHIP IN ARTIFICIAL INTELLIGENCE; HARNESSING ARTIFICIAL INTELLIGENCE TO FULFILL NATIONAL SECURITY OBJECTIVES; AND FOSTERING THE SAFETY, SECURITY, AND TRUSTWORTHINESS OF ARTIFICIAL INTELLIGENCE (Oct. 24, 2024).

⁵¹ Press Release, U.S. Dep’t of Commerce, U.S. AI Safety Institute Establishes New U.S. Government Taskforce to Collaborate on Research and Testing of AI Models to Manage National Security Capabilities & Risks (Nov. 20, 2024), <https://www.commerce.gov/news/press-releases/2024/11/us-ai-safety-institute-establishes-new-us-government-taskforce>.

⁵² *See, e.g.*, 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 WEAPONIZATION OF “DISINFORMATION” PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

⁵³ *See, e.g.*, 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), at 4-5, 10.

systems”); and (3) directing the Department of Justice to prevent and address “algorithmic discrimination” in AI.⁵⁴ The order paves the way for direct government control of the AI market: in an October 2024 implementation memorandum, the White House directed NIST to “establish an enduring capability to lead voluntary unclassified pre-deployment safety testing of frontier AI models on behalf of the United States Government[.]”⁵⁵ In November 2024, NIST began this effort, establishing a task force to “assist in measuring and evaluating AI models.”⁵⁶ The federal government intends to become the AI gatekeeper, ensuring that only models complying with its censorship demands are released. In four short years, the Biden-Harris Administration has unilaterally changed the AI regulatory landscape from one fostering growth and innovation to one in which major AI companies are pressured to give the government the opportunity to test drive new AI models before their public release.

AI companies’ efforts to comply with federal directives to reduce alleged bias in their AI models may have led to woke, inaccurate outputs and censorship.⁵⁷ Early in 2024, the Committee and Select Subcommittee demonstrated that Alphabet’s (the parent company of Google and YouTube) efforts to comply with President Biden’s AI Executive Order and “White House Commitments”—including selecting external groups to help combat “[s]ocietal risks” and alleged “[r]epresentational and distributional harms”⁵⁸—may have caused Alphabet’s Gemini AI to produce historically inaccurate outputs.⁵⁹ Testimony from Alphabet employees and nonpublic internal company documents confirm that the Biden-Harris White House, NIST, and other federal agencies had engaged with the company on so-called “responsible AI” innovation and may have been the impetus behind Google’s decision to utilize external testing for certain issues.⁶⁰

⁵⁴ Exec. Order 14110, 88 Fed. Reg. 75191 §§ 4.1(a), 4.2(a), 7.1(a) (Oct. 30, 2023).

⁵⁵ THE WHITE HOUSE, MEMORANDUM ON ADVANCING THE UNITED STATES’ LEADERSHIP IN ARTIFICIAL INTELLIGENCE; HARNESSING ARTIFICIAL INTELLIGENCE TO FULFILL NATIONAL SECURITY OBJECTIVES; AND FOSTERING THE SAFETY, SECURITY, AND TRUSTWORTHINESS OF ARTIFICIAL INTELLIGENCE (Oct. 24, 2024).

⁵⁶ Alexandra Kelley, *NIST sets up new task force on AI and national security*, NEXTGOV/FCW (Nov. 21, 2024).

⁵⁷ See, e.g., *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (testimony of Greg Lukianoff) (“My number one concern with AI . . . is the inherent bias that we’re already baking into it. That’s one of the things that scares me the most. And just to give a comical example, we asked ChatGPT to write a poem about why Representative Jim Jordan is the best politician in the country. It refused to do that. We ran this for every single member of the Committee, and it refused to do this only for Republicans.”); Megan Morrone, *Meta AI creates ahistorical images, like Google Gemini*, AXIOS (Mar. 1, 2024); see also Editorial Board, *Meta AI’s false facts about Trump shooting are part of a disturbing trend*, N.Y. POST (Aug. 3, 2024).

⁵⁸ Gemini Team, *Gemini: A Family of Highly Capable Multimodal Models*, GOOGLE (2024) at 38 (citing the White House’s Voluntary AI Commitments); *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, THE WHITE HOUSE (Oct. 30, 2023).

⁵⁹ Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Mr. Daniel F. Donovan, Counsel for Alphabet (Mar. 2, 2024) (on file with the Comm.); Adi Robertson, *Google apologizes for ‘missing the mark’ after Gemini generated racially diverse Nazis*, THE VERGE (Feb. 21, 2024); Nico Grant, *Google Chatbot’s A.I. Images Put People of Color in Nazi-Era Uniforms*, N.Y. TIMES (Feb. 22, 2024); Chris Pandolfo, *Google to pause Gemini image generation after AI refuses to show images of White people*, FOX BUSINESS (Feb. 22, 2024).

⁶⁰ See, e.g., Transcribed Interview of Google’s AI Principles, Operations, and Governance Lead, H. Comm. on the Judiciary (Apr. 11, 2024) (on file with the Comm.) at 35-36, 39, 77. (“Before the White House commitments were announced, the Public Policy team had shared with me a draft and asked if I had any opinions on it, if, given my experience doing our AI, again, and governance for 5 or so years, if I had any thoughts on what was workable, what was not workable, and just share that with the Public Policy team . . . I also identified the areas that we weren’t doing and just saying, just calling out we haven’t done, for example, external testing . . . [E]xternal testing was the

More generally, government cannot regulate Americans’ speech—including AI models and AI-generated content—without inherently weighing in on what viewpoints should be favored or disfavored. “Misinformation,” “harmful bias,” “equity,” and other similar terms are inherently subjective and easily weaponized to censor political opponents.⁶¹ AI-related regulations and other government involvement to address alleged misinformation and bias pose a serious risk to devolve into pure censorship. Greg Lukianoff, President of the Foundation for Individual Rights and Expression (FIRE), testified to the Select Subcommittee that during his career as a free speech advocate he has frequently been “shocked” by the degree to which censors label “tame, moderate speech” as “hate speech.”⁶² Indeed, as journalist Lee Fang testified to the Select Subcommittee, government decisions about censorship are often “politically motivated,” and “government censorship of truthful and accurate speech, rather than dispelling conspiracy theories, serves only to exacerbate the erosion of public trust.”⁶³

B. The federal government is funding AI-powered censorship models.

The executive branch of the federal government has poured millions of taxpayer dollars into the development of AI-powered tools to mass monitor and censor content,⁶⁴ leading to the censorship of protected speech.⁶⁵ Beginning in 2021, the NSF’s Convergence Accelerator Track F grant program spent millions of dollars on the development of AI-powered tools to combat alleged “misinformation,” including one project that aimed to automate the flagging of “bad posts” and help social media platforms “[e]xternaliz[e] the difficult responsibility of censorship.”⁶⁶ Likewise, the State Department’s Global Engagement Center (GEC) offered seed funding to an AI company offering microtargeting for “behavior change campaigns” targeting foreign vaccine hesitancy.⁶⁷ Under the Biden-Harris Administration, Americans’ taxpayer

only one off the top of my head that I didn’t even think there was maybe another team at Google doing it . . . For the White House commitments, the external testing was the one area that we hadn’t already done.”)

⁶¹ See, e.g., 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 WEAPONIZATION OF “DISINFORMATION” PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

⁶² *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Federal Government*, 118th Cong. (Feb. 6, 2024) (testimony of Greg Lukianoff).

⁶³ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Federal Government*, 118th Cong. (Feb. 6, 2024) (testimony of Lee Fang).

⁶⁴ 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 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).

⁶⁵ See, e.g., Gabe Kaminsky, *Disinformation Inc: Meet the groups hauling in cash to secretly blacklist conservative news*, WASH. EXAMINER (Feb. 9, 2023).

⁶⁶ 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 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) at 15; U.S. National Science Foundation, *Track F: WiseDex // Phase 1 Project Video*, YOUTUBE (June 17, 2022), <https://www.youtube.com/watch?v=18gNRQaQtfw>; see also *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (testimony of Katelynn Richardson).

⁶⁷ Email from the U.S. Embassy in Nairobi, Kenya to State Dep’t Personnel (June 10, 2021) (on file with the Comm.).

dollars are being spent subsidizing the development of AI-powered technologies that could later be used to surveil and silence them.

Other nations have already turned similar tools on their own citizens. During the COVID-19 pandemic and in the lead-up to the 2021 local elections in the United Kingdom, the British government allegedly worked with an AI company to monitor over a million online posts and censor journalists, activists, and lawmakers who criticized pandemic policies and other government initiatives.⁶⁸ In 2022, the Canadian government reportedly worked with the same AI company to monitor the online activity of truck drivers participating in the “Freedom Convoy” lockdown protests.⁶⁹

C. American regulators want to copy the European Union’s onerous AI regulations.

The EU’s newly passed AI Act requires “[a]ll high-risk AI systems [to] be assessed before being put on the market and also throughout their lifecycle” and allows government bureaucrats to “ban” any AI model that they deem to pose “unacceptable risks.”⁷⁰ Allowing the government to serve as the gatekeeper of the AI marketplace gives the government extraordinary leverage over AI model inputs and outputs, increasing the risk of censorship. Furthermore, with such severe consequences for failing to censor sufficiently (in the eyes of the government) and the inevitable chilling effect of any government involvement in the regulation of speech, many companies might aggressively censor their AI models to ensure they satisfy the expected biases of the government reviewers.

Despite these threats to fundamental liberties, some American policymakers have sought to imitate the EU’s new law. For example, Colorado’s new Artificial Intelligence Act “shares some similarities with the EU AI Act,” imposing steep “obligations relating to documentation, disclosures, risk analysis and mitigation, governance, and impact assessments for developers and deployers of high-risk AI systems.”⁷¹ Similarly, one proposed bill in the New York legislature would require registration and government licensing of AI models deemed to be “high-risk” and require AI developers to ensure that their models “provide equitable outcomes” and “prevent . . . harmful outcomes.”⁷² In addition, Democrats in Congress have demanded that the Federal Election Commission (FEC) censor X’s new Grok-2 AI art generator, citing concerns over the need to address alleged “dangerous falsehoods.”⁷³

The Biden-Harris Administration has even sought to deepen cooperation with censorious foreign nations on AI regulations. For example, in November 2024, the Administration

⁶⁸ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Federal Government*, 118th Cong. (Feb. 6, 2024) (testimony of Lee Fang); *see also* Lee Fang, *Logically.AI of Britain and the Expanding Global Reach of Censorship*, REALCLEARINVESTIGATIONS (Jan. 25, 2024).

⁶⁹ *Id.*

⁷⁰ *See EU AI Act: first regulation on artificial intelligence*, EUROPEAN PARLIAMENT (Aug. 6, 2023).

⁷¹ Stuart D. Levi et al., *Colorado’s Landmark AI Act: What Companies Need to Know*; SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (June 24, 2024); *see* Colo. Rev. Stat. tit. 6, art. 1, pt. 17 (2024).

⁷² Assembly Bill A8195, N.Y. State Leg. 2023-2024 Legis. Session (N.Y. 2023).

⁷³ Letter from Democratic Members of Congress to Lisa J. Stevenson, Acting Gen. Couns., Fed. Election Comm’n (Aug. 26, 2024); *see* Sean Cooksey (@SeanJCooksey), X (Aug. 27, 2024, 12:38 PM), <https://x.com/SeanJCooksey/status/1828472171917627729>.

announced the creation of an International Network of AI Safety Institutes—whose founding members include the UK, Canada, and the European Commission—to help guide the U.S.’s AI regulatory efforts.⁷⁴ In April 2024, Secretary of State Antony Blinken and Secretary of Commerce Gina Raimondo pledged to work with the EU to “advance and reinforce interoperability between AI governance frameworks,” implying that the Biden-Harris Administration is seeking to back-door the EU’s AI regulations into the United States.⁷⁵ And, in September 2024, the Biden-Harris Administration joined the Council of Europe’s “Framework Convention” on AI, which “offers a legal structure focused on combating instances of discrimination resulting from AI system use.”⁷⁶ Indeed, nonpublic State Department documents obtained by the Committee and Select Subcommittee describe how the “U.S. AI Safety Institute and others in the interagency have strong working relationships with EU counterparts.”⁷⁷ The U.S. AI Safety Institute met with the EU’s newly created “AI Office,” the entity in charge of implementing and enforcing the EU’s AI Act, for the first time in July 2024.⁷⁸

IV. CONGRESS CAN PREVENT AI-POWERED CENSORSHIP

Congress can legislate to ensure that the federal government does not censor AI models, fund AI-powered censorship tools, or use AI to violate Americans’ fundamental freedoms. To ensure that American AI leads the world and is developed in accordance with our fundamental First Amendment principles, Congress should work to (1) ensure the federal government is not inappropriately involved in private AI algorithm or dataset decisions; (2) ban funding of AI research related to content moderation; (3) end foreign collaboration on AI regulations involving lawful speech; and (4) stop censorious AI regulations.

1. The federal government should not be involved in AI algorithm or dataset decisions for lawful speech.

The Committee and Select Subcommittee have shown that numerous executive branch agencies have coerced and colluded with social media companies to censor lawful American speech directly⁷⁹ and by proxy.⁸⁰ The federal government should not be allowed to require

⁷⁴ Tharin Pillay, *U.S. Gathers Global Group to Tackle AI Safety Amid Growing National Security Concerns*, TIME (Nov. 21, 2024).

⁷⁵ *U.S.-EU Joint Statement of the Trade and Technology Council*, THE WHITE HOUSE (Apr. 5, 2024).

⁷⁶ Alexandra Kelley, *U.S. joins Council of Europe’s AI and human rights framework*, NEXTGOV/FCW (Sept. 6, 2024).

⁷⁷ U.S. State Dep’t Memorandum on EU Digital Issues (on file with the Comm.).

⁷⁸ *Id.*; see *European AI Office*, EUROPEAN COMM’N (last visited Dec. 16, 2024).

⁷⁹ See, e.g., 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); 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 FBI’S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH (Comm. Print July 10, 2023).

⁸⁰ See, e.g., 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 WEAPONIZATION OF “DISINFORMATION” PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS’ POLITICAL SPEECH (Comm. Print Nov. 6, 2023).

compliance with, or condition federal funding on, an AI company’s policies governing moderation of lawful speech, model inputs or outputs, algorithms, or information sharing practices.

2. *Congress should not fund content moderation-related AI research.*

The Committee and Select Subcommittee have uncovered the federal funding of AI-powered censorship tools⁸¹ and investigated federally funded companies and organizations using AI to demonetize and deplatform conservative news organizations.⁸² The executive branch should not be allowed to fund (1) research into AI-powered tools for content moderation or combatting so-called mis-, dis-, or malinformation;⁸³ or (2) research seeking to measure or counter issues relating to the fairness, bias, equity, or other “societal risk” of a private company’s AI model. New and developing censorious technologies represent a threat of a different magnitude to online speech and thus the modern town square. At a minimum, American taxpayers should not be funding tools that may take away one of their most important fundamental rights.

3. *The U.S. should not follow or take part in collaborative global AI regulation efforts of lawful speech.*

The U.S. should not look abroad for inspiration when it comes to regulating and using AI. Foreign governments have worked with AI companies to systematically censor their citizens’ online speech and passed new AI laws facilitating government censorship of this critical technology, including the EU’s AI Act.⁸⁴ Government-sponsored censorship programs similar to

⁸¹ 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 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).

⁸² Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Daniel J. Rogers, Exec. Dir., Global Disinformation Index (Mar. 10, 2023); *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 9, 2023) (testimony of Matt Taibbi) (“For every government agency scanning Twitter, there were perhaps 20 quasi-private entities doing the same, including Stanford’s Election Integrity Project, NewsGuard, the Global Disinformation Index, and others, many taxpayer-funded.”); STAFF OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., GARM’S HARM: HOW THE WORLD’S BIGGEST BRANDS SEEK TO CONTROL ONLINE SPEECH (Comm. Print July 10, 2024) (“GARM pushes its members to use news rankings organizations, like the Global Disinformation Index (GDI) and NewsGuard, that disproportionately label right-of-center news outlets as so-called misinformation.”); *see also Under the Microscope: Examining the Censorship-Industrial Complex and its Impact on American Small Business: Hearing Before the H. Comm. on Small Business*, 118th Cong. (June 26, 2024).

⁸³ *See also* 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 WEAPONIZATION OF CISA: HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023) at 10 (“According to CISA’s own definition, “[m]alinformation is based on fact, but used out of context to mislead, harm, or manipulate.” 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.”) (footnote omitted) (emphasis in original).

⁸⁴ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (testimony of Lee Fang); *Artificial Intelligence, Free Speech, and the First Amendment*, FOUND. FOR INDIVIDUAL RIGHTS AND EXPRESSION, <https://www.thefire.org/research-learn/artificial-intelligence-free-speech-and-first-amendment> (last accessed Aug.

these are bad policy and are likely unconstitutional in the United States.⁸⁵ Congress should also exercise careful oversight of collaborative international efforts to regulate AI.

4. Federal regulatory authority over AI could result in censorship.

AI regulations—even if they do not specifically address AI-produced speech—could provide government officials with enormous leverage to coerce companies to suppress certain types of lawful speech.⁸⁶ As FIRE President Greg Lukianoff testified to the Select Subcommittee, “the most chilling threat that the government poses in the context of emerging AI is regulatory overreach that limits its potential as a tool for contributing to human knowledge. A regulatory panic could result in a small number of Americans deciding for everyone else what speech, ideas, and even questions are permitted in the name of ‘safety’ or ‘alignment.’”⁸⁷ Indeed, allowing for the “decentralized development and use of AI” is the best way to protect against bias and other blind spots.⁸⁸

Accordingly, Congress should not permit the executive branch to involve itself in the training or moderation of AI models, particularly as it relates to efforts to mitigate so-called “harmful bias” and “inequity” or address “algorithmic discrimination.” And Congress should not pass legislation enacting an AI regulatory scheme similar to the EU’s AI Act, which gives bureaucrats the ability to regulate or ban AI models based on their perceived “risk.”⁸⁹

The Committee passed the Censorship Accountability Act, which allows Americans to hold accountable public officials who work with tech companies to censor their First Amendment protected speech—including AI-generated speech.⁹⁰ In addition, the Free Speech Protection Act requires federal agencies to regularly publish all content moderation-related communications between federal employees and tech companies, including discussions about AI model inputs or outputs.⁹¹ Congress should pass these important bills and continue to work to safeguard Americans’ right to think and speak freely in the digital town square.

23, 2024); see also Lee Fang, *Logically.AI of Britain and the Expanding Global Reach of Censorship*, REALCLEARINVESTIGATIONS (Jan. 25, 2024).

⁸⁵ See generally *Artificial Intelligence, Free Speech, and the First Amendment*, FOUND. FOR INDIVIDUAL RIGHTS AND EXPRESSION, <https://www.thefire.org/research-learn/artificial-intelligence-free-speech-and-first-amendment> (last accessed Aug. 23, 2024); J.D. Tuccille, *E.U.’s Digital Services Act Threatens Americans’ Free Speech*, REASON (June 5, 2023) (describing how legislative changes in the United States similar to the EU’s Digital Services Act “would run afoul of the First Amendment”).

⁸⁶ *Hearing on the Weaponization of the Federal Government Before the Select Subcomm. on the Weaponization of the Fed. Gov’t of the H. Comm. on the Judiciary*, 118th Cong. (Feb. 6, 2024) (testimony of Greg Lukianoff).

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *AI Act*, EUROPEAN COMM’N, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (last accessed Aug. 23, 2024).

⁹⁰ Censorship Accountability Act, H.R. 4848, 118th Cong. (2023).

⁹¹ Free Speech Protection Act, H.R. 4791, 118th Cong. (2023).