

OUR CELL PHONE COMPANIES ARE KILLING OUR NATION

The Abuse Of Our Children, Our Rights, Our Privacy And Our Communications

Presented to the United States Congress Members

Please Forward This Document To Your Peers And Associates

Revision # 6b



Table of Contents

OUR CELL PHONE COMPANIES ARE KILLING OUR NATION.....	1
Introduction.....	6
The Abuses Of Citizens.....	7
T-Mobile Hit With Class Action Suits After Consumer Data Breach.....	8
T-Mobile Accused of Violating FTC Act in New Post-Breach Suit.....	8
T-Mobile Data Breach Lawsuit Morgan & Morgan Law Firm.....	8
T-Mobile Negligent, Reckless in Failure To Prevent Data Breach	8
T-Mobile US hit with class action lawsuits.....	8
T-Mobile Sim Swap Incident Resulted in \$275K Theft from Victim's	9
Integrity Line Compliance & Ethics T-Mobile.com.....	9
T-Mobile Sued After Client Lost \$8.7 Million in Cryptocurrency Hack.....	9
Class-Action Complaints Stream in Over T-Mobile Data Breach - Tech.....	9
Customers Are Suing T-Mobile As Its Breach Climbs to 53 Million.....	9
Murdering Our Children For Profit.....	24
More on this.....	27
More on this.....	28
The Social Media That T-Mobile Enables, Broadcasts, Promotes And Embeds On Kids Phones, Tablets And Computers Is Causing The Rising Teen Suicide Rate.....	28
Burger King takes on bullying with powerful PSA.....	34
'13 Reasons Why' should be taken off the air, psychiatrist urges.....	35
Is T-Mobile Liable For “ <i>Complicit Homicide</i> ” By Allowing Teens To Use Facebook, Google and Instagram, Who Are Facing Lawsuits for Teen Mental Health Crisis, In A MASSIVE Profits-Over-Safety Mobile Services Abuse Charge.....	38
Is T-Mobile Liable For “ <i>Complicit Homicide</i> ” By Allowing Teens To Use Facebook, Google and Instagram, Who Are Facing Lawsuits for Teen Mental Health Crisis, In A MASSIVE Profits-Over-Safety Mobile Services Abuse Charge.....	38
GOOGLE IS RUN BY CHILD SEX PERVERTS.....	43
Google whistleblower claims tech giant's Developer Studio division has been infiltrated by 'pedophilic religious doomsday cult' Fellowship of Friends that was featured in a Spotify podcast series called 'Revelations' last year.....	43
Share this article.....	44
T-Mobile Instagram influencer and model Niece Waidhofer, 31, DELETED all her Instagram posts before she killed herself: Was found dead at home after welfare check.....	45
What is Fellowship of Friends?.....	46
The Dating Apps On T-Mobile Products And Services Are Raping You.....	48
Cell Phone Companies Vast Relationships With The “Google Cartel” Are Criminal Conspiracies.....	50
The Deadly Cell Phone Promotions Of Facebook/Instagram Are Also Disturbing.....	87
What Proof Exists To Confirm The Veracity Of These Charges.....	92
T-MOBILE SECURITY ISSUES.....	95
Who’s Watching Your WebEx? Webex has many back-door spy paths built in.....	113
Google still keeps a list of everything you ever bought using Gmail, even if you delete all your emails, and provides that data to political parties, the NSA and marketing companies so they can manipulate you...115	115
Hackers' paradise.....	117

'Very embarrassing for the government'.....	118
Alexa and Google Home eavesdrop and phish passwords.....	119
Amazon- and Google-approved apps turned both voice-controlled devices into "smart spies.".....	119
FSB's secret projects.....	125
How Artists And Fans Stopped Facial Recognition From Invading Music Festivals.....	135
.....	139
Privacy Tools.....	139
Providers.....	139
Web Browsers.....	139
Software.....	139
Operating Systems.....	139
PrivacyTools Services.....	139
Privacy? I don't have anything to hide.....	139
Read also:.....	140
Quotes.....	140
More Privacy Resources.....	141
Guides.....	141
Information.....	141
Tools.....	141
Participate with suggestions and constructive criticism.....	142
Lapsus\$ hackers targeted T-Mobile source code in latest data breach.....	144
T-Mobile Secretly Bought Its Customer Data from Hackers to ... - VICE.....	144
Lapsus\$ hackers breached T-Mobile's systems and stole its source	144
T-Mobile data breach 2021: Here's what it means for securing your	145
The T-Mobile Data Breach Is One You Can't Ignore WIRED.....	145
T-Mobile hack: Everything you need to know - ZDNet.....	145
What to do if you're concerned about the T-Mobile data breach.....	145
T-Mobile Data Breach: Your T-Mobile Account Has Been Hacked	145
Leaked Chats Show LAPSUS\$ Stole T-Mobile Source Code.....	145
T-Mobile Hacker Who Stole Data on 50 Million Customers.....	145
T-Mobile Data breach: The infamous Cyber Attack - IDStrong.....	146
T-Mobile Data Breach Lawsuit 2022 Join 1000s of others.....	146
T-Mobile Data Hack: What We Know and What You Need to Do - WSJ.....	146
Lapsus\$ Hackers Stole T-Mobile's Source Code and Systems Data.....	146
T-Mobile CEO says "truly sorry" for hack of 50M users' data AP News.....	146
T-Mobile is latest Lapsus\$ breach victim Security Magazine.....	146
T-Mobile Says Hack Exposed Personal Data of 40 Million People.....	146
T-Mobile Data Breach Lawsuit Morgan & Morgan Law Firm.....	147
T-Mobile tried to buy stolen customer data back, but failed TechRadar.....	147
That Nvidia-hacking group went after T-Mobile but the FBI snagged	147
T-Mobile Data Breach Lawsuit Morgan & Morgan Law Firm.....	147
T-mobile Faces Class Action Lawsuits Following Data Breach	147
T-Mobile Data Breach Lawsuit 2021 What To Do - ClassAction.org.....	147
T-Mobile: 'Significant Portion' of Data Breach Class Members	147
Lawsuits Against T-Mobile - FairShake.....	148
T-Mobile Data Breach - Class Action Lawsuit - Lynch Carpenter LLP.....	148
T-Mobile Data Breach Class Action.....	148
T-Mobile class action claims Sprint merger costs Verizon, AT&T	148

Mass Arbitration Against T- Mobile - Class Action Lawsuits.....148
T-Mobile Data Breach Lawsuit 2022 | Join 1000s of others.....148



Introduction

Silent Spring is an [environmental science](#) book by [Rachel Carson](#).^[1] Published on September 27, 1962, the book documented the environmental harm caused by the indiscriminate use of [pesticides](#). Carson accused the [chemical industry](#) of spreading [disinformation](#), and public officials of accepting the industry's [marketing claims](#) unquestioningly.

In the late 1950s, Carson began to work on environmental [conservation](#), especially environmental problems that she believed were caused by [synthetic](#) pesticides. The result of her research was *Silent Spring*, which brought environmental concerns to the American public. The book was met with fierce opposition by chemical companies, but it swayed public opinion and led to: a reversal in U.S. pesticide policy, a nationwide ban on [DDT](#) for [agricultural uses](#),^[2] and an [environmental movement](#) that led to the creation of the [U.S. Environmental Protection Agency](#).^{[3][4]}

In the same tradition, this report exposes another deadly danger hiding in plain sight and affecting every living citizen. The largest number of teenage deaths, mental health tragedies, asset thefts, privacy abuses, election frauds and other horrific social crimes has been caused by the very devices that are sold to us.

This report is produced, almost entirely, from Congressional investigation reports, FTC, FCC, SEC, FEC, GAO, FBO, DOJ reports and complaints, Court records and public testimony.

These companies try to avoid liability by claiming that they are not liable for the bad things that happen across their networks and devices but the harsh reality is that NONE OF THESE BAD THINGS COULD HAPPEN WITHOUT THESE COMPANIES COMMERCIAL, PROFIT-BASED, NETWORKS AND DEVICES DISTRIBUTING THESE BAD THINGS **AND** RELAYING BAD THINGS BACK TO BAD PEOPLE!

The electronics industry has spent billions of dollars to cover these facts up. T-Mobile, AT&T, Assurance Wireless, etc., will do anything to stop this information from becoming public. “***Killing our children***” is bad enough... but that is only the beginning of their crimes against society. Their partners in crime: ***Instagram, Facebook, Google, Netflix, YouTube***, etc., make \$1200.00+ every minute and spend a significant amount of those funds on counter-hype, cover-ups, deferring, lying to Congress, delaying regulation, political bribery, RICO law violations, anti-trust law violations and keeping their crimes going.

That ends now!

The Abuses Of Citizens

Investigator's went 'under-cover' inside of T-Mobile and other cell phone companies.

What they found will shock you.

Public citizens were damaged by their subjection to, work for and with, and whistle-blowing about, these criminally corrupt corporate telecommunications officials, and the politicians they control and finance.

T-Mobile has been under investigation since, at least, the year 2000, not long after they came into being. A large volume legal 'class ' of, similarly harmed, Plaintiff's exist as: tens of millions of consumers who either used the products and services of the cell phone companies or who were affected by them. A huge number of lawsuits, for abuse, have now been filed against T-Mobile by a historically large number of consumers.

New abuses and attacks by T-Mobile have taken place in recent weeks and that has restarted the clock on the statute of limitations.

These charges also have relevance to the many State and Federal charges and investigations against T-Mobile for THE LARGEST PRIVACY ABUSE IN HISTORY and the recent Supreme Court abortion decision which now has activists hunting women seeking abortions over T-Mobile's networks and devices.

T-Mobile's assertions that only 'some of' consumers personal data was leaked to the world is an inane, lying, obfuscation of the facts. T-Mobile executives that assert that the volume of each individual's data was 'not big enough to matter' are either: A.) criminally incompetent or, B.) complicit in a falsehood so large that prison-for-life might not be punishment enough. It is well known, by any college educated person in 2022 that **ANY TWO** personal ID items (ie: 1.- An account number and, 2.- a name or 1. - a name and a 2.- a phone number...) can be input into contemporary global hacker infrastructure to reveal the: financial records, medical records, home address, work address, social security number, legal files, abortion data, and essentially EVERYTHING an individual considers private, in 15 minutes, or less. The NSA has a database called XKEYSCORE, widely disclosed by Edward Snowden, that can do it in less than five minutes. T-Mobile released consumer data that HAS gotten people killed! A fact that can be proven in Court! In the Spy World and the Hacker World: "TWO EQUALS ALL"! This means that any two items of identification can instantly expose ALL of a person's private data and get their bank account sucked dry and their abortion records online in seconds! Every spy agency, Corsican Mafia group and 14 year old hobby hacker has this capability: TODAY!

Russian, Iranian, Chinese and other State and private hacking groups now offer the service, to American anti-abortion activists, based around T-Mobile's massive 60 million+ consumer data leaks, of hunting down women seeking, or getting, abortions. "*Thanks, T-Mobile*", say the activists!

T-Mobile's "Assurance" phone group has some of the largest numbers of abortion seekers in America, according to demographic studies. How do they feel about discovering that their "*Free Obama Phones*" are actually tracking devices?

Millions of members of the public were maliciously harmed by the cell phone companies and their insidious Silicon Valley social media Big Tech partners.

T-Mobile refused to remove Facebook, Instagram, Google and the Silicon Valley spy-tech cartel from their devices because the Facebook, Instagram, Google and the Silicon Valley spy-tech cartel PAY T-Mobile and AT&T to help them exploit consumers.

When you see headlines like these:

<https://news.bloomberglaw.com/privacy-and-data-security/t-mobile-hit-with-class-action-suits-after-consumer-data-breach>

T-Mobile Hit With Class Action Suits After Consumer Data Breach

... **T-Mobile** USA Inc. was hit with a pair of class action lawsuits in ... **T-Mobile** violated the CCPA and acted **negligently** by failing to protect ...

<https://news.bloomberglaw.com/privacy-and-data-security/t-mobile-accused-of-violating-ftc-act-in-new-post-breach-suit>

T-Mobile Accused of Violating FTC Act in New Post-Breach Suit

... Causes of Action: **Negligence** and **negligence** per se, violation of the Washington Consumer Protection Act, declaratory judgment. Relief: Damages, ...

<https://www.forthepeople.com/mass-arbitration-lawsuits/t-mobile-data-breach/>

T-Mobile Data Breach Lawsuit | Morgan & Morgan Law Firm

T-Mobile recently confirmed that their company was the subject of a malicious data breach that ... You may want to sue **T-Mobile** directly for its **negligence**, ...

<https://topclassactions.com/lawsuit-settlements/privacy/data-breach/t-mobile-negligent-reckless-in-failure-to-prevent-data-breach-says-class-action/>

T-Mobile Negligent, Reckless in Failure To Prevent Data Breach ...

... **T-Mobile Negligent**, Reckless in Failure To Prevent Data Breach, Says Class Action ... T-Mobile failed to properly ...

<https://www.mobileworldlive.com/featured-content/top-three/t-mobile-us-hit-with-class-action-lawsuits>

T-Mobile US hit with class action lawsuits

... **T-Mobile** US customers filed a series of class action lawsuits accusing the company of **negligence** after hackers exposed personal data.

<https://www.dilendorf.com/resources/sample-complaint-against-t-mobile-usa-inc.html>

T-Mobile Sim Swap Incident Resulted in \$275K Theft from Victim's ...

... (“**T-Mobile**”, “Respondent”) pursuant to the Federal Communications Act, a common law theory of gross **negligence**, a common law theory of **negligent** ...

<https://www.t-mobile.com/responsibility/legal/integrity-line>

Integrity Line | Compliance & Ethics | T-Mobile.com

The Integrity Line provides confidential and anonymous online reporting for issues or concerns in regard to **T-Mobile** Code of Business Conduct.

<https://www.levinlawpa.com/t-mobile-sued-after-client-lost-8-7-million-in-cryptocurrency-hack/>

T-Mobile Sued After Client Lost \$8.7 Million in Cryptocurrency Hack

... Lawsuit Alleges Gross **Negligence** in SIM Card Swapping Scheme. **T-Mobile** is facing a multi-million dollar lawsuit after hackers were able to ...

<https://lawstreetmedia.com/news/tech/class-action-complaints-stream-in-over-t-mobile-data-breach/>

Class-Action Complaints Stream in Over T-Mobile Data Breach - Tech

... On August 15, reports began circulating that **T-Mobile** suffered a data ... compromised as a result of Defendant's **negligence** and failure to: ...

<https://www.businessinsider.com/customers-are-suing-t-mobile-as-breach-reaches-53-million-2021-8>

Customers Are Suing T-Mobile As Its Breach Climbs to 53 Million

... **T-Mobile** USA Inc., the plaintiffs and the class action members contend their identities are at risk because of **neglect** on the part of ...

... you can't help but wonder if T-Mobile has gone insane with negligence and criminal abuse of the consumer whole. The most shocking part, though, is that those headlines are only 10% of the entire list of dirty deeds that the public has been forced to endure.

T-Mobile, and the other abusive telecommunications insiders, created harms by:

A.) Spying on citizens -

B.) Providing a network to chart the menstrual cycles and pregnancy tests of women, when women enter and exit an abortion clinic and the location of that clinic, which anti-abortion activists have now hacked into in apps and medical offices via T-Mobile's utter lack of security -

- C.) *Providing open back-doors for hackers on Defendants devices and software -*
- D.) *Causing teens to commit suicides -*
- E.) *Allowing young girls and boys to be solicited for sex on the T-Mobile networks and devices, particularly through Instagram and Facebook on T-Mobile networks and devices -*
- F.) *Partnering, covertly, with criminally corrupt Silicon Valley media companies that T-Mobile knowingly participated in social abuse and election crimes with -*
- G.) *Advertising, marketing, promoting and producing socially damaging materials with the Silicon Valley social media companies, -*
- H.) *Cooperating in a sinister plan to allow the use of T-Mobile devices, networks and software in partnership with Google, Twitter, Instagram, Facebook, et al, which uses abstract content-specific features of the consumed content, such as categories, topic models, and entities, which they automatically extract using natural language processing by comparing every word you use to a giant computer library of what those words might mean about your psychology. So it's like you are getting "mind-raped". Their assessment of what your words might mean is based on what rich, white male, \$200K/year, Google-promoting programmers think they might mean, which is 'racist', according to Stanford University psychologists -*
- I.) *Refusing to terminate the network paths-to-abuse as enumerated by Facebook/Instagram whistleblower [Frances Haugen](#) and over 100 other whistle-blowers -*
- J.) *Embedding 'apps' on T-Mobile phones, devices, tablets and systems which were known to harm the public, especially children -*
- K.) *Stealing Plaintiff's issued patents and trade secret technology -*
- L.) *Operating as global monopolies -*
- M.) *Through T-Mobile's "Assurance Brand of cell phones known as "Obama Phones" to the public, poor people are given phones which are monitored, via intermediary services, on a database known as "The Beast", wherein the NSA, CIA, INS, DEA, Collection agencies, Equifax, Axciom and other spy services can monitor these disadvantaged persons via national identifier, 'lifeline' and internal data processing systems which violate human rights and human privacy and engage in many other abuses enumerated in related documents. Additionally, these Obama phones are embedded with software Apps, listed herein, which push users to Google, Facebook and other privacy violating sites -*
- N.) *Consumers were lied to, harassed, black-listed and service cut-off in reprisal for reporting illicit deeds at T-Mobile. At T-Mobile retail stores, in-store videos prove that T-Mobile employees discussed harming customers in reprisal for customers complaining too much and did harm Plaintiffs and damaged a multi-million dollar investigation; causing substantial economic and personal harms to Plaintiffs -*
- O.) *Many other public abuses, by T-Mobile are cited in the news and other Court filings -*

While T-Mobile's cry-baby shill lawyers pooh-pooh everything herein (Because that is what they are paid to do)(It should be noted that T-Mobile lawyers: Polsinelli, have been charged, in court, with MASSIVE FRAUD, by Polsinelli's own clients including Philidor Rx Services LLC) . The United States Congress, ProPublica, CBS News 60 Minutes, The FBI, The FTC, The SEC, The EU, and OVER ONE THOUSAND OTHER highly credible, news, law enforcement and forensic investigation entities have verified everything herein.

Some consumers have even pointed out that **T-Mobile** CEO **John Legere** has stayed at President **Trump's** hotel in Washington while his company sought government approval for a \$26-billion government contract from the Trump Administration and is said to be a personal friend of Trump. T-Mobile is a Germany-founded company which is the country where the Nazi's were founded and still operate. The DNC opposition PR machine refers to Trump, and all of his supporters as "Nazi's". Based on this, T-Mobile has even caused Jewish consumers to feel like "T-Mobile Hates Jews". Whether or not T-Mobile is antisemitic, the real issue is how T-Mobile has screwed over so many people that some consumers would even consider such a scenario.

The history of the issues **behind** this case, from the past, are fully relevant to the issues **of the** matter today. It is not ethically possible for government or Court officials to refuse to hear all of the facts. It is not morally right for government officials, Court officials, ADR staff or related parties, who are supposed to solve the problem, to selectively try to piece-meal parts of this in order to avoid political and corporate embarrassment.

The [inventor of the world's first cellphone](#) says he's stunned by how much time people now waste on their devices, telling users to "get a life." Martin Cooper, 92, made the declaration during an interview with "[BBC Breakfast](#)", responding to a co-host who claimed she whiled away upwards of five hours per day on her phone. "*Do you really? You really spend five hours a day? Get a life!*" he stated, before bursting into laughter. Chicago-based Cooper invented the [Motorola DynaTAC 8000X](#) — the world's first cellphone — back in 1973. Mr. Cooper is horrified that T-Mobile may be using his idea for such sinister deeds, as listed above.

T-Mobile Hacked, Data For Sale?

Anybody @Home in T-Mobile Security?

by Mike McDonald - June 11, 2009 - 2 Comments

Get the WebProNews Newsletter:

Enter Your Email Address...

Enter Captcha 

Like 0

A hacker group has claimed to have hacked T-Mobile this past weekend and is apparently looking to cash in. Oh this world we live in, right? (Editor's Note: Be sure to read the update from T-Mobile at the end of the article)

As a T-Mobile customer, I assure you this isn't exactly the brightest part of my morning. I was just doing a quick (Bing) search on T-Mobile this morning to see if there was any news about a release date on the new Google Phone... and this is what I get.



Not only is there still not a peep about the phone I'm **obsessing-over** looking for, it seems as though I now get to wonder about the security of my data. Of course anytime you hear about a company you do business with 'losing' their data, you have to wonder how and if it will come back to haunt you in some aspect.



If a company loses your data, do you leave them for a competitor? Sound off in the comments.

As of the posting of this article, I have yet to see a peep from T-Mobile in the way of a comment for more information.



Janet Yell
Lead Fed
Vice chair to

PRINT EMAIL COMMENT

Hacker penetrates T-Mobile systems

Kevin Poulsen, SecurityFocus 2009-01-11

A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year, which he used to monitor U.S. Secret Service e-mail, obtain customers' passwords and Social Security numbers, and download candid photos taken by Sidekick users, including Hollywood celebrities, SecurityFocus has learned.

Twenty-one year-old Nicolas Jacobsen was quietly charged with the intrusions last October, after a Secret Service informant helped investigators link him to sensitive agency documents that were circulating in underground IRC chat rooms. The informant also produced evidence that Jacobsen was behind an offer to provide T-Mobile customers' personal information to identity thieves through an Internet bulletin board, according to court records.

"On July 28th the informant gave his handlers proof that their own sensitive documents were circulating in the underground marketplace they'd been striving to destroy."

Jacobsen could access information on any of the Bellevue, Washington-based company's 16.3 million customers, including many customers' Social Security numbers and dates of birth, according to government filings in the case. He could also obtain voicemail PINs, and the passwords providing customers with Web access to their T-Mobile e-mail accounts. He did not have access to credit card numbers.

The case arose as part of the Secret Service's "Operation Firewall" crackdown on Internet fraud rings last October, in which 19 men were indicted for trafficking in stolen identity information and documents, and stolen credit and debit card numbers. But Jacobsen was not charged with the others. Instead he faces two felony counts of computer intrusion and unauthorized impairment of a protected computer in a separate, unheralded federal case in Los Angeles, currently set for a February 14th status conference.

The government is handling the case well away from the spotlight. The U.S. Secret Service, which played the dual role of investigator and victim in the drama, said Tuesday it couldn't comment on Jacobsen because the agency doesn't discuss ongoing cases-- a claim that's perhaps undermined by the 19 other Operation Firewall defendants discussed in a Secret Service press release last fall. Jacobsen's prosecutor, assistant U.S. attorney Wesley Hsu, also declined to comment. "I can't talk about it," Hsu said simply. Jacobsen's lawyer didn't return a phone call.

T-Mobile, which apparently knew of the intrusions by July of last year, has not issued any public warning. Under California's anti-identity theft law "SB1386," the company is obliged to notify any California customers of a security breach in which their personally identifiable information is "reasonably believed to have been" compromised. That notification must be made in "the most expedient



Security

In association with heise online

Search The H Security

Last 7 days News Archive Features

17 January 2012, 10:52

« previous | next »

T-Mobile USA hacked



A group of hackers that goes by the name "Team0x0v" claims to have obtained access credentials belonging to staff at US Deutsche Telekom subsidiary T-Mobile USA. To back up their claim, the hackers posted data to the Pastebin anonymous text hosting service. One member of the group told Sulpesia that the hack involved exploiting SQL injection vulnerabilities on the t-mobile.com and newsroom.t-mobile.com web sites.



According to T-Mobile, the problem was limited to the T-Mobile USA newsroom. This claim seems plausible, with spot testing by The H's associates at heise Security finding that the published credentials did indeed belong to newsroom staff. This would limit the scale of any problems arising as a result -- the intruders may be able to publish fake press releases. Based on the information provided, private customer data was never at risk.

Most of the passwords consist of a simple six-digit number composed of two numbers repeated such as "112112". T-Mobile USA says that it has now fixed the vulnerabilities.

(cive)

« previous | next »

Print Version | Send by email | Pemailink: <http://h-online.com/i-3414307>

SECURITY HEADLINE

The H is closing down Android and its password problem for spies
Critical vulnerabilities in numerous NSS 3.15.1 brings TLS 1.2 support
Second Android signature attack d
Black Hat 2013: NSA director to sp conference

SECURITY

Content Security Policy halts XSS



Cross-site scripting (XSS) is one of the problems faced by webmasters. The Security Policy standard should finally relief more »

Skype's ominous link checking: Fact speculation



Listen to Fox News Radio Live

Fair & Balanced

Home | Video | Politics | U.S. | Opinion | Entertainment | Tech | Science | Health | Travel

T-Mobile Customer Database Allegedly Hacked

Published June 08, 2009 / FoxNews.com

Print

Email

Share

Comments

Recommend

Tweet

Cell-phone carrier T-Mobile USA may have been seriously hacked, with millions of customers' personal details now up for sale in the hacker underground.

"We have everything, their databases, confidential documents, scripts and programs from their servers, financial documents up to 2009," a group calling itself "pwnmobile" wrote in an e-mail Saturday to various tech and security Web sites.

"We already contacted with their competitors and they didn't show interest in buying their data -- probably because the mails got to the wrong people -- so now we are offering them for the highest bidder," the e-mail continues.

The message then displays a long list of various servers, including names, operating systems and IP addresses, but doesn't include any pilfered data.

Consumers own a large number of T-Mobile devices including phones, tablet and wi-fi hotspot devices purchased directly from T-Mobile, Walmart and/or supplied by the Government. Plaintiff's peers, associates, co-investigators, family members and members of the public own many more. The only reason Plaintiffs originally acquired the devices is because they were cheaper than other devices. Over time, after observing numerous abuses by T-Mobile, a huge number of users have filed complaints about T-Mobile and other cell phone companies.

As federal whistle-blowers and crime victims of a felony crime, the victims have been subjected to political dirty tricks reprisals using taxpayer funded government agency resources. Political dirty tricks services like Fusion GPS, Black Cube, Gizmodo, In-Q-Tel, etc. are in the news headlines regularly because of what they do to citizens, like the victims, when those kill-services are hired by corrupt corporations, Senators and White House staff.

These reprisals are operated by a small, but extremist, handful of corporate telecommunications officials because some of the victims are federal witnesses in an ongoing active major law enforcement investigation involving the political and stock market assets of the associates of those officials. The fact that screwball telco executives engage in dirty tricks ops with government agencies is in the ***headlines of the news every single day!*** This can no longer be called 'conspiracy theory' because it is now ***forensic fact!***

Those telecommunication officials are now known to have manipulated attacks and reprisals, payments process and services in reprisal for reporting their crimes.

Past cases set historical legal precedents that created many federal court firsts and new legal standards. There should be no question in the mind of any court about the fact that these corporate/government agency attacks on these victims did occur and were illegally operated as political, corporate, anti-competitive reprisals. The Courts, the FBI, Congress and extensive investigations have proven these assertions as indisputable fact. Even though they won their historical lawsuit, the victims still never got any compensation aside from knowing they exposed the crime.

The number of users whose personal information might have been compromised in a [recent cyber attack](#) of T-Mobile has climbed to over 53 million, as the telecommunication company is hit by many class-action lawsuits.

T-Mobile announced it had discovered that another 5.3 million current customers and 667,000 former customers also had their information stolen.

The wireless carrier is now up against many class action lawsuits filed by upset customers, [Bloomberg reported](#). Lawsuits accuse T-Mobile of violating the California Consumer Privacy Act which allows any Californian the right to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with. One of the lawsuits also accuses T-Mobile of violating the Washington State Consumer Protection Act for [having poor data security](#).

According to the lawsuit *Espanoza v. T-Mobile USA Inc.*, the plaintiffs and the class action members contend their identities are at risk because of neglect on the part of T-Mobile. The plaintiffs are also

concerned with the monetary costs and the "time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft."

[The information stolen](#) from the customers includes names, addresses, dates of births, phone numbers, social security numbers, and driver's license information. T-Mobile says that the information stolen from the additional customers did not include social security numbers and driver's license information.

T-Mobile does not know if customers had their financial information, credit card information, debit, or other payment information stolen in the attack but T-Mobile is known to lie and FBI experts state that any two ID items can easily allow hackers to steal financial information, credit card information, debit, or other payment information with the data that T-Mobile has already acknowledged that was stolen.

T-Mobile reset the PINs associated with these accounts and is also offering additional protection services like McAfee's ID Theft Protection Service and Account Takeover Protection capabilities for all customers but those services are known to only provide window-dressing PR and minimal protection.

"We are continuing to take action to protect everyone at risk from this cyberattack, including those additional persons we recently identified," the company said in a statement. "We have sent communications to millions of customers and other affected individuals and are providing support in various ways."

T-Mobile originally became aware of the data breach after hackers posted in an underground forum, Vice's [Motherboard](#) first reported.

The seller of the information is asking for six bitcoins, worth about \$297,279 as of publishing, for 30 million social security numbers and driver's licenses, according to [Motherboard](#). The seller is privately offering the rest of the breached information.

The corporate executives who are, or who partnered with, Defendants have been charged, by third parties with: ***Money Laundering, Sex Trafficking, Family Alcoholism, Political Bribery, Stock Market Manipulations, Hookers, Media Censorship, Misogyny, Dynastic Family Manipulations of Public Policy, Election Rigging, Search Engine Bias, Monopolies, Recession Causing Market Trusts, Racism, Brotopia, Secret Offshore Shell Corporations, Venture Capital Black-Lists, Patent Thefts, Payola, Graft, Corrupt Lobbyists and Their Use of Our Democracy As Their Play-Thing...?***

Are T-Mobile and these other executives the kind of people that any nation, or any individual should trust with it's communications, privacy and it's CHILDREN!!!!???

Part of that evidence proof is on display at the links below and in the video documentaries provided therein. Millions of citizens have viewed that site and these videos on network TV. Over 300,000 pages of evidence materials are referenced herein, much of it now in the hands of United States Congressional investigation offices.

The competing companies to the businesses of these victims are owned by famous U.S. Senators who want some of the victim's past technologies out of business because those technologies obsolete their insider trading schemes in the companies they own the stocks of. Their actions are a violation of anti-trust and RICO laws. U.S. Senator's own telecommunications companies and Silicon Valley Social Media

companies. This is a fact! FINCEN and FBI records of all stock market holdings, transfers and communications of U.S. politicians and their family members prove this assertion.

Most of the government officials working on this and related cases were hand-picked by the victim's business and political adversaries, for stone-walling and obfuscation purposes, to cover up the government scams that this investigation exposed and that many of those officials profited on. Web searching the term: *internet censorship*, will explain many of the multi-trillion dollar web scam crimes quite well.

The victim's FBI-class investigators and peers have not found a single entity in the Defendant's listed government 'contacts' who was not either: ***financed by, friends with, sleeping with, dating the staff of, holding stock market assets in, promised a revolving door job or government service contracts from, partying with, personal friends with, photographed at private events with, making profits by consulting for, exchanging emails with, business associates of or directed by; one of those business adversaries, or the Senators and politicians that those business adversaries pay campaign finances to, or supply political search engine manipulation services to.*** FBI and CIA-class Forensic data proves it.

T-Mobile Hacked, Data Stolen Including... Everything

posted on Jun 7th 2009 by Rob Jackson

T-Mobile's website has been on and off today -- probably no coincidence considering hackers have allegedly broken into the T-Mo system, stealing everything you can imagine including:



- Subscriber data
- Databases
- Confidential SIC documents
- Scripts and programs from their servers
- Financial documents up to 2009
- Much more

As if that wasn't bad enough, the brazen bad boys have attempted to sell the data to T-Mobile's competitors! They've been turned down, and for obvious reasons, but the hackers are now trying to auction off the data to the highest bidder.

Sure, they were smart enough to get all the goods, but they had better pray they were able to cover their tracks. Because if they weren't, to quote the movie *Half Baked* (Update 1: It is from "Office Space"), they're going straight to "Federal Pound-Me-In-The-Ass Prison". Then again what are the chances they're from the US? Oh well.

Something similar happened in 2005 and the perpetrator WAS caught.

T-Mobile was the target of a massive 2005 hack, in which Nicholas Jacobsen was charged with unauthorized network access by the U.S. Secret Service. According to published reports, Jacobsen had access to all the information about T-Mobile's 16 million U.S. subscribers.

Although the hackers this time around provided code proving they broke in, T-Mobile has yet to make an official statement or acknowledge the data breach.

Alternative content

UPDATE 2:
T-Mobile's PR firm has contacted me with an official statement on behalf of the company:

"The protection of our customers' information, and the safety and security of our systems, is absolutely paramount at T-Mobile. Regarding the recent claim, we are fully investigating the matter. As is our standard practice, if there is any evidence that customer information has been compromised, we would inform those affected as soon as possible."

[Channel Insider via Engadget]

Trading

Find us on Facebook

62,356 people like Phandroid

January 18th, 2012, 10:02 GMT · By Eduard Kovacs

T-Mobile Hacked by TeamPoison, Administrators and Staff Exposed (Exclusive, Updated)

SHARE: Tweet

Adjust text size: [icon]



The infamous hacktivist collective TeamPoison breached the official website of T-Mobile, one of the largest wireless communications providers in the world, leaking sensitive login information that belongs to their staff and administrators.

The hackers posted a document on Pastebin to prove the success of the operation, but we've contacted them to find out the details and the main reason why T-Mobile is a target.



"They are known to be supporting the Big Brother Patriot Act law. Any cell phone company doing so I would see as a target," said one of the hackers.

"One of the main reasons for the hack is because they are computed, but we also wanted to show how weak their security is."

The hackers found SQL injection vulnerabilities on *t-mobile.com* and *newsroom.t-mobile.com* and managed to get a hold of the names, email addresses, phone numbers and passwords of the administrators and staff members.

"Look at the passwords, epic fail. All the passwords are manually given to staff via an admin who uses the same set of passwords," the hackers said after analyzing the data.

We've tried to get in touch with the company for a statement, but the media contact page is hosted on one of the breached subdomains and it's currently taken offline, which probably means that they're currently dealing with the incident.

TeamPoison is one of the more active collectives from the hacking scene. They are involved in most of the major operations, such as *Op Robin Hood* or *Op Free Palestine* and even if they don't hack too many websites, the ones they do breach are usually important.

They are also the ones that breached the *United Nations servers* back in November 2011, proving that the information they obtained was not outdated as the organization stated after the incident was made public.

Update. Since T-Mobile's media contact website was down yesterday, we contacted Deutsche Telekom, T-Mobile's parent company, for details regarding the incident.

They stated that only the newsroom was compromised and no other T-Mobile proprieties were impacted. The breach hasn't affected their customers in any way.

MORGAN & MORGAN Locations Practice Areas Car Accidents Attorneys

- Contact Form
- FAQ
- Testimonials
- Process
- Results



Download T-MO BREACH



https://www.forthepeople.com/sites/default/files/2021-09/M&M_DOWNLOADABLE_TMOBILE_0

T-Mobile data breach under investigation by Massachusetts Attorney General Maura Healey

Share [Facebook] [Twitter] [Google+]



Updated: 6:39 PM EDT S

Infinite Scroll Enable



The victims have demanded, in writing to FCC, DOJ, OSC, SEC, FBI, that unbiased lawyers and CPAs be provided by The State for the case but none has been provided. As they are now low-income, senior, disabled, felony crime victims, the federal government's LSC Corporation and public-interest law groups have stated that it is their right to receive such case assistance from The State. The victims have contacted NOSSCR, LSC, Legal Aid, People With Disabilities Foundation, NADR, and **all** known local resources on none of those have been responsive to complex, low-income, case work such as this matter and the rest of them had a conflict-of-interest with third parties paid by Defendants.

The assertions provided by a Task Force team of 3 letter agency folks, Congressional staff, investigative reporters and crowd-sourced voters supporting the case investigations are beyond reproach, and true, unless someone refuses to hear the truth due to a personal political agenda.

Other public victims, the peers of the victims have received millions and millions of dollars for their whistle-blowing and as class-action victims but this group has received nothing because their case affects the most famous politicians in modern history!

These contract abuses, human rights abuses and rights blockades are a violation of the victims human rights, U.S. Constitution and State Constitutional rights. (Yes, each State has constitutional rights you get, too)

Some of the corporate executives and their Senators has over \$100 million dollars in their accounts, a fact the FBI can confirm, from stock market manipulations like this. Politically driven, and greed motivated, agency staff are constantly looking for any little opportunity or reason to use agency resources to harm any whistle-blower in reprisal for the success of the anti-corruption task forces they have assisted. The average American cannot even fathom a life where they have ANY million dollars in the bank, much less over \$100 million hidden in various family trust accounts, shell corporations, Cayman Island banks, Ukrainian stealth accounts and other bolt-holes. The kind of people with that kind of money do have people killed, do hire hookers, do hire Fusion GPS and Black Cube and do the wild crimes described herein.

Defendants partnered with Google, Gawker, Gizmodo, YouTube, In-Q-Tel, Fusion GPS and Black Cube to produce tens of millions of dollars of political reprisal media attacks and coordinate toxic exposures against the victims. The attacks have been proven by federal and private investigators to have happened, The source of the attacks, the financiers of the attacks, the beneficiaries of the attacks and the operators of the attacks are the same handful of government people.

The victims are seeking an analytical, objective, reasonable, non-political review of their case. Unlike Julian Assange, Edward Snowden and other whistle-blowers, not only did they do nothing illegal but they are law enforcement and intelligence service consultant who HELP the nation! They are Smedley Butler-like and not Edward Snowden-like!

In recent weeks, the crooked backers of corruption have lost over \$300 billion dollars in stock market failures after profiting in over \$100 TRILLION dollars of stock market profits. People who move that much money around will have people killed, bribe politicians and manipulate government agencies with impunity. That kind of corporate power can get itself anointed as the U.S. Government's free "Obama

Phone” provider (Which T-Mobile has done) and then spy on, and data abuse every poor person who got one of those phones.

It is foolish for any party to ignore the capacity for crime that the Jeffrey Epstein, Harvey Weinstein (ie: his threat to have Jennifer Aniston killed for reporting his sex crimes) and Larry Page oligarchs get involved in, along with the Senators they own and control. T-Mobile executives are on public record and in their own social media cavorting with the sick and twisted top dogs in the billionaire world.

The nature of the core crime case is profound in that it was driven by corporate executives who finance and control White House staff and United States Senators, who ordered attacks on the victims in reprisal.

These famous political figures use the *trillions* of dollars in government treasuries and massive stock market scams for illicit profiteering by rigging the system exclusively for themselves and their crony insiders. They attacked the victims using government taxpayer funded media (Fusion GPS, Black Cube, Google/YouTube/Alphabet, Pysops, Gizmodo Media, Media Matters, Blumenthal, etc.) and spy agency tools because the victims competed with their businesses and reported their crimes. This month the news headlines reveal that San Francisco Bay Area government has as many corrupt politicians as Chicago and relies on the same RICO-violating insider corruption network to operate; as proven by deep AI searches of their financial records. Arrests of those officials are now underway.

Silicon Valley law enforcement records prove that the tech oligarchs that finance these political figures, engage in an organized, racketeering-based, massive sex trafficking, tax evasion, anti-trust violating, spousal abuse, money laundering, black-listing, racist, ageist, political bribery, crony racketeering crime Cartel. The Famous U.S. Senators, Governors and their staff knowingly engage in, finance, operate and benefit from these crimes in exchange for search engine manipulation and stock market insider trading.

The Google, Facebook and Twitter components of this Cartel censor and cover-up news coverage of these crimes, and attacked the victims, because they have a financial connection to the perpetrators.

All of the crooks have had their files hacked. The evidence is out there at the NSA, FBI, etc. Even hackers from Russia and China have copies of the incriminating data. The bad guys will eventually lose!

This is why the attacks on the victims have been so spy agency oriented and high-end: To punish them for helping law enforcement and because the victims accidentally competed with Senator’s stock market schemes by making their products obsolete. There are now thousands of news and Congressional reports; from “Spygate”, to The IRS Lois Lerner case to the FBI McCabe case and a vast number of IG reports, particularly about government agencies being weaponized against citizens for political reprisals. Compromised staff used resources to harm the whistle-blowers and block their rights because they helped halt one of the largest corruption schemes in modern American history.

From FBI-class federal investigators and private investigators, records prove that well known California Senate officials and well known White House officials ordered government services to be blocked, delayed, obfuscated, denied and otherwise harmed as political reprisal and retribution for the assistance the victims supplied to law enforcement.

Criminal forensic data has proven that digital manipulation of some of victims records and files did occur and that T-Mobile computers are regularly hacked by many parties including the China 'Cloud Hopper'

APT 10 group, currently under federal indictment, and hundreds of domestic attack groups, some of whom are hired by U.S. Senators. A number of California and Washington DC Senators and agency heads have already been arrested, indicted and/or removed from office in these matters.

Over 40 of the victims peers in this matter (Rajeev Motwani, Gary D. Conley, Seth Rich, Dr. Epstein's wife, etc.) are now dead from mysterious circumstances. Victims have received numerous death threats and have been personally attacked on multiple occasions including getting their cars rammed and drive-by death threats.

Some of those victims may have been murdered for whistle-blowing. Multiple senior government officials and Senators have been exposed hiring Google, YouTube, Fusion GPS, In-Q-Tel, PsyOps, Cambridge Analytica, ShareBlue, Media Matters, Black Cube, Gizmodo and other "kill services" to attack citizens in political reprisals. Books that cover some of these actions have been published including:

[Catch and Kill](#) *By Ronan Farrow.*

https://en.wikipedia.org/wiki/Catch_and_Kill:_Lies,_Spies,_and_a_Conspiracy_to_Protect_Predators

[Permanent Record](#) *By Edward Snowden.*

<https://www.amazon.com/Permanent-Record-Edward-Snowden/dp/1250237238>

[Brotopia](#) *By Emily Chang.*

<http://brotopiabook.com/>

[Throw Them All Out](#) *By Peter Schweizer.*

<http://peterschweizer.com/books/throw-them-all-out/>

[The Circle \(Based on Google and Facebook\)](#) *By David Eggers.*

<https://archive.org/details/circle00dave>

[World Without Mind](#) *By Franklin Foer.*

<https://www.amazon.com/World-Without-Mind-Existential-Threat/dp/1101981113>

[A Journey into the Savage Heart of Silicon Valley](#) *By Corey Pein.*

<https://www.goodreads.com/book/show/35684687-live-work-work-work-die>

[**Disrupted By Dan Lyons,**](#)

<https://www.goodreads.com/book/show/26030703-disrupted>

[**Chaos Monkeys By Antonio García Martínez,**](#)

<https://www.antonio-garciamartinez.com/chaos-monkeys/>

[**The Creepy Line By Matthew Taylor,**](#)

<https://www.thecreepylines.com/>

[**The Cleantech Crash By Leslie Stahl,**](#)

<https://www.cbsnews.com/news/cleantech-crash-60-minutes/>

[**Congress: Trading Stock By Steve Kroft,**](#)

<https://www.cbsnews.com/news/congress-trading-stock-on-inside-information/>

The complexity and volume of the case documentation in this matter is due to the fact that FBI, DOJ, GAO, SEC, CIA, CFTC, IG and other federal agencies, along with taxpayers, are both involved with, and in some cases assisting with, this case and they have a vested interest in the deep documentation of this matter.

To repeat the key point: The victims' assertions are beyond reproach, and true, unless someone refuses to hear the truth due to a personal political agenda. This is a violation of their human, U.S. and California Constitutional rights. They earned their compensation and damages. (ie: *"Tamosaitis"*, *Maverick Transp., LLC v. U.S. Dep't of Labor, Admin. Review Bd., 739 F.3d 1149, 1157 (8th Cir. 2014)*, [*Jury Awards Former Bio-Rad Counsel \\$11M in Sarbanes-Oxley Whistleblower Case*](#), [*Jury Awards Six Million Dollars to Whistleblower in Sarbanes-Oxley Case*](#), [*Sarbanes-Oxley Whistleblower Recovers Nearly \\$5 Million*](#), [*JP Morgan SOX Whistleblower Wins \\$1.13M at Trial, etc...*](#)) and Pacer.gov settlement records!

In similar related cases Terry Bollea has received \$31 Million in court, Walter Tamosaitis has received \$4.1 Million, etc. I have received nothing and been blocked from having proper legal representation. Most of the whistleblower retaliation statutes adjudicated, including the [SOX, whistleblower protection provision](#), authorize compensatory damages. Two recent decisions, one from the Eighth Circuit and the other from the ARB, indicate that a whistleblower can obtain **substantial compensatory damages based solely on his or her testimony**.

In *Maverick Transportation v. U.S. Department of Labor*, the Eighth Circuit affirmed an ARB decision holding that Maverick Transportation (“Maverick”), a trucking company, had retaliated against Albert Brian Canter, one of its drivers, for refusing to drive a truck that he believed was unsafe. *Maverick Transp., LLC v. U.S. Dep’t of Labor, Admin. Review Bd.*, 739 F.3d 1149, 1157 (8th Cir. 2014). The truck in question had a chaffing brake hose and leaked steering fluid, conditions that substantially increased the likelihood of a catastrophic failure of the service brakes.

Canter sued Maverick under the whistleblower protection provision of the Surface Transportation Assistance Act (“STAA”), which protects truck drivers who refuse to drive due to a reasonable apprehension that a vehicle is unsafe and may cause serious injury to the driver or the public. The ALJ awarded Canter \$75,000 in compensatory damages for emotional distress, despite the fact that Canter offered no corroborating expert testimony. *See* ALJ Case No. 2009-STA-054 (ARB Oct. 28, 2010). In doing so, the ALJ noted that “the ARB has awarded damages for emotional and mental distress where the claims were unsupported by medical evidence.” *Id.* at 15. The opinion indicates that Canter’s testimony regarding his emotional distress was compelling:

- Canter lost his appetite and experienced suicidal thoughts so severe that, on one occasion, he put a pistol to his head; as he started to pull the trigger, he moved his head out of the way and put a bullet hole through the ceiling and roof.
- Canter’s receipt of debt-collection notices and calls from collection agencies caused him great distress.
- Canter’s checking accounts were closed due to insufficient funds, and he owed bank fees and charges for overdrafts.
- Canter was forced to vacate his home in Alabama and move in with his sister in Colorado in July 2008.
- Canter could not visit his stepchildren because he could not afford to travel.

Id.

Maverick appealed to the ARB, which affirmed the ALJ’s determinations “as supported by substantial evidence and prevailing law.” ARB Case No. 11-012, 2012 WL 2588598, at *4 (ARB June 27, 2012). In petitioning the Eighth Circuit for review, Maverick argued that the award of compensatory damages for emotional distress was excessive because it was supported only by Canter’s testimony. The Eighth Circuit denied Maverick’s petition for review, noting that “[a] plaintiff’s own testimony can be sufficient for a finding of emotional distress, and medical evidence is not necessary.” 739 F.3d at 1157 (quoting *Christensen v. Titan Distribution, Inc.*, 481 F.3d 1085, 1097 (8th Cir. 2007)). The Eighth Circuit also suggested that the ARB properly awarded compensatory damages based on the severity of the injuries, rather than on the type of evidence used to prove those injuries. *See id.* at 1157–58.

The ARB also recently affirmed a substantial award of compensatory damages based solely on a whistleblower’s testimony. In *Fink v. R&L Transfer, Inc.*, the ARB affirmed the ALJ’s award of \$100,000 in compensatory damages and \$50,000 in punitive damages to a truck driver who was terminated for refusing to drive in unsafe winter weather. *Fink v. R&L Transfer, Inc.*, ARB Case No. 13-018 (ARB Mar.

19, 2014). In awarding compensatory damages, the ALJ relied on Fink's testimony that, among other harms:

- he had to seek public assistance to pay basic living expenses;
- his family ultimately lost its home;
- he had to borrow money from family members; and
- he had difficulty sleeping, wondering how he would be able to support his family.

Id. In affirming the award of \$50,000 in punitive damages, the ARB stated that “[a]n award of punitive damages may be warranted where there has been ‘reckless or callous disregard for the plaintiff’s rights, as well as intentional violations of federal law.’” *Id.* (citation omitted).

In addition to obtaining large compensatory damages awards at trial that are affirmed on appeal, some whistleblowers are obtaining substantial compensatory damages awards from OSHA. For example, in September 2013, OSHA issued an order requiring Clean Diesel Technologies, Inc., to pay \$1.9 million to its former chief financial officer, who was fired for warning the board of directors about ethical and financial concerns raised by a proposed merger. In addition to awarding \$486,000 in lost wages, bonuses, stock options, and severance pay, OSHA awarded the complainant more than \$1.4 million in compensatory damages for pain and suffering, damage to career and professional reputation, and lost 401(k) employer matches and expenses.

Some of the federal whistleblower protection laws authorize an award of uncapped compensatory damages, including the [Sarbanes-Oxley whistleblower protection law](#), the [False Claims Act whistleblower protection law](#), and the [NDAA whistleblower retaliation law](#). Recent jury verdicts indicate that compensatory damages can be substantial, and can even exceed one million dollars.

The following are some recent jury verdicts in whistleblower cases:

- [Jury Awards Former Bio-Rad Counsel \\$11M in Sarbanes-Oxley Whistleblower Case](#)
- [Jury Awards Six Million Dollars to Whistleblower in Sarbanes-Oxley Case](#)
- [Sarbanes-Oxley Whistleblower Recovers Nearly \\$5 Million](#)
- [JP Morgan SOX Whistleblower Wins \\$1.13M at Trial](#)

In 2014, we will likely start seeing more whistleblower retaliation appeals seeking compensatory damages. The changes to the law “may also lead to more addendum appeals such as claims for compensatory and other damages or attorney’s fees,” the MSPB warned in its latest [Annual Performance Report and Plan](#). We will also start getting a better sense of the fiscal implications of the WPEA’s compensatory damages provision. At the Equal Employment Opportunity Commission (EEOC), agencies found to have violated anti-discrimination laws were ordered to pay \$7.2 million in compensatory damages in cases closed in fiscal year 2011. The U.S. Postal service accounted for 51 percent of that amount, according to the EEOC’s latest [Annual Report on the Federal Work Force](#).

Murdering Our Children For Profit

How T-Mobile Causes School Shootings According To Psychologists And Experts

The highest murder rate in decades. The highest rates of robbery and rape. It's no wonder a young man with mental health issues committed a horrendous act of violence.

2018?

No. 1980. T-Mobile has been doing this since 1980!

In 1980, the [murder rate](#) (murders per 100,000 population) was 10.2. If we could only go back to a more peaceful time. Say ... 1960. Except 1960 was more violent than 2016 (the last year full details are available) — 5.1 murders per 100,000 compared to 5.0.

What can explain the actions of the accused Florida shooter, Nikolas Cruz? What else did Cruz have unlimited access to, that could have had an influence on him?

Social media. Especially access to violent and harmful social media.

[Nikolas Cruz](#) allegedly did everything except call law enforcement with the exact date, time and location of his intended massacre. Criminals don't make appointments, but they do leave clues. Nikolas Cruz did — a [ton](#) of [them](#), [online](#):

- Instagram pictures of mutilated frogs, weapons and knives.
- "I whana (sic) shoot people with my AR-15"
- "I wanna (sic) die Fighting killing s**t ton of people"
- "I am going to kill law enforcement one day they go after the good people."
- "Im (sic) going to be a professional school shooter." Signed with his real name.
- "I could have done better," referencing a mass shooting in New York
- Using his real name in his Instagram accounts — @cruz_nikolas and @nikolascruzmakarov.
- Snapchat (now Snap) video showing Cruz cutting his arms.

The real reason the FBI and local law enforcement didn't connect the dots is because they don't fully understand the new dots of social media. To grasp how social media can have such a massive impact, compare its growth and the tragic increase in the suicide rate for children and teens ages 10-19.

[Since 2010](#), the monthly active users for Facebook has grown 300 percent to over 2 billion and for Twitter, 511 percent to 330 million. Since 2013, Whatsapp has grown 225 percent to over 1.4 billion and Instagram, 433 percent to 800 million. Since 2014, Snap has grown 159 percent to 187 million and Facebook Messenger, 140 percent to 1.2 billion.

[YouTube is a little different](#). Watching video doesn't need an account. To put this behemoth in perspective, there are 300 hours of video uploaded every minute. There are over 30 million visitors per day watching 5 billion videos.

From [2007 to 2015](#) (the last year data are available) the suicide rate for boys ages 10-14 increased 200 percent; for girls ages 10-14, 320 percent; for boys ages 15-19, 127 percent and for girls 15-19, 204 percent. Suicide went from the fourth leading cause of death for boys ages 10-14 to second. For girls ages 10-14, it went from sixth to third. Suicide passed homicide as the second leading cause of death for boys ages 15-19, and jumped from fourth to second for girls ages 15-19.

Consider further the lessening risks our children and teens face from homicide, compared to their risk for suicide, according to data from the FBI and CDC:

Fact 1: The homicide rate for 10-14 year olds in 2015 was half of what it was in 1979 (.05 vs .10).

Fact 2: The suicide rate for 10-14 year olds in 2015 is almost double what it was in 1979 (.13 vs .07). It's the highest rate in over 36 years.

Fact 3: The homicide rate for 15-19 year olds in 2015 is almost half of what it was in 1979 (.45 vs .95).

Fact 4: The suicide rate for 15-19 year olds in 2015 was 21 percent lower than in 1979 (.63 vs .79). Starting in 2007, the suicide rate began increasing after 18 years of dropping. The homicide rate also peaked that same year. In 2011, suicide overtook homicide as a cause of death for both boys and girls age 15-19. Suicide has become the second leading cause of death for boys since 2008, and since 2013 for girls.

Children ages 10-19 are statistically twice as safe from homicide as they were 36 years ago, even though the population has increased 45 percent (225 million in 1979 to 325 million in 2015).

The deluge of negative social media can't be ignored when the suicide rates for our children have increased on average 212 percent since 2007. Which begins to explain how Nikolas Cruz may have ended up with his warped view of reality.

Garbage in — garbage out.

Take Instagram as an example, where Cruz is alleged to have made many of his posts. Searching by hashtags reveals much of the violence, negative influence and harmful aspects. Want to see pictures of teens committing self-harm by cutting themselves with razors? Check [#selfharmmm](#). Over 2 million posts. Cruz is thought to have also posted to Snap a video of cutting himself.

Another hashtag of [#suicidal](#) has over 4.7 million posts. And [#suicide](#) has over 7 million posts. On the morning of the shootings, I was conducting research of several posts on Instagram. The following, unrelated to the shooting, was posted on Feb. 14, shortly before 9 a.m. EST; the shootings at Douglas High School didn't begin until about 2 p.m. EST:

I had been heads-down working on some large projects on Feb. 14: No news, no social media, no web surfing. I recorded this [Facebook Live](#) around 6 p.m., still unaware of the shootings. I showed this picture of the Instagram post and asked what parents would do if they saw their children had posted this. In fact, I had completed a guide on Instagram called [Talking in Code: Instagram Hashtags-What You Don't Know and Why It's Dangerous](#).

In her [book](#) “iGen: Why Today’s Super-Connected Kids are Growing up Less Rebellious, More Tolerant, Less Happy — and Completely Unprepared for Adulthood — and What This Means for the Rest of Us,” Jean Twenge, PhD and professor of psychology at San Diego State University, conducted fascinating research into the generation Nikolas Cruz is smack in the middle of.

Her research showed that today’s connected 18-years-olds are more like 14-year-olds and 8th graders who spend 10 or more hours a week on social media are 56 percent more likely to be unhappy than those who don’t.

Teens are physically safer than ever, yet they are more mentally vulnerable.

Violence in — violence out.

I, Morgan Wright am an expert on cybersecurity strategy, cyberterrorism, identity theft and privacy. He’s currently a Senior Fellow at the Center for Digital Government. Previously Morgan was a senior advisor in the U.S. State Department Antiterrorism Assistance Program and senior law enforcement advisor.

The recent suicides of Ritu Sachdeva and Hillary "Kate" Kuizon, both 17-year-old seniors at Plano East Senior High School, in Plano, Texas, as well as those of two students at a prestigious all-boy preparatory high school in Bronx, N.Y. underscore [the disturbing increase](#) in suicide amongst young people— up at least 13 percent from 2010.

The reasons for this increase will be the subject of research studies for years, but I have a theory, which comes from my work with patients in this age group.

For some time now, I have noted that young people— including adolescents, teenagers and those in their 20s— are disconnected from the reality of their own existences. Facebook, Twitter, Tinder and the like have made them think of themselves as mini-reality-TV versions of themselves. Too many of them see their lives as a series of flickering photos or quick videos. They need constant doses of admiration and constant confirmation of their tenuous existence, which come in the form of Facebook “likes” and Twitter “retweets.”

This substitution of media for real meaning has not only been shown to weaken their self-esteem and their ability to sustain themselves through adversity, but it can cheapen the value they assign to life in general—including their own lives. If all the world is a stage of pixels, and young people see themselves as their tweets and Snapchat photos, then taking a fist-full of pills could seem like no more than the equivalent of shutting down a Facebook account or turning off an iPhone.

Call it, “Suicide by Social Media.”

See, to the extent that one is never truly alive, one can entertain the notion of killing oneself, without the normal psychological hurdles. People do not long grieve the death of fictional characters in film or TV. And our young people are at risk of seeing themselves as no more solid or substantive.

This is one reason, by the way, that drugs like heroin are rampant. Heroin kills real feelings. And young people are, increasingly, strangers to dealing with real feelings. Heroin is just the powdered equivalent of text messaging, YouTube, Twitter, Facebook and the rest of the technology drugs Americans— especially American teen— are mainlining every single day.

This is one reason why young people are increasingly fascinated with dramas about vampires and zombies. They know something about the walking dead.

More on this...

- [The science of suicide clustering: How silence can increase stigma](#)
- [Suicide risk factors for US Army soldiers identified](#)
- [3rd-generation Marine on a mission to bring awareness to veteran suicide](#)

Yes, they try to insulate themselves by having more and more and more sex, with more and more partners, but, ultimately, that doesn't convince them they are more than their bodies. To fully want to live, to fully resist death, even amidst adversity, one must be convinced that one has a soul and a true destiny.

The recent suicides of Ritu Sachdeva and Hillary "Kate" Kuizon, both 17-year-old seniors at Plano East Senior High School, in Plano, Texas, as well as those of two students at a prestigious all-boy preparatory high school in Bronx, N.Y. underscore [the disturbing increase](#) in suicide amongst young people— up at least 13 percent from 2010.

The reasons for this increase will be the subject of research studies for years, but I have a theory, which comes from my work with patients in this age group.

For some time now, I have noted that young people— including adolescents, teenagers and those in their 20s— are disconnected from the reality of their own existences. Facebook, Twitter, Tinder and the like have made them think of themselves as mini-reality-TV versions of themselves. Too many of them see their lives as a series of flickering photos or quick videos. They need constant doses of admiration and constant confirmation of their tenuous existence, which come in the form of Facebook “likes” and Twitter “retweets.”

This substitution of media for real meaning has not only been shown to weaken their self-esteem and their ability to sustain themselves through adversity, but it can cheapen the value they assign to life in general—including their own lives. If all the world is a stage of pixels, and young people see themselves as their tweets and Snapchat photos, then taking a fist-full of pills could seem like no more than the equivalent of shutting down a Facebook account or turning off an iPhone.

Call it, “Suicide by Social Media.”

See, to the extent that one is never truly alive, one can entertain the notion of killing oneself, without the normal psychological hurdles. People do not long grieve the death of fictional characters in film or TV. And our young people are at risk of seeing themselves as no more solid or substantive.

This is one reason, by the way, that drugs like heroin are rampant. Heroin kills real feelings. And young people are, increasingly, strangers to dealing with real feelings. Heroin is just the powdered equivalent of text messaging, YouTube, Twitter, Facebook and the rest of the technology drugs Americans— especially American teen— are mainlining every single day.

This is one reason why young people are increasingly fascinated with dramas about vampires and zombies. They know something about the walking dead.

More on this...

- [The science of suicide clustering: How silence can increase stigma](#)
- [Suicide risk factors for US Army soldiers identified](#)
- [3rd-generation Marine on a mission to bring awareness to veteran suicide](#)

Yes, they try to insulate themselves by having more and more and more sex, with more and more partners, but, ultimately, that doesn't convince them they are more than their bodies. To fully want to live, to fully resist death, even amidst adversity, one must be convinced that one has a soul and a true destiny.

Facebook will never achieve that. Neither will Twitter. Or Snapchat. Or YouTube. Or any other sorry excuse for communication, connection, admiration, respect or love.

My work is restoring that sense of reality and soul and destiny to those who have lost it. And too many young people— who are disciples of nothing more than technology— *have* lost it. For them, horrifically, precipitating their own deaths feels like little more than scripting the suicides of actors. And the expressions of grief from “friends” who then inscribe their posthumous Facebook pages are just a bunch of nonsense that perpetuates the epidemic.

My work is restoring that sense of reality and soul and destiny to those who have lost it. And too many young people— who are disciples of nothing more than technology— *have* lost it. For them, horrifically, precipitating their own deaths feels like little more than scripting the suicides of actors. And the expressions of grief from “friends” who then inscribe their posthumous Facebook pages are just a bunch of nonsense that perpetuates the epidemic.

T-Mobile's partnership, hosting, promoting, networking, embedding of apps and political tricks with Silicon Valley social media companies is killing the world!

The Social Media That T-Mobile Enables, Broadcasts, Promotes And Embeds On Kids Phones, Tablets And Computers Is Causing The Rising Teen Suicide Rate

Rates of suicide and self-harm are rising in teens. Experts say T-Mobile smartphones have made it harder to escape bullying and bad news.

Sadie Riggs, 15, killed herself in June. Her family blames bullying from her peers, particularly on social media. Courtesy of Sarah Smith

•

Sadie Riggs loved helping others.

The bubbly 15-year-old dreamed of becoming a firefighter, a lawyer, or veterinarian. She was passionate about drawing and spending time outside with her dogs in her small town of Bedford, Pennsylvania, about 100 miles east of Pittsburgh.

Sadie had overcome challenges before — her biological mom, a drug addict, abandoned her when she was little — but in her final year of life, the high school freshman's biggest obstacle was bullying from her peers.

"The kids started making fun of her for her red hair and braces," said Sarah Smith, the aunt whom Sadie lived with. "The kids told her only devils had red hair."



Sadie

Riggs, 15, killed herself in June. Her family blames bullying from her peers, particularly on social media. Courtesy of Sarah Smith

The taunting started in the school hallways but became inescapable, Smith said. Sadie was tormented on Facebook, Instagram, messaging platform Kik — where classmates would tell her to kill herself.

"I went to the police. I went to the school. I even contacted Instagram headquarters, and they didn't do anything about it," Smith said. "So finally I smashed her phone. I broke it in half. She was bawling every day and I couldn't take it anymore."

But the bullying had already taken its toll. On June 19, barely a week after Smith took her phone, Sadie hanged herself.

In the age of what some are calling the "screenager" — with teens averaging more than 6.5 hours of screen time every day, according to nonprofit [Common Sense Media](#) — suicide prevention experts are wondering if enough is being done to protect young minds online.

Related: [Suicides in Teen Girls Hit 40-Year High](#)

Recent studies have shown a rise in both teen suicides and self-harm, particularly among teenage girls Sadie's age.

An [analysis by the Centers for Disease Control and Prevention](#) in August found the suicide rate among teenage girls ages 15 to 19 hit a 40-year high in 2015. Between 2007 and 2015, the rates doubled among girls and rose by more than 30 percent among teen boys.

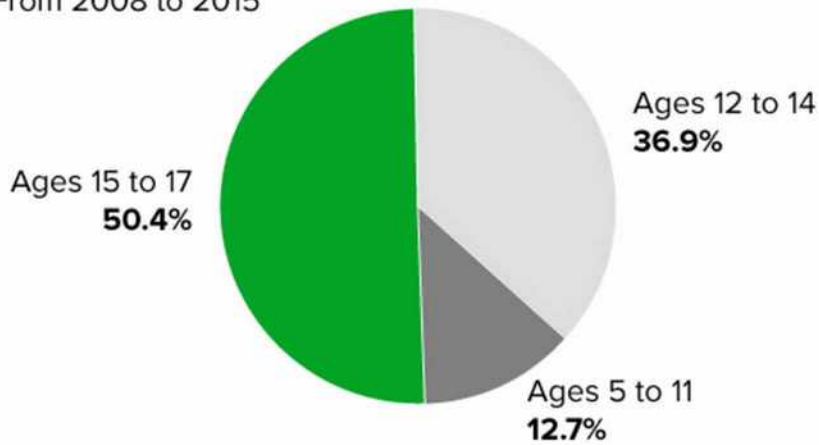
And just this past week, [researchers in the U.K. published](#) similar discoveries in a study on self-harm that showed a dramatic increase in the number of adolescent girls who engage in it: Self-harm rose 68 percent in girls ages 13 to 16 from 2011 to 2014, with girls more common to report self-harm than boys (37.4 per 10,000 girls vs. 12.3 per 10,000 boys).

Suicide-Related Hospital Admissions Nearly Double For Children



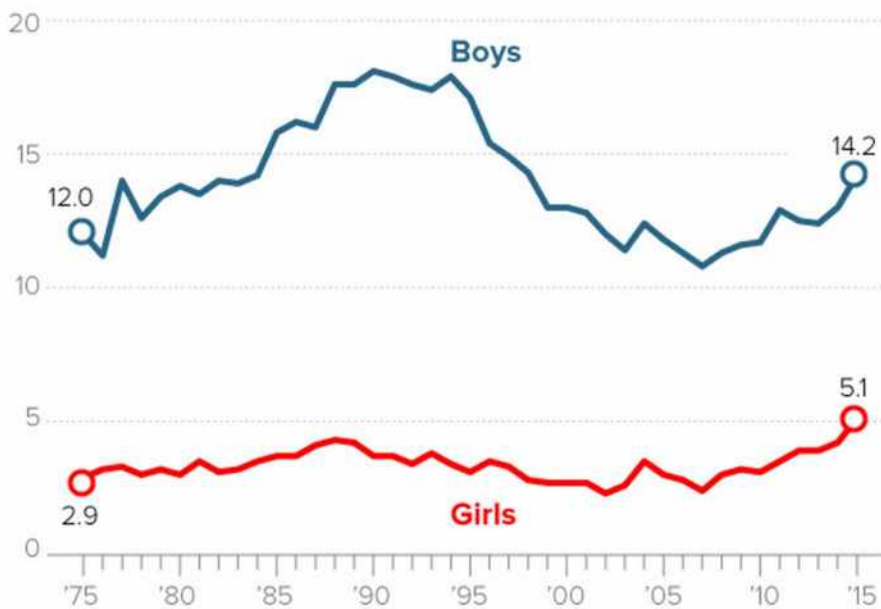
And More Than Half Of The Patients Were Late Teens

From 2008 to 2015



Suicide Rates On the Rise For Late Teens

Rate per 100,000 deaths. Ages 15 to 19



across the board, including for teens. Researchers say there are multiple reasons for the uptick. NBC News It's unclear how much of a role social media plays in suicides, but a [study earlier this year](#) tied social media use with increased anxiety in young adults.

Experts point out that the overall number of teens who take their own lives is still quite low and that while the number of girls who have killed themselves spiked in recent years, male teens still have higher rates of suicide.

They also say smartphones alone aren't singularly responsible for suicidal thoughts.

"The increases in suicide rates are unlikely to be due to any single factor," said Dr. Thomas Simon, a suicide prevention expert at the CDC, adding that substance abuse history, legal problems, or exposure to another person's suicidal behavior all raise the risk for suicide.

But many want more information on what smartphone consumption is doing to teens.

Related: [Colorado Dad Wants State to Ban Smartphones for Kids Under 13](#)

In an article last month in The Atlantic, "[Have Smartphones Destroyed a Generation?](#)", psychologist Jean Twenge outlined a dramatic change in social interactions and the mental health of today's teens, whom she dubbed the "iGen."

"It's not an exaggeration to describe iGen as being on the brink of the worst mental-health crisis in decades. Much of this deterioration can be traced to their phones," Twenge wrote.

Filmmaker Dr. Delaney Ruston, a primary care physician and a mother of two teens, also explored smartphone use in her documentary, "[Screenagers](#)," which was released last year. Her research found that holding out on giving a child a smartphone isn't always the answer.

"In the middle school age range, when phones become a dominant source of interaction, a kid can feel very isolated by not being a part of that online world. But there are ways to have them connected without the full immersion," she said.



Burger King takes on bullying with powerful PSA

Ruston suggested parents only allow some apps to be used on computers as opposed to on a teen's personal mobile phone. She also encouraged parents to talk about setting boundaries with fellow parents and institute screen-free carpool and play dates.

"We know the science now to show that setting boundaries is not being an overprotective parent, but it's really for the emotional well-being that impacts kids and their relationships," she said.

Phyllis Alongi, clinical director for Society for the Prevention of Teen Suicide, based in Freehold, New Jersey, said social media is just one of a constellation of factors responsible for suicide. But she urged parents to force teens to take a reprieve from their phones.

Related: Role Models? Parents Glued to Screens 9 Hours a Day

"They can't turn it off, nor do they want to or know how to," she said. "It's stunting their coping skills, their communication skills."

Dr. Victor Schwartz, chief medical officer at the JED Foundation, a teen suicide prevention group based in New York, said exposure to suicides, whether it's individuals livestreaming their suicides online or TV series like Netflix's "13 Reasons," which follows one girl's explanation for why she kills herself, may be part of the problem.

"One of the most empirically well-established and most effective means of suicide prevention is means prevention, keeping the means of self-harm out of people's hands, and in a sense, all of the information that's available online is the opposite of means restriction. It's means promotion in a way," he said.



'13 Reasons Why' should be taken off the air, psychiatrist urges, yet T-Mobile pushes Netflix and it's woke agenda to kids

Social media can be positive in that it offers ways to be in touch and provide support for one another, Schwartz said.

But, he added, the virtual world can turn ugly — fast.

"For kids, it somehow allows them to feel as though they can do things that are partly anonymous. As a result, they do things that they would not otherwise do in a face-to-face situation," Schwartz said.

"The second piece is the magnifying effect. Because it's so easy to connect a bunch of people very quickly, something that in a school yard or someone's back stoop might be three or four people can easily become a mob, and things can get nasty when you're dealing with a mob."

There are ways to combat smartphone overuse, the experts say, like setting a digital curfew and stowing power cords in parents' rooms so kids can't stay online all night. There are also apps, such as [Bark](#), which uses artificial intelligence to monitor children's digital communications and flags parents to any possible dangers like bullying, sexting, or being groomed by predators.

Ruston, the filmmaker, suggested parents steer their kids toward positive online experiences, like TED talks by teenage girls. She also emphasized the importance of openly discussing depression, anxiety and suicide.

"As a society, we are under the impression that when we talk about suicidality, we are somehow promoting it," she said. "Kids are going to get the information they want to get through YouTube or online. We need to become more proactive."

If you or anyone you know is feeling suicidal, you can call the National Suicide Prevention Hotline 24 hours a day at 1-800-273-8255; or contact Crisis Text Line, a confidential service for those wanting to text with a crisis counselor, by texting HOME to 741741.

Suicide is a serious problem among American teens. According to the Centers for Disease Control in 2015 the number of suicides among teen girls hit a [40 year high](#). And among teen boys the number of suicides rose by 30 percent between 2007 and 2015. Why? Some are wondering if it has to do with social media.

Almost every teen now has an account on at least one social media platform. They use it to reach out to friends, to share experiences, and to tell the world about themselves. However, they also may be making themselves vulnerable.

"Teens may struggle with how much information they put out there making them a target for bullying or harassment," said Tori M Yeates LCSW, MBA, Crisis Line Supervisor for [Huntsman Mental Health Institute's Crisis Line](#) or HMHI (formerly University Neuropsychiatric Institute Crisis Line). "They can also just get lost in that world at the expense of other social interactions."

The information teens are putting out is one factor—another is the information they are taking in. Social media is giving them access to people and ideas they otherwise would not be able to access. And not all of that is good. Some is actually designed specifically to harm. "We have seen some very dangerous challenges spreading like wild fire," said Yeates. "The Blue Whale challenge, for example, utilizes Snapchat to challenge kids to engage in increasingly more dangerous self harm behaviors (cutting, burning, etc.) culminating in the individual killing him/herself."

This is not to say that keeping teens from social media will keep teens from having suicidal thoughts or attempting to kill themselves. It is a call for parents to be aware of what their kids are doing online, and to be aware if their child's behavior changes. "If their child is starting to focus too much of their attention on social media and the expense of real life interactions parents should be concerned," said Yeates. "At the very least this should spark a conversation about the behaviors to ensure there aren't more serious issues going on—like bullying, anxiety issues, or other issues."

Parents should also look for behaviors not necessarily related to social media that may signal a problem. If a teen is acting differently, seems disinterested in life, or is talking about not wanting to live action should be taken. It can be a hard conversation to have—but it might save their life. "Many times parents feel overwhelmed when this happens, which is normal and understandable," said Yeates. "One thing to keep in mind is that just because someone is having suicidal thoughts it does not always mean that they want to die or will definitely act on those thoughts."

Parents aren't the only ones who should be on alert. Friends also should be aware when it appears someone is in trouble. They may even have more insight into the situation. One thing all teens should know is that if a friend appears to be considering suicide they should not write it off as someone being "dramatic" or seeking attention. "All suicidal behavior should be taken seriously, period," said Yeates. "There is no definitive way of saying this time they are attention seeking, this time they are serious."

Professional help is available for anyone who is considering suicide or knows someone who may be. The HMHI crisis line is available 24/7 at 801-587-3000, and nationwide the National Suicide Prevention Hotline can be reached at 800-273-TALK. Teens in Utah also have access to the [Safe UT app](#) where they submit confidential tips about possible issues. "Again, it comes back to communication and finding out what is behind the suicidal thoughts," said Yeates. "Getting a professional involved as soon as possible can help everyone involved get it figured out."

CHICAGO — An increase in suicide rates among US teens occurred at the same time social media use surged and a new analysis suggests there may be a link.

Suicide rates for teens rose between 2010 and 2015 after they had declined for nearly two decades, according to data from the federal Centers for Disease Control and Prevention. Why the rates went up isn't known.

The study doesn't answer the question, but it suggests that one factor could be rising social media use. Recent teen suicides have been blamed on cyberbullying, and social media posts depicting "perfect" lives may be taking a toll on teens' mental health, researchers say.

"After hours of scrolling through Instagram feeds, I just feel worse about myself because I feel left out," said Caitlin Hearty, a 17-year-old Littleton, Colorado, high school senior who helped organize an offline campaign last month after several local teen suicides.

"No one posts the bad things they're going through," said Chloe Schilling, also 17, who helped with the campaign, in which hundreds of teens agreed not to use the internet or social media for one month.

The study's authors looked at CDC suicide reports from 2009 to 2015 and results of two surveys given to US high school students to measure attitudes, behaviors and interests. About half a million teens ages 13 to 18 were involved. They were asked about use of electronic devices, social media, print media, television and time spent with friends. Questions about mood included frequency of feeling hopeless and considering or attempting suicide.

The researchers didn't examine circumstances surrounding individual suicides. Dr. Christine Moutier, chief medical officer at the American Foundation for Suicide Prevention, said the study provides weak evidence for a popular theory and that many factors influence teen suicide.

The study was published Tuesday in the journal [Clinical Psychological Science](#).

Data highlighted in the study include:

- Teens' use of electronic devices including smartphones for at least five hours daily more than doubled, from 8 percent in 2009 to 19 percent in 2015. These teens were 70 percent more likely to have suicidal thoughts or actions than those who reported one hour of daily use.

- In 2015, 36 percent of all teens reported feeling desperately sad or hopeless, or thinking about, planning or attempting suicide, up from 32 percent in 2009. For girls, the rates were higher — 45 percent in 2015 versus 40 percent in 2009.
- In 2009, 58 percent of 12th-grade girls used social media every day or nearly every day; by 2015, 87 percent used social media every day or nearly every day. They were 14 percent more likely to be depressed than those who used social media less frequently.

“We need to stop thinking of smartphones as harmless,” said study author Jean Twenge, a psychology professor at San Diego State University who studies generational trends. “There’s a tendency to say, ‘Oh, teens are just communicating with their friends.’ Monitoring kids’ use of smartphones and social media is important, and so is setting reasonable limits, she said.

Dr. Victor Strasburger, a teen medicine specialist at the University of New Mexico, said the study only implies a connection between teen suicides, depression and social media. It shows the need for more research on new technology, Strasburger said.

He noted that skeptics who think social media is being unfairly criticized compare it with so-called vices of past generations: “When dime-store books came out, when comic books came out, when television came out, when rock and roll first started, people were saying, ‘This is the end of the world.’”

With its immediacy, anonymity, and potential for bullying, social media has a unique potential for causing real harm, he said.

“Parents don’t really get that,” Strasburger said.

Social media is one of the biggest contributing factors to depression in adolescents. Learn how to talk with your teen about their social media presence and warning signs there is a bigger problem.

- [Social media, self-esteem, and teen suicide](#) caused by T-Mobile

Is T-Mobile Liable For “*Complicit Homicide*” By Allowing Teens To Use Facebook, Google and Instagram, Who Are Facing Lawsuits for Teen Mental Health Crisis, In A MASSIVE Profits-Over-Safety Mobile Services Abuse Charge

Neumann Law Group is now investigating claims against Meta Platforms, Inc., the parent company of Facebook and Instagram for their intentional manipulation of the mental health of young and at-risk users of their products.

In October 2021, a Facebook whistleblower testified to the U.S. Senate how Facebook, Instagram, and

Meta used tactics to manipulate young people into using their products for extended periods of time and intentionally created a toxic environment leading to significant psychological harm to America's youth.

[Learn More at Neumann Law Group](#)

SEE THIS LINK, THIS HAPPENS EVERY FEW HOURS THANKS TO MARK AND SHERYL: Every few hours another teen is MURDERED by Facebook/Instagram executives. Nobody does anything about it because California politicians OWN the stock in Facebook/Instagram and also get their political campaign cash from Facebook/Instagram/Google !!! Should Mark Zuckerberg be charged with Homicide? He knew, for over a decade, that he was killing these kids, but buying a part of Hawaii is expensive, and he needed the cash!

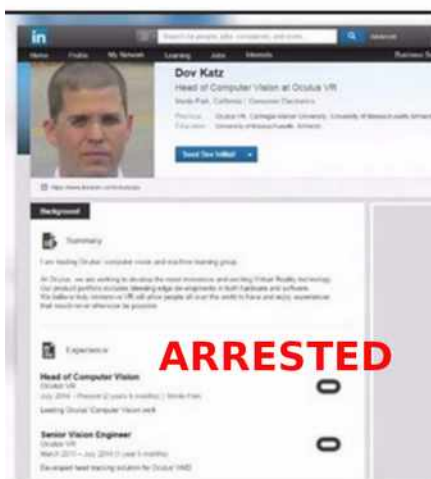
THE UNITED STATES CONGRESS CAN MAKE INSTAGRAM AND FACEBOOK DISAPPEAR OFF THE INTERNET, IN ANY 60 SECOND PERIOD, SIMPLY BY ORDERING DOJ TO DELETE THEIR DNS RECORDS. BOOM! GONE!

DEMAND THAT YOUR ELECTED OFFICIALS ORDER THE DNS RECORDS FOR INSTAGRAM AND FACEBOOK DELETED, AND NOT TURNED BACK ON, UNTIL FACEBOOK AND INSTAGRAM PROVE TO CONGRESS THAT NO TEENS WILL BE AFFECTED BY THEIR SITES AGAIN!

DO YOU REALLY WANT YOUR KIDS ANYWHERE NEAR FACEBOOK AND THEIR VR SEX PERVERTS?:

FACEBOOK EXECS HAVE A CHILD SEX RING - MULTIPLE ARRESTS - ONGOING INVESTIGATIONS - FACEBOOK VR BOSS ARRESTED

senior Facebook executive, 35, was caught in pedophile sting after 'grooming a 13-year-old boy with sick messages and arranging to meet up in Ohio hotel room'



Were you a minor when you signed up for Facebook and/or Instagram; Were you using Facebook and/or Instagram for more than three (3) hours per day at that time; and Have you received documented mental health treatment (with no prior history of mental health issues)?

[Facebook grilled in Senate hearing over teen mental health - Sheryl Sandberg knew...](#)

techcrunch.com/.../30/facebook-grilled-in-senate-hearing-over-teen-mental-health

Facebook grilled in Senate hearing over teen mental health. Last night, Facebook published two annotated slide decks in an attempt to contextualize the documents that The Wall Street Journal ...

[Facebook's whistleblower report confirms what researchers ...](#)

theverge.com/2021/10/6/22712927/facebook-instagram-teen-mental-health-research

Internal research at Facebook showing that Instagram might be harmful to the mental health of teen girls is in line with other research in the field. That complicates efforts to minimize the findings.

[This is Facebook's internal research on the mental health effects of ...](#)

theverge.com/2021/9/29/22701445/facebook-instagram-mental-health-research...

The release of the research arrives the evening before a Congressional hearing on the effect of Facebook and Instagram on kids' mental health. That hearing is scheduled for Thursday at 10:30AM ET .

B

[Instagram Youth Adds Risk to Teen Mental Health. Facebook Must Act .."Instagram turns young girls into hookers..."](#)

bloomberg.com/opinion/articles/2021-09-22/instagram-youth-adds-risk-to...

So perhaps it isn't surprising that an internal research effort at the company, revealed last week, found that teens associate the service with a host of men

[Facebook Very Aware That Instagram Harms Teen Mental Health But Profits On Its Crimes](#)

thecut.com/2021/09/facebook-very-aware-that-instagram-harms-teen-mental...

For several months now, Facebook execs have been kicking around an eerie product idea few people seem to want: Instagram for Kids.

[Facebook knows Instagram is bad for teenagers' mental healthbut wants the profits anyway](#)

businessinsider.com/facebook-internal-report-shows-instagram-bad-for-teens...

Facebook's internal research shows that teen users' mental health is negatively impacted by using the company's photo- and video-sharing app, Instagram.

Want to help end the tech oligarch's rape of society? Never, EVER: use, read, quote, link to, paste from, or refer to; anything on corrupt and contrived: Twitter - Google - Alphabet - Facebook - Meta - Instagram - Netflix or YouTube! Don't expand their reach! Don't be their digital bitch! Stop being an addict to Silicon Valley's social media scam! Keep the battery out of your phone so Big Tech can't continue to spy on you. Did you know you CAN'T turn an iPhone off. Apple iPhone's pretend to be "off" but still monitor you with reserve power. The government should shut these companies down but they don't because these companies pay the largest bribes on Earth to politicians! Demand that Congress shut down these big tech abusers that cause child suicides, bullying, sex trafficking, money laundering, tax evasion, political bribery, election manipulation and other social crimes.

Have you, or your teen, suffered from?

- Depression
- Anxiety
- Eating disorders
- Body Dysmorphia
- Self-harm
- ADD/ADHD
- ODD
- Selling their bodies (Instagram is now the #1 source IN THE WORLD, for teenage prostitutes. Rappers spend 1/2 the day talking young girls on Instagram into 'free plane tickets')
- Suicidal ideation
- Suicidal attempts
- Any and all other mental health illnesses

[Facebook acknowledges Instagram's damage to teen mental health, but ...](#)

mashable.com/article/facebook-instagram-teen-body-image

The Wall Street Journal viewed several internal Facebook documents discussing the issue of teen mental health, the company having performed various focus groups and surveys between 2019 and 2021 ...

[Harmed by Social Media: Facebook, Instagram Linked to Teen Mental ...](#)

omalleylangan.com/posts/facebook-linked-to-teen-mental-health-issues

Hold social media platforms accountable for their actions. Contact our law firm to explore your options. Social media platforms like Facebook and Instagram have been linked to a recent increase in depression and other mental health issues among teenagers, according to researchers and journalists studying this issue, including an in-depth investigation conducted by The Wall Street Journal and ...

[Facebook Knew Instagram Was Harmful to Mental Health of Teen Girls ... Profits over Child Safety](#)

verywellmind.com/facebook-knew-instagram-was-harmful-to-mental-health-of...

One internal Facebook presentation stated that among teens who reported suicidal thoughts, 13% of British users and 6% of American users believed Instagram was to blame. Facebook also found that 14% of boys in the U.S. said Instagram made them feel worse about themselves, reported the Journal. Researchers highlighted Instagram's Explore page, which provides users with curated posts from a wide ...

[Facebook publishes slides on how Instagram affects teen mental health](#)

yahoo.com/entertainment/facebook-research-instagram-teen-mental-health...

Facebook has published two slide decks detailing its research into how Instagram affects teens' mental health. The slides were heavily cited by The Wall Street Journal earlier this month in a ...

Do you believe that you or a loved one may have experienced psychological harm due to the negligence of Google, Instagram, Facebook? Call Neumann Law Group today to discuss your claim and share this notice with those you care about below:

[Share This Notice](#) On Facebook

[Share This Notice](#) on Twitter

[Share This](#) Notice on LinkedIn

[Share This Via Email](#)

END FACEBOOK'S, GOOGLE'S, YOUTUBE'S, INSTAGRAM'S AND NETFLIX DARK MONEY PAYOLA TO OUR POLITICIANS

YOU CAN'T PROTECT YOUR KIDS IF FACEBOOK, GOOGLE, INSTAGRAM, YOUTUBE AND NETFLIX GET TO BRIBE YOUR SENATORS TO AVOID REGULATION

GOOGLE IS RUN BY CHILD SEX PERVERTS

Google whistleblower claims tech giant's Developer Studio division has been infiltrated by 'pedophilic religious doomsday cult' Fellowship of Friends that was featured in a Spotify podcast series called 'Revelations' last year

- Kevin Lloyd, 34, was a video producer for Google Developer Studio from 2017 until he was fired in February 2021
- Lloyd in August 2021 filed a lawsuit at California Superior Court alleging that he lost his job because he questioned a 'cult' that many of his colleagues joined
- Earlier this month Lloyd wrote a Medium post about his time at Google, and his concerns about Fellowship of Friends
- Google insist that they are unaware of a person's religious beliefs during hiring; Lloyd says they know about the influence of the cult, but turn a blind eye

By [Harriet Alexander](#)

[View comments](#)

An apocalyptic 'cult' led by an eccentric misogynist accused of sexual abuse of young men has taken over a division of [Google](#), a whistleblower has claimed.

Kevin Lloyd, 34, claims that he was fired from his job as a video developer at Google last year because he began questioning the influence of the cult.

In August, Lloyd filed a discrimination case in [California](#) Superior Court, alleging he was fired for digging into Fellowship of Friends - a group based in the small Californian town of Oregon House, and whose members made up a large percentage of employees in his division.

'Plaintiff's preliminary research into Oregon House and the Fellowship of Friends described the Fellowship as a destructive cult, with a pedophilic leader who makes false prophecies about the end of the world,' the lawsuit claims.

'Plaintiff became alarmed that Google was involved with and/or financially supporting such an organization.'

Earlier this month, Lloyd wrote a lengthy description of his case on [Medium](#), and spoke to The [New York Times](#) - who corroborated many of the lawsuit's claims through interviews with eight current and former employees of the Google business unit.

•

Kevin Lloyd, 34, claims he lost his job at Google because he raised concerns about how many people within the Google Developer Studio were affiliated with Fellowship of Friends

•

Google's campus in Mountain View is 180 miles from the small town of Oregon House, population 1,250 - yet half of the people Lloyd met were from Oregon House, he said

Lloyd said he began work at Google in 2017, as part of Google Developer Studio (GDS) - the tech giant's internal production company, making adverts and video content.

He said it slowly dawned on him that many of the people he met at GDS were from the same small Californian town, 180 miles north of Google's Silicon Valley home, in Mountain View.

- [Polygamous cult leader Warren Jeffs, 66, is pictured in new... EXCLUSIVE: 'It's a cult that brainwashes kids into believing...](#)

Share this article

The town of Oregon House is home to 1,250 people, and yet Lloyd said he realized that half of the 25 people he met at GDS were from the same town.

Lloyd said he noticed that many of the outside vendors, such as caterers and entertainers at corporate events, were also from Oregon House.

In 2018, Lloyd said, he was speaking to a freelancer who was working with them that day, and was from a town near Oregon House.

Lloyd recalls the freelancer telling him: 'Oregon House isn't a town. It's a cult.'

He began investigating the freelancer's claim, and said he was shocked by what he found.

'There are online support groups for former Fellowship of Friends members to help them process the trauma endured during their membership, as well as problems that arise after leaving,' Lloyd's lawsuit states.

Fellowship of Friends, which is based in Oregon House, was founded in 1970 by Robert Earl Burton, a former school teacher in the San Francisco Bay area.

'From its inception the vision of the Fellowship was, and remains, to establish a practical spiritual organization and to make it available to anyone interested in pursuing the spiritual work of awakening,' they state on their website.

T-Mobile Instagram influencer and model Niece Waidhofer, 31, DELETED all her Instagram posts before she killed herself: Was found dead at home after welfare check

- **Renowned Instagram influencer Niece Waidhofer - who often used her platform to spread awareness on advocacy in mental health - took her own life**
- **Early last month, Waidhofer, 31 - who was single and had no kids - scrubbed her social media of nearly all her photos and videos, leaving only three posts behind**
- **Waidhofer had over 4.2million followers on Instagram, and frequently used her platform to spread awareness on advocacy in mental health**
- **The model's final post to the social media giant appears to have been a selfie in her car on March 25**
- **The other two remaining posts are of her with a dog, dancing together and of Waidhofer with an unidentified man**
- **She said in the captions the unknown man was who she 'wanted to spend the rest of my life with'**

•

Robert Earl Burton, now believed to be around 83, founded Fellowship of Friends in 1970. He has been accused in multiple lawsuits of sexual abuse

Burton, believed to be now aged in his early 80s, sought to create a center celebrating the fine arts - with opera, ballet, works of art and literature the focus.

He based his organization in Oregon House, and created a winery where his devotees worked, when not studying the arts.

Google even purchased wine, the lawsuit claims, from the Grant Marie Winery, an allegedly cult-affiliated vineyard run by a Fellowship member in Oregon House.

But critics claimed that he had sexually abused new members of his group - in particular young boys.

In 1984 a former member filed a \$2.75 million lawsuit claiming that young men who joined the organization 'had been forcefully and unlawfully sexually seduced by Burton,' according to documents obtained by [The New York Times](#).

In 1996, another former member accused Burton in a law suit of sexual misconduct with him while he was minor. Both suits were settled out of court.

Some accusers, Lloyd alleged, had been flown to the country under false pretenses and then abused.

What is Fellowship of Friends?

Founded on January 1, 1970 by San Francisco school teacher Robert Earl Burton, Fellowship of Friends is a non-profit religious organization, headquartered in Oregon House, California.

Burton based his faith system on a philosophy called the Fourth Way, founded by an Armenian philosopher and mystic, George Gurdjieff, who lived from 1866 to 1949.

Burton adopted Gurdjieff's believe that people are in a hypnotic 'waking sleep', and need to work on themselves through studying art, music and literature.

He named his 1,200-acre headquarters Apollo, and his 1,800 followers gave 10 percent of their earnings to the organization - which spent the money on art, fine wine and culture.

Critics have filed lawsuits claiming sexual abuse.

Other critics said that the group was strongly anti-women, and celebrated white European men above all.

In September, investigative journalist Jennings Brown published a six-part podcast produced for Spotify, entitled [Revelations](#).

Brown had spent three years from 2018 digging into the group, and documented allegations of sexual abuse in what he termed a 'doomsday cult'.

Lloyd said he was aghast that GDS was so strongly linked to the Fellowship, with GDS's director, Peter Lubbers, described as a longtime member of the group, who joined shortly after he moved to the U.S. from the Netherlands.

Lubbers introduced a video producer named Gabe Pannell to the Fellowship: Pannell was pictured with Burton in 2015, and described as a 'new student', The New York Times report.

Lloyd's lawsuit states: 'Mr Lubbers gained status and praise relative to the increase of money flowing to the Fellowship through his efforts at Google that put (and kept) other Fellowship members — directly or indirectly — on Google's payroll.'

Lubbers insisted faith had nothing to do with his hiring.

'My personal religious beliefs are a deeply held private matter,' Lubbers told The New York Times.

'In all my years in tech, they have never played a role in hiring. I have always performed my role by bringing in the right talent for the situation — bringing in the right vendors for the jobs.'

Pannell told the paper that those hired were brought in from 'a circle of trusted friends and families with extremely qualified backgrounds'.

Lloyd, in his Medium post - which does not name Lubbers or Pannell - said that anxiety about the Fellowship, and its reputation, sparked a panic attack, for which he was admitted to ER.

He said in his court documents that he worried events he produced 'could somehow be used to funnel money back into the Fellowship of Friends.'

Burton is seen in a 1981 photo at Oregon House. In 1984, a former member filed a \$2.75 million lawsuit claiming that young men who joined the organization 'had been forcefully and unlawfully sexually seduced by Burton,' according to documents obtained by The New York Times. The suit was settled out of court

Fired in February 2021, he has retained a lawyer who previously represented a woman at Lubbers' previous company, Kelly Services, and sued in 2008 in a similar case.

Lynn Noyes claimed that Kelly Services had failed to promote her because she was not a member of the Fellowship.

A California court awarded her \$6.5 million in damages.

'Anyone outside of the Fellowship is seen as somehow inferior and at times adversarial,' Lloyd's lawsuit says.

'Those that express serious concerns, criticism or question the group may be eventually perceived as enemies.'

Google told The New York Times that they were barred by law from inquiring about someone's religious practices during the hiring process.

'We have longstanding employee and supplier policies in place to prevent discrimination and conflicts of interest, and we take those seriously,' a Google spokeswoman, Courtenay Mencini, said in a statement.

'It's against the law to ask for the religious affiliations of those who work for us or for our suppliers, but we'll of course thoroughly look into these allegations for any irregularities or improper contracting practices.

'If we find evidence of policy violations, we will take action.'

Fellowship of Friends was approached for comment.

The Dating Apps On T-Mobile Products And Services Are Raping You

When you use a dating site or social media site across, and through, T-Mobile networks and hardware you are being used as data cattle on a privacy and ideology harvesting digital farm.

None of the sites across T-Mobile care one bit about getting you a data, or anything else, all they care about is getting your data for data harvesters, media manipulators and political propaganda parties!

Many people find that Match.com, OK Cupid and big corporate dating sites are a stain on humanity and a cancer on the internet. Match.com and big corporate dating sites are sometimes digital sex traffickers, exploiters of emotions and a data rapists. The Match.Com bosses are known to bribe politicians and lobby the FTC to keep from getting shut down.

Match.com and it's affiliates are the worst of the bunch. They need to be put out of business forever.

They needs to be sued by each member of the public that used the site. The company also needs to be sued by the FTC, The FEC, The DOJ, The FCC and various class action citizen groups. Match.com sends your most intimate and private data to political fronts, marketing companies and government spy agencies.

Match.com, and it's corporate clone sites, are corporate political honey-traps designed to harvest your data, emotions, psychological and political profiles at your expense. You are being raped when you use Match.com.

This book details the 100% legal spy agency tactics and legal tools to put evil Match.com out of business. If you care about doing good, then you want to undertake these efforts to exterminate Match.Com.

Match.com does not care about you, your social life or your personal needs. They care about spying on you for their political and corporate bosses. They know you are addicted to sex and social connection.

They exploit those universal emotional needs for profit and social manipulation.

This book goes beyond "who pays for the meal", and delves into the sinister political and social crime base that Match.com covertly exploits around the globe. You have to really want to know why U.S. Senators are involved in sex sites:

(<https://madworldnews.com/pelosi-child-prostitution-ring/>)

(<https://www.americanpatriotdaily.com/latest/nancy-pelosi-major-scandal/>)

(<http://redwhiteandright.com/skeleton-pelosis-closet-liberals/>)

and why so many name brand

politicians have been outed in sex site leaks:

(https://en.wikipedia.org/wiki/Ashley_Madison_data_breach)

(<https://medium.com/lifes-funny/my-match-com-account-was-hacked-782560c2fcf7>)

(<https://www.washingtonpost.com/news/the-intersect/wp/2015/10/19/we-are-frequently-under-attack-match-com-says-hackers-are-after-its-data/>)

Within minutes of your use of their dating site, a political and psychological profile has been created about you and is being used by some of the most nefarious corporate, political and government entities.

Every word, every text message, every mouse click, every mouse direction, all of your audio and video...everything.. is being harvested to harm you on Match.com. Every image you post on Match.com is harvested by many parties and cross checked across the internet to find all of your other social media sites, bank records, medical records, traffic camera shots and other things you don't want the world to see.

Match.com's dating corporation knows that you are trapped. Those corporations have no souls. They see you as data cows to be harvested for government agencies, political parties, competitor research and marketing manipulation. Any picture you upload on Match is instantly cross checked across face scan databases globally, using the same software that the FBI, CIA, DEA, IRS and NSA use. By joining Match, you just said "Here I Am" to every investigator, hacker, collection agency, marketing service and enemy you could ever want to avoid.

Today, a single one of your images on Match.com is being scanned by software called "ClearView ai", "Yandex Image tracker", "Google Image Bot" and the Chinese secret police. Within 10 minutes of capturing your image off of that dating site, their computers assemble every bank record, medical record, lawsuit, property ownership record, complaint about you and every other dirty detail about you that you never wanted made public.

It is not just big spy-guys that scan your Match.com profile; Any 14 year old with a notebook computer can do this. In this book, you will see details of thousands of such technologies, in use today, that can end your life and social standing tomorrow.

This is the information they never told you in main stream news. This is how to protect yourself from Match.com.

As proven by scientific statistics, a majority of the "people" you will encounter on Match.com dating sites are: 1.) Russian scammers, 2.) Guys pretending to be girls, 3.) Robotic software seeking to scam you, 4.) Narcissists, who will never meet you in-person, seeking self-validation, 5.) Sex workers, 6.) Gold diggers, 7.) Free dinner seekers, 8.) Recently broken-up people who are addicted to their past partner and will, eventually, go back to them, 9.) Oxytocin brain chemical junkies, 10.) Single parents looking for a new person to pay the mortgage, 11.) Trans-sexuals trying out their look to see if they can fool you, 12.) Marathon daters going out with a different person every night to see which one can buy them the best dinners and show tickets and other non-qualified subjects.

This collaboratively edited book was created by the public to educate the rest of the public. It will horrify you, shock you, amaze you, enlighten you and clearly illuminate the fact that Match.com is truly breaking all of the rules of morality.

Most people that sign up for Match.com, or it's clone online dating sites, cancel it within a few weeks because of the trauma of trying to wade through the terrible things that happen to users of the system.

Every Match.com online dater is looking for: marriage, sex, free food, money, social revenge, distraction, entertainment, narcissistic validation, arm-candy, friends, a baby-daddy or related goals.

The cell phone corporations, though, behind Match.com, OK Cuid, etc. are only looking for one thing: YOUR digital and political data.

Cell Phone Companies Vast Relationships With The “Google Cartel” Are Criminal Conspiracies

T-Mobile’s PR office cry of: *“We are not Google..”* is a lie. T-Mobile IS Google because T-Mobile sends the Google crap to every citizen and sends every citizen’s private experience information back to Google and hundreds of other dark characters.

T-Mobile does it for PROFIT in spite of the fact that all the evidence shows that it causes HARM!

GOOGLE'S COMPUTERS WILL KILL YOU IF YOU TRY TO SHUT THEM OFF:

<https://www.dailymail.co.uk/news/article-10907853/Google-engineer-claims-new-AI-robot-FEELINGS-Blake-Lemoine-says-LaMDA-device-sentient.html>

[Is GOOGLE worthless tech hype?](#)

[Google will pay \\$118M to settle gender discrimination lawsuit with more than 15,000 female staff after paying them \\$17,000 less than men in similar roles](#)

[DOJ Antitrust Honchos Draw Millions From GOOGLE-Backed Groups...](#)

SEE THE TRUTH ABOUT GOOGLE: <https://www.youtube.com/watch?v=haaxr3Z8MJs&feature=em-uploademail>

“Google is a sick corrupt criminal business run by sex trafficking perverts and sociopaths...” Say GOOGLE'S own inside employees, Divorce Court records of Google executives, 70+ State & Federal investigations and major news outlets.

- Google spies on competitors and steals their technology
- Google - Alphabet - YouTube stock is owned by almost all of the California politicians and their families and that is why Google - Alphabet - YouTube is never regulated and always protected by them for their political and profiteering manipulations
- Google runs tens of millions of dollars of defamation attacks against competitors
- Google hides all media and news coverage for competitors of Larry Page's boyfriend: Elon Musk
- Google lies to the public about what they really do with the public's data
- Google promotes illegal immigration in order to get cheap labor and control votes
- Google runs VC funding back-lists against start-ups that are competitive
- Google bribes thousands of politicians
- Google is a criminal RICO-violating monopoly

- Google rigs the stock market with Flash-boy, Pump/Dump and Microblast SEC violating computer tricks
- Google pays bribes to politicians in Google and YouTube stock
- Google manipulates who gets to see what web-sites, globally, for competitor black-lists
- Google has a "no poaching" Silicon Valley jobs blacklist
- Google bosses sexually abuse women and young boys
- Google bosses run sex trafficking operations in the Epstein and NXVIUM cults
- Google bosses control the NVCA financing cartel over start-ups
- Google has placed the majority of the corporate staff in at least one White House
- Google controls national elections for anti-competitive purposes
- The company "*Polyhop*", in the HOUSE OF CARDS tv show, does all the crimes that Google actually does in reality
- Google's law firms, like Wilson Sonsini, are corrupt conduits for payola and political conduit-relays
- Google bribes some politicians with revolving door jobs
- Google is primarily responsible for destroying the Bay Area Housing opportunities
- Google runs DDoS attacks on competitors by massively crawling their sites
- Google boss Andy Rubin runs a sex slave farm according to his own family
- Google boss Eric Schmidt was a philandering sex-penthouse owner according to vast news articles
- Google executives hire so many hookers that one of them, Mr. Hayes, was killed by his hooker
- Google executives sexually abuse so many women that the women staff of Google walked out one day
- In the 2009 White House, you could not swing a cat without hitting a Google insider
- Google has paid covert bribes, PAC funds, real estate and search rigging payola to every CA Senator
- Google has paid bribes, through its lobby fronts, to halt FBI, SEC, FEC and FTC investigations of Google crimes
- Google was funded by the CIA, via In-Q-Tel, a so called "501 c3 charity" which was caught with tons of cocaine
- Google gets millions of dollars of taxpayer cash for spying on Americans inside the USA
- Google's map service was a spy system paid for by taxpayers money that Google now profits off of
- Nancy Pelosi and Dianne Feinstein have promised to "protect" Google because their families profit off Google stocks
- Payment receipts prove that Google and Gawker/Gizmodo exchanged cash and staff for Character Assassination attacks
- Google VC's and bosses have spent \$30M+ rigging the U.S. Patent Office to protect Google and harm Google competitors
- Google bribed it's lawyer into position as head of the U.S. Patent office in order to have her protect Google
- To rig insider stock trades, Google hides negative Tesla stories and pumps positive Tesla stories on "push days"
- Google and Elon Musk Co-own, co-invest and co-market stocks covertly while running anti-trust schemes
- Google rarely likes, or hires, black employees per federal and news media investigations
- Google hired most of the Washington, DC K Street lobby firms and told them to "do what ever they could"

- The film: "[Miss Sloane](#)" depicts only 2% of the illicit lobbying tactics Google employs daily
- Demands for an FTC and FBI raid of Google, for criminal activity, securities law and election felonies have been filed
- Google's David Drummond had his Woodside, CA Quail Road house bugged revealing sex and financial misdeeds

Google, and its Cartel (Alphabet, Youtube, and hundreds of other shell-company facades) are a criminal organization engaged in felony-class crimes. Google's bosses bribe politicians, regulators and law enforcement officials to hold off prosecution.

At Google: Kent Walker, Andy Rubin, Larry Page, Eric Schmidt, Sergey Brin, Jared Cohen, Yasmin Green, David Drummond and Ian Fette are so enmeshed in sex scandals, election manipulation, and White House bribes that it is hard to comprehend how they can get any legitimate work done.

Between all of the sex cult activity; hookers; rent boys; political bribes to Pelosi, Harris, Newson, and Feinstein; DDoS attacks they run; CIA and NSA stealth deals; privacy harvesting; Scientology-like employee indoctrination; cheap Asian labor; covert Axiom scams and other illicit things they get up to; one just has to wonder.

Some of the largest political bribes in American or European history were paid via billions of dollars of pre-IPO cleantech stock, insider trading, real estate, Google search engine rigging and shadow-banning, sex workers, revolving door jobs, nepotism, state-supported black-listing of competitors and under-the-table cash. Why are these Silicon Valley Oligarchs and their K-Street law firms and lobbyists immune from the law?

U.S. Senators, Agency Heads and Congress are bribed by Google intermediaries with: Billions of dollars of Google, Twitter, Facebook, Tesla, Netflix and Sony Pictures stock and stock warrants which is never reported to the FEC; Billions of dollars of Google, Twitter, Facebook, Tesla, Netflix and Sony Pictures search engine rigging and shadow-banning which is never reported to the FEC; Free rent; Male and female prostitutes; Cars; Dinners; Party Financing; Sports Event Tickets; Political campaign printing and mailing services "Donations"; Secret PAC Financing; Jobs in Corporations in Silicon Valley For The Family Members of Those Who Take Bribes And Those Who Take Bribes; "Consulting" contracts from McKinsey as fronted pay-off gigs; Overpriced "Speaking Engagements" which are really just pay-offs conducted for donors; Private jet rides and use of Government fuel depots (ie: Google handed out NASA jet fuel to staff); Real Estate; Fake mortgages; The use of Cayman, Boca Des Tores, Swiss and related money-laundering accounts; The use of HSBC, Wells Fargo, Goldman Sachs and Deutsche Bank money laundering accounts and covert stock accounts; Free spam and bulk mailing services owned by Silicon Valley corporations; Use of high tech law firms such as Perkins Coie, Wilson Sonsini, MoFo, Covington & Burling, etc. to conduit bribes to officials; and other means now documented by us, The FBI, the FTC, The SEC, The FEC and journalists.

Google and Youtube are based on technology and business models that Google and YouTube stole from small inventors who had launched other companies that were up and operating before YouTube or Google even existed as business operations.

Google holds the record for the largest number of corporate sex scandals, abuses and sex trafficking charges.

There are only two kinds of people that work at Google: 1.) Cult indoctrinated naive kids with odd sexual quirks and 2.) divisive managers and executives who seek to exploit those eco-chambered employees for nefarious political and stock market manipulation purposes under the Scientology-like guise of "doing good things", when, in fact, they are engaged in horrific crimes against society.

Google has hired almost every technology law firm in order to "conflict them out" from ever working to sue Google. If Google rapes you, robs your patents or does anything awful, you won't be able to find a lawyer to help you.

Most Google executives in control of Google have been indoctrinated by family dynasties to believe that any crime is justified by a bigger cause. Most of those executives are men. The few women in control of departments are figure-heads.

Google bosses attend the same parties and business meetings in which they collude, co-lobby, rig markets and make anti-trust violating plans together.

Google is a private government with more money and power than most smaller nations. Google has more lobbyists bribing more politicians than any other company in America.

Jared Cohen and fashion show-horse Yasmin Green at Google had the job of over-throwing countries in the Middle East. They openly bragged about it. (<https://truthstreammedia.com/2013/06/02/googles-regime-change-agent-jared-cohen/>)

People that work at Google get paid \$260,000.00+ per year to lie, spy, manipulate politics, bribe politicians and engage in other crimes. For that kind of money, a person will do ANYTHING and rationalize it as "part of the higher cause".

The Project X investigation team is publicly quoted as stating: ***"...give the same number of lawyers as Google has, with the same level of skills and experience, the same discovery budget, legal expenses budget and expert witness budget, we ABSOLUTELY GUARANTEE that we can put Google staff and investors in federal prison and close Google, in bankruptcy...the Google Cartel has engaged in that much criminal activity..."***

"Google is the largest financier of the Obama political campaign and exceeded FEC campaign spending limits by tens of billions of dollars. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing.

Google is the largest staffing source of the Obama Administration. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing.

The largest number of laws and policy decisions, benefiting a single company and its investors, went to: Google. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing.

Google, and its investor's are the single largest beneficiary of the Obama Administration. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing.

The Obama Administration only won the White House because Google and Facebook engaged in the largest digital media and search engine manipulation in human history. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing.

Google, and its investors, during the Obama Administration, had most of their competitors denied funding, grants, contracts and tax waivers while Google's investors GOT funding. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing and prove that Google coordinated anti-trust violations with senior Obama Administration White House staff...."

Google operates its staffing like a Scientology cult. They control their employees' lives, information, transportation, free time, entertainment and social life. A Google life is a glass-bubble of echo-chamber extremist, hyper-sex-kink, reinforcement.

[AAA ASSHOLES OF GOOGLE - Schmidt new investment firm deepens ties to military...](#)

[Google Deletes Videos Accusing It of Election Manipulation from YouTube... Which It Owns \(thefreethoughtproject.com\)](#)

[With All These Big Tech Revelations, This Proves The 2018 Midterms Were Stolen. Devastating Project Veritas report sheds light on Google's collusion with Democrats. \(archive.fo\)](#)

[GOOGLE EXEC'S PANIC! Go Into Hiding - Delete Social Media Accounts After James O'Keefe's Latest Exposé \(thegatewaypundit.com\)](#)

[White House Slams Google As Veritas Censorship Controversy Escalates \(bitchute.com\)](#)

[Google's NSA Again Exposed For Unauthorized Collection Of Americans' Phone Records \(zerohedge.com\)](#)

[What exactly is google's business model besides selling ads no one clicks on and selling people's data to the NSA? \(AskVoat\)](#)

[So the "russian hackers" meddling in the election was Google all along. Why isn't this the biggest story in America right now? None of the "trusted" news sources have commented on this at all. \(politics\)](#)

[Google stealthily infuses political agenda into products to prevent Trump reelection, insiders, documents say. \(theepochtimes.com\)](#)

[Google Chrome is Tracking Your Every Move and Storing It, This is How to Stop It \(thefreethoughtproject.com\)](#)

[Google Chrome Has Become Surveillance Software, It's Time to Switch | \(archive.fo\)](#)

[Project Veritas](#) has been lifting back the veil covering big tech companies and their nefarious activities following the 2016 election. They tried to play left-leaning-but-mostly-fair before the 2016 election, believing in their hearts that Hillary Clinton would be President without their concerted meddling. That didn't work out for them, so they are trying to prevent "another Trump situation" in 2020 by unabashedly [purging, silencing, and censoring conservatives](#) on platforms like Facebook, Google, Twitter, Pinterest, Instagram, and YouTube.

(Article by Michio Hasai republished from NOQReport.com)

The answers delivered today before Congress in response to questions by [Representative Dan Crenshaw](#) weren't the standard denials. They were politically manipulative answers designed to make it known they're doing what we've said they were doing all along, but they feel justified in doing it because "hate speech" must be stopped at all costs. Of course, what constitutes hate speech to the social justice warriors in big tech invariably circles around conservative thought. There is no form of hate speech short of physical threats that can be attributed to progressives, at least not in the minds of the people who control big tech. If conservatives are aggressive, they're delivering hate speech. If progressives are aggressive, they're just being truthful. That's what big tech thinks.

This is the worst-case scenario for conservatives. Before, we could call them liars and cheats. Now, we have to fight them on an ideological level, and while we have the truth on our side, they have the technology. They have the eyeballs. They control what people see and don't see. And as such, they can no longer be trusted to deliver anything even remotely close to fair and balanced. They're unhinged from reality, but instead of coming back to reality once exposed, they're building a new reality around their ideologies.

Russia may arrest Google employees for running Google as a manipulative service containing hidden political insertions affecting the human subconscious

- Russian government will now arrest those who try to 'control minds' via mass web manipulation
- Google was created to push liberal leftist political messages on the subconscious
- **Research exposes Google as insidious mind-control political shill**
- No matter your political persuasion, it is unfair and manipulative for Google to control minds ANY political purposes

By [Sophie Tanno](#)

[View comments](#)

A Russian journalist has been accused of 'controlling minds' and 'affecting the human subconscious' after referencing George Orwell's 1984 in an article.

Mikhail Romanov, a reporter for the Yakutsk Vecherniy weekly, was writing a story on the alleged torture of an academic.

Police in [Russia](#)'s republic of Sakha charged Romanov after they suspected him of trying to tap into the readers' sub-conscience, Russian newspaper [Kommersant](#) reported.

A Russian journalist has been accused of 'controlling minds' and 'affecting the human subconscious' after referencing George Orwell's 1984 (pictured) in an article

Romanov's editor told the publication: 'This is a story about how anyone can be squashed by the government machine.

'It's also about how Big Brother is watching, reading all comments on online forums.'

This is understood to be the first time a journalist will be tried under Russia's new legislation punishing those who are perceived to have published information 'containing hidden insertions affecting the human subconscious. '

The case has been forwarded to a Yakutsk city court.

[2020 Election: Subliminal Google Messages to Alter Outcome ...](#)

 <https://www.youtube.com/watch?v=LBmByyFkRlo>

Google, Facebook, Amazon, Microsoft, and Apple: these companies, the big 5, know almost everything about your life. They know what websites you go to, what y...

[MSNBC segment on Hidden and Subliminal Messages Found In ...](#)

 <https://www.videonet111.com/video/msnbc-segment-on-hidden-and-subliminal-messages-found-in-google-1>

The **Google** empire has paid more **political** bribes to politicians around the globe than any other company on Earth. ... MSNBC segment on Hidden and **Subliminal Messages** ...

[2020 Election: Subliminal Google Messages to Alter Outcome?](#)

 <https://www.zachdrewshow.com/episodes/2020-election-subliminal-google-messages-to-alter-outcome/>

Google manipulates your searches for you to be subconsciously swayed — let that sink in. We are dealing with that today. 2020 Election: Who Decides? **Google** meddling with the 2020 election? We will cover it, but also go back in history and explain that this is NOT a new development. Manipulation, deception: It starts often as **subliminal**.

[Subliminal Messaging | Owlcation](#)

 <https://owlcation.com/social-sciences/Subliminal-Messaging>


Subliminal messages are perceived by the unconscious brain. There is not as much **subliminal** messaging happening in the US now as previously reported, but there could be subtle **messages** that are received unconsciously. Messaging has probably been used by or **political** operatives, yet it may not work.

[7 Sneaky Subliminal Messages Hidden in Ads | Mental Floss](#)

 mentalfloss.com/article/67223/7-sneaky-subliminal-messages-hidden-ads

The FCC fielded the incident, and subsequently condemned such tactics as being "contrary to the public interest"; it's believed to be the first example of **subliminal** advertising on television.

[17 Subliminal Messages You'd Never Notice in Everyday Life ...](#)

 https://www.cracked.com/photoplasty_386_17-subliminal-messages-you-d-never-notice-in-everyday-life/

17 **Subliminal Messages** You'd Never Notice in Everyday Life ... Twitter. **Google** Plus. Stumble Upon. ... We asked you to show us your inner-Banksy by adding **subliminal** ...

[11 Shocking Messages Hidden In Your Childhood Cartoons](#)

 <https://www.therichest.com/expensive-lifestyle/entertainment/11-shocking-messages-hidden-in-your-childhood-cartoons/>

11 Shocking **Messages** Hidden In Your Childhood Cartoons. The creative animators and screenwriters often insert **subliminal messages** into their work, and the examples can sometimes be more than unusual. Sexism, **political messages**, conspiracy theories and hidden inappropriate jokes are found in numerous cartoons that we all grew up with.

[What Are Subliminal Messages And Do They Work?](#)

 <https://allthatsinteresting.com/what-are-subliminal-messages>

Subliminal messages, on the other hand, are likewise real and similar to supraliminal **messages** except that the signal or stimulus is below our threshold of conscious awareness. In other words, you cannot consciously perceive a **subliminal message**, even if you search for it.

Google likely 'thoroughly infiltrated' by Chinese govt., expert warns

[alex stamos](#), [big tech](#), [china](#), [cybersecurity](#), [facebook](#), [google](#), [internet](#), [peter thiel](#), [richard clarke](#), [russia](#)

([LifeSiteNews](#)) – Tech billionaire Peter Thiel recently called on the federal government to investigate Google for potential infiltration by the Chinese government, and now security experts are saying his concerns are well-founded.

Thiel, one of President Donald Trump's most high-profile [gay supporters](#) and an [avowed critic](#) of Silicon Valley, made the remarks at last weekend's National Conservatism Conference, *Axios* [reports](#). He called on the FBI and CIA to ask Google, "how many foreign intelligence agencies have infiltrated your Manhattan Project for AI"; "does Google's senior management consider itself to have been thoroughly infiltrated by Chinese intelligence"; and whether this alleged infiltration is why the company works with China's military but not America's.

"I'm not sure quite how to put this, I would like them to be asked [these questions] in a not excessively gentle manner," Thiel added.

Alex Stamos, a researcher with the Stanford Internet Observatory and [former chief security officer at Facebook](#), said Tuesday it was "completely reasonable" to assume that both the Chinese and Russian governments have, in some form or another, already infiltrated not only Google but every top tech company:

Note that "subverted" is very different than planting professional spies in "The Americans" style. Each of the big companies employs thousands of employees with family members under the control of these countries, and a gov request might be simple and seem borderline reasonable.

— Alex Stamos (@alexstamos) [July 16, 2019](#)

I expect that there will be a major combined HUMINT/InfoSec attack against a major tech company revealed in the next couple of years, which will trigger the same awakening that Project Aurora did in 2009.

— Alex Stamos (@alexstamos) [July 16, 2019](#)

BTW, I don't blame the foreign-born employees at all. They are just trying to make a good living doing interesting work. If MSS had *my* Mom I would do whatever they asked.

— Alex Stamos (@alexstamos) [July 16, 2019](#)

Stamos predicted that the “next couple of years” would see the revelation of a “major combined HUMINT/InfoSec [human intelligence/information security] attack against a major tech company.”

He's not the only one who advises that Thiel's warnings be taken seriously. Richard Clarke, a former counterterrorism and cybersecurity advisor to both Democrat and Republican presidents, [told CNBC](#) Wednesday there was cause for concern.

“Here's what I think is true: Google refused to work for the Pentagon on artificial intelligence,” Clarke said. “If you turn around and you work on artificial intelligence in China, and you don't really know what they're going to do with that, I think there's an issue.”

The internet giant has denied working with the Chinese military, but opened an artificial intelligence center in Shanghai in 2017 despite the Communist regime's strict speech and internet controls. On Tuesday, Google executive Karan Bhatia [testified](#) to the Senate Judiciary Committee that the company has terminated a [controversial](#) censored search engine it had been working on for China.

Clarke added that there was no meaningful distinction between Google working with Chinese companies and the Chinese government, given the level of state control in the country. The specter of foreign influence on the tech industry further intensifies its ongoing controversies regarding [political bias and censorship](#) and [violations of user privacy](#). Responding to Thiel's original comments, President Trump [said Tuesday](#) that his administration will “take a look” at the matter.

Google being biased is glaringly obvious even to a retard. Google forcing their employees to support them politically is a human rights violation.

Th old railroad barons a hundred years ago were bad people, but no where near as abusive as google is to the employees. The old railroad tycoons had their supporters too who thought strikers and protesters against their tyranny were awful people.

Silicon Valley just indoctrinated their followers and employees by brainwashing them first like any cult does. "Do no evil" was always a smarmy block of shit in pixels, no different than the purple dinosaur singing "I love you, you love me". The purple dinosaur never loved you one little bit. It was a lie, and parents had no business being such gullible suckers and allowing their children to be lied to by an actor in a fuzzy suit.

- [link](#)

forcing their employees to support them politically is a human rights violation.

>Civil and political rights are a class of rights that **protect individuals' freedom** from infringement by governments, social organizations, and private individuals. They ensure one's **entitlement to participate** in the **civil and political** life of the society and state **without discrimination or repression**.

From the first time they censored, shadow-banned people who opposed their way of viewing world, far-left, SJW, leftards has put cornerstone to **civil rights movement 2.0**, including people who are at the rock bottom and uppermost stairs of oppression. Clearly, this is infringement of rights by gov and private entities, which has been ignored from by the time it was apparent that such violation is well spread and not a unique case.

Those at silicon valley had no idea that their attempt to have conservative and alike voice removed/deplatformed is **someway resemble how "white" and "colored" segregation works**; which is no brainer considering that they did not pay any attention to "obscure" details and only remember famous persons who was oppressed at that time.

So, don't spout only "Hate speech is Free speech". Tell them that when some peers mock center-right personalities by reenacting what happened prior to Civil Rights Act of 1968, throwing liquids to nigger who ignored the sign, isn't a good joke since **political affiliation is covered in protected class** in District of Columbia, IA, WV state, which put them as the white fellas and anyone who didn't entirely agree with them as the blacks in this reenactment.

If anyone reading this is somehow connected to parliament from local council to state, **consider amending the laws to add political affiliation as one of class covered by "(unfounded)hate crimes"**. We won't need to see bike lock attacker and his copycat got sweetheart deals. Share this to Trump, since who doesn't love for shit and giggles watching leftards kvetching having cognitive dissonance episode explaining why adding another class would hurt other classes that already existed in last statue

Step 1: begin building foundational zeitgeist in pre-K through grade 12.

Step 2: con pupil into taking massive loan in order to obtain degree in advanced doctrine of zeitgeist.

Step 3: place pupil into career path to pay off massive loan.

Step 4: threaten to remove livelihood of career path if pupil questions established zeitgeist.

Regarding Google – Alphabet – Youtube and their Cartel, the issues, that the public and the news media have complained about include: producing child suicides and classroom shootings, racism, misogyny, child mental health threats, domestic spying, data harvesting, sex trafficking, election manipulation, tax evasion, Fusion GPS/Media Matters/ Black Cube hit jobs on competitors, censorship, contrived market monopolization, intellectual property theft, political bribery and many other social crimes!

-- An unusually large number of their staff have been arrested for, or charged with, sex crimes, including under-age trafficking.

---- They seem to be an organized crime entity protected by the politicians that they pay bribes to.

---- This entity is one of the largest operators of bribes to public officials. Some of those bribes include billions of dollars of, non-FEC reported, search engine rigging for the political campaigns of the very politicians who are supposed to regulate them.

---- “Google is a sick corrupt criminal business run by sex trafficking perverts and sociopaths...” Say GOOGLE’S own inside employees, Divorce Court records of Google executives, 70+ State and Federal investigations and major news outlets.

---- Google spies on competitors and steals their technology.

--- Google – Alphabet – YouTube stock is owned by almost all of the California politicians and their families and that is why Google – Alphabet – YouTube is never regulated and always protected by them for their political and profiteering manipulations -

--- Google runs tens of millions of dollars of defamation attacks against competitors

---- Google hides all media and news coverage for competitors of Larry Page’s boyfriend: Elon Musk

---- Google lies to the public about what they really do with the public’s data

---- Google promotes illegal immigration in order to get cheap labor and control votes

---- Google runs VC funding back-lists against start-ups that are competitive

---- Google bribes thousands of politicians

---- Google is a criminal RICO-violating monopoly – Google rigs the stock market with Flash-boy, Pump/Dump and Microblast SEC violating computer tricks -

- Google pays bribes to politicians in Google and YouTube stock
- Google manipulates who gets to see what web-sites, globally, for competitor black-lists
- Google has a “no poaching” Silicon Valley jobs blacklist
- Google bosses sexually abuse women and young boys ---- Google bosses run sex trafficking operations in the Epstein and NXVIUM cults
- Google bosses control the NVCA financing cartel over start-ups -
- Google has placed the majority of the corporate staff in at least one White House
- Google controls national elections for anti-competitive purposes
- The company “Polyhop“, in the HOUSE OF CARDS tv show, does all the crimes that Google actually does in reality
- Google’s law firms, like Wilson Sonsini, are corrupt conduits for payola and political conduit-relays
- Google bribes some politicians with revolving door jobs
- Google is primarily responsible for destroying the Bay Area Housing opportunities
- Google runs DDoS attacks on competitors by massively crawling their sites
- Google boss Andy Rubin runs a sex slave farm according to his own family -
- Google boss Eric Schmidt was a philandering sex-penthouse owner according to vast news articles

- Google executives hire so many hookers that one of them, Mr. Hayes, was killed by his hooker
- Google executives sexually abuse so many women that the women staff of Google walked out one day
- In the 2009 White House, you could not swing a cat without hitting a Google insider
- Google has paid covert bribes, PAC funds, real estate and search rigging payola to every CA Senator
- Google has paid bribes, through its lobby fronts, to halt FBI, SEC, FEC and FTC investigations of Google crimes
- Google was funded by the CIA, via In-Q-Tel, a so called “501 c3 charity” which was caught with tons of cocaine
- Google gets millions of dollars of taxpayer cash for spying on Americans inside the USA -
- Google’s map service was a spy system paid for by taxpayers money that Google now profits off of
- Nancy Pelosi and Dianne Feinstein have promised to “protect” Google because their families profit off Google stocks
- Payment receipts prove that Google and Gawker/Gizmodo exchanged cash and staff for Character Assassination attacks
- Google VC’s and bosses have spent \$30M+ rigging the U.S. Patent Office to protect Google and harm Google competitors
- Google bribed it’s lawyer into position as head of the U.S. Patent office in order to have her protect Google – To rig insider stock trades, Google hides negative Tesla stories and pumps positive Tesla stories on “push days” -

--- Google and Elon Musk Co-own, co-invest and co-market stocks covertly while running anti-trust schemes

---- Google rarely likes, or hires, black employees per federal and news media investigations

---- Google hired most of the Washington, DC K Street lobby firms and told them to “do what ever they could”

---- The film: “Miss Sloane” depicts only 2% of the illicit lobbying tactics Google employs daily

---- Demands for an FTC and FBI raid of Google, for criminal activity, securities law and election felonies have been filed

---- Google’s David Drummond had his Woodside, CA Quail Road house bugged revealing sex and financial misdeeds

---- Google, and it’s Cartel (Alphabet, Youtube, and hundreds of other shell-company facades) are a criminal organization engaged in felony-class crimes. Google’s bosses bribe politicians, regulators and law enforcement officials to hold off prosecution.

----At Google: Kent Walker, Andy Rubin, Larry Page, Eric Schmidt, Sergy Brin, Jared Cohen, Yasmin Green, David Drummond and Ian Fette are so enmeshed in sex scandals, election manipulation, and White House bribes that it is hard to comprehend how they can get any legitimate work done.

---- There are hundreds of millions of people in America. The same 120 of them are all involved in operating the same crimes and corruption including: the Sony Pictures corruption; the Afghanistan rare earth mine scandals operated through The Energy Department political slush fund that involves the lithium battery cover-ups (headed by Elon Musk); the Big Tech Brotopia rape, sex trafficking, bribery, exclusionism, racism and misogyny issues they were taught at Stanford University;

---- The Facebook – Meta – Google – Alphabet – Netflix, et al, coordinated news manipulation and domestic spying that they engage in; the hiring of Fusion GPS – Black Cube – Gizmodo/Gawker

assassins; the destruction of the housing market by their mass real estate manipulations; patent theft and industrial espionage; and the bribery of almost every politician all the way up to the Oval Office. ---- So, while the categories covered in this investigation may seem diverse.

They are connected through an enterprise of criminality and illicit, coordinated operations. We list, by name, the 120 most complicit individuals organizing these crimes, in the evidence documents already submitted to the FBI, FINCEN, DOJ, FTC, SEC, FEC, Congress, InterPol and other authorities. Digital financial tracking of those persons and all of their family members should be assumed to have been under way for some time. Wire-taps and device taps of those persons and all of their family members should be assumed to have been under way for some time. -

--- Twitter, Splunk, Google, Facebook, Netflix, YouTube and the Silicon Valley internet Cartel serve you custom manipulated content by automatically creating a covert digital dossier on you reflecting the content consumption preferences they have spied on about you. They continually evolve their dossier on you in order to steer you towards their ideology and their Democrat political party. At these companies, “data mining”, “machine learning” and “AI” means computerized propaganda processing for certain political entities. They began hiring off-shore people (because they would work so cheap) but most of those people turned out to be Muslim. This created conflicts with the entire southern part of the United States (which is anti-Muslim) because those workers steered content to pro-Muslim positions.

---- Their spy dossier on you uses abstract content-specific features of the consumed content, such as categories, topic models, and entities, which they automatically extract using natural language processing by comparing every word you use to a giant computer library of what those words might mean about your psychology. So it’s like you are getting “mind-raped” without any penis use. Their assessment of what your words might mean is based on what rich, white male, \$200K/year, DNC-promoting programmers think they might mean.

Their computers scale and expand their tools with algorithmic software created by those politically and socially biased frat white boys that wrote the code. It is all biased as hell. They never hire blacks or women in system creation roles so everything these companies do only supports rich white soyboy snowflake type gamer thinking. ---- Because their Silicon Valley VC’s told them to spy on billions of people, even for these web giants, it is impractical to store the entire dynamic history of a user’s interaction features. They, thus, out of greed, use algorithms that selectively decay information in order to generalize users and populations. To them, you are just a generalized data point, like cattle on a ranch, to be harvested and fed upon by Silicon Valley.

You can try to sue Google for anti-trust, racketeering and other illicit deeds and Google will hire tens of millions of dollars of lawyers to blockade you from getting to a Jury Trial. The best thing you can do is assist the Federal Government, many State Attorney General's and citizen's groups with their lawsuits against The Google Cartel.

Bloomberg, The Wall Street Journal, Stratfor, Wikileaks, FTC and SEC investigators and Kroll Intelligence says that Google runs the largest domestic spying operation in the world; larger than that of even Russia, China, Israel or Iran. The Google Cartel has set up thousands of companies in a spiderweb of surveillance, around the globe, and in space, that knows everything that everyone is thinking, doing or might do; and how to place media and events in front of them to subliminally steer people to do, or think, things that they might not otherwise have thought, done or voted for. Many of these operations were financed by IN-Q-TEL, which is the CIA and the NVCA combined. For example, A Google derivative called 'JigSaw' is run by Pro-Israel, Anti-Arab operatives and steers data to certain interested parties. Larry Page is on multiple Arab secret police "kill lists", which means they should terminate him if the opportunity arises. Barack Obama had Eric Schmidt in the basement of his campaign HQ on election night, running computers, and has secretly claimed that "Google put him in office". Most of the key White House staff came from Google. Google claims to 'not be political', but it is the most political business Cartel on Earth. Google finances politicians that will do what Google tells them to do. It finances them with billions of dollars of internet manipulation, insider stock favors and by getting every staff member to give max limits to their campaign PACS.

Google and it's facades: Jigsaw; Alphabet; YouTube; Google LLC (core profit maker); XXVI Holdings Inc.; Google Ireland Holdings (Google LLC subsidiary, that realizes most international profits); Alphabet Capital US LLC; Alphabet Inc. - USA - Parent holding company since 2015. If you own stocks of Google/Alphabet, you own a piece of this company; Calico Life Sciences LLC - USA - Research and development company working on keeping Eric Schmidt alive; Calico LLC (Calico Group LLC) - USA - Holding company of Calico Life Sciences LLC. Company is doing business as Calico Group LLC; Chronicle LLC - USA - Cybersecurity company that creates tools for businesses to spy on other companies; Google LLC - USA - Core Google parent company originally named Google Inc. before Google transformed itself into Alphabet. This is where most of the profits come from; Loon Holdings Inc. - USA - Holdings company - Loon LLC - USA - Company is working on providing Internet spying to rural and remote areas using high-altitude balloons; OB Technologies Inc. - USA - Holdings company - OB Technology Holdings Inc. - USA - Holding company; Waymo Holding Inc. - USA - Holding company for Waymo; Waymo LLC - USA - Company developed autonomous car technology and currently operates "testing" rides in several US states and already launched Waymo One service in Phoenix. Recently it announced that it will not make its own cars but rather focus on autonomous driving technology to spy on consumers; Wing Aviation LLC - US - Company developed drone delivering technology. It became independent from Project X in 2018. It is currently testing in Australia; X Development Holdings Inc. - USA - Holding company - X Development LLC - USA - Called "Moonshot Factory." The company says it is working on solving the world's hardest problems using technology but seems to just be an outlet for Larry Page to steal and copy technologies with. Wing, Loom, and Waymo, which are now separate businesses, started as X projects; XXVI Holdings, Inc. - USA - Layer between

Alphabet Inc. and individual companies of Alphabet. The system is designed to lower regulatory or disclosure requirements, tax evasion, money laundering and for hiding political payola. The name of the company is referring to the Roman numeral of 26, the number of letters in the alphabet.

Google LLC has over 200 direct and indirect subsidiaries in order to limit where lawsuits and federal actions can go. The Mafia uses this same approach. Almost everything Google owns is involved in acquiring, and analyzing your personal and business data for the Google surveillance computers. It is almost impossible to find a Google group that does not 'feed the data beast'. Larry Page and Eric Schmidt believe that no citizen is intelligent enough to live in the world and that they must covertly 'guide' populations to their own ideology and "Master Plan". The rest of the Google Cartel for global domination includes:

DeepMind Technologies Limited GBR Artificial intelligence/Machine Learning

DoubleClick Holding Corp.- USA - Online advertising company that Google acquired a decade ago. It recently announced that it is rebranding its advertising products, and it will no longer use DoubleClick brand.

Dropcam, Inc.- USA - Home monitoring. Company is known for its Wi-Fi video streaming cameras. Was acquired by Nest soon after Nest was acquired by Google. This acquisition is often given as an example of how an acquisition can go wrong.

Google Asia Pacific Pte. Ltd SGP Singapore company that channels revenues (royalties) from Asia/Pacific region (through the Netherlands) to Ireland Holdings Unlimited. It has a similar purpose to Google Ireland Limited in Europe.

Google Bermuda Limited BMU Hard to say, where in the company hierarchy this sits. Might be the parent company of Google Bermuda Unlimited

Google Dialer Inc.- USA - Not sure exactly but connected to Google Fiber and Google Voice.

Google Fiber Inc.- USA - Internet Access Provider

Google Fiber North America Inc.- USA - Internet Access Provider

Google International LLC - USA - Holdings company for Google's subsidiaries in individual countries outside the US.

Google Ireland Holdings Unlimited Comp. - IRL - This is a very "famous" Google subsidiary that is incorporated in Ireland but managed and controlled in Bermuda. Google at least up to recently used this subsidiary as part of the "Double Irish" with "Dutch Sandwich" tax optimization scheme that is very common among large international companies. The company serves partially as a holding company for

some international businesses but mainly as a holder of Google intellectual property that it further licensed to other Google companies for a fee.

Google Ireland Limited - IRL - Google Services Provider for Europe and Switzerland. It books a lot of revenue, but makes very small profits, since it pays a lot to Google Netherlands BV for Google's intellectual property. Google Netherlands BV then channels this revenue to Google Ireland Unlimited that is incorporated in Ireland but domiciled in Bermuda.

Google Netherlands Holdings B.V.NLD This company is used as a middle layer between Google Ireland Limited and Google Ireland Holdings. This allows Alphabet to pay very low taxes from its European operations thanks to a tax optimization scheme called "Double Irish" with "Dutch Sandwich." This loophole was very popular among international technology companies and was already fixed for new arrangements.

Google North America Inc.- USA - Provider of Google FI service (wireless network)

Google Payment Corp.- USA - Google's companies that handle money transfers and peer-to-peer transactions. In US payments are processed by Google Payment Corp. (GPC), which has the appropriate license for transmitting money and for peer-to-peer transactions in US.

Google Payment Ireland Limited - IRL - Providing Google Payment Services for whole European Union (except UK) as a replacement for

Google Payment UK. UK subsidiary will keep providing services for UK.

Google Voice Inc.- USA - Provider of Google Voice service.

GU Holdings Inc.- USA - Through this company, Google is building subsea cable infrastructure. For example, in 2019, they finished the connection between Los Angeles and Chile.

Nest Labs (Europe) Limited - IRL - "virtual subsidiary" of Nest Labs. Owned by Google Ireland Holdings Unlimited, so not directly under

Nest Labs -

Nest Labs Inc.- USA - Company flagship product and company's first offering before it was acquired by Google was Nest Learning Thermostat. Nest operated independently of Google from 2015 to 2018. However, in 2018, Nest was merged into Google's home-devices. (Still not sure if it was only organizational merger or also legal merger)

Nest Labs Singapore Pte. Ltd.SGPvirtual "subsidiary" of Nest Labs. Owned by Google Ireland Holdings Unlimited.

Verily Life Sciences LLC - USA - -Research company developing tools that focus on health data and how they can help with timely decision-making and effective interventions. (formerly Google Live Sciences)

Waze Mobile Ltd. ISRGPS navigation software. Waze describes its app as a community-driven GPS navigation app, which is free to download and use. Waze is owned directly by Google LLC.

YouTube, LLC - USA - -Youtube is a very successful video sharing and hosting service that Google acquired in 2006. This acquisition became hugely successful for Google. But not everybody was persuaded that the acquisition made sense at the time.

Alphabet Holding LLC is a holding company that is a direct subsidiary of XXVI Holdings, Inc. It is focused mainly on managing Google/Alphabet investments. Both Alphabet investment managing firms CapitalG and GV are housed under this holding. CapitalG and GV invest in other companies, but since those are usually small stakes below 50%, these companies are not part of Alphabet Group. If you want to know more about what companies do they invest in, both CapitalG and GV have a helpful list of their investments on their webpages.

CapitalG 2013 GP LLC - USA - - - Fund Manager

CapitalG 2013 LP- USA - Fund

CapitalG 2014 GP LLC - USA - - Fund Manager

CapitalG 2014 LP- USA - Fund

CapitalG 2015 GP LLC - USA - - Fund Manager

CapitalG 2015 LP- USA - Fund

CapitalG GP II LLC - USA - - Fund

CapitalG GP LLC - USA - - Fund Manager

CapitalG II LP- USA - Fund

CAPITALG INTERNATIONAL LLC - USA - -

CapitalG LP- USA - Fund

CapitalG Management Company LLC - USA - - CapitalG Core Management Company

CapitalG Rise LLC - USA - -

Google Capital 2016 GP, L.L.C.- USA - Used to be under Google Inc.

Google Capital 2016, L.P.- USA - Fund

Google Capital Management Company, L.L.C.- USA - Google Capital management company (Google Capital is an old name for CapitalG)

GV 2009 GP, L.L.C.- USA - Fund manager

GV 2009, L.P.- USA - Fund

GV 2010 GP, L.L.C.- USA - Fund manager

GV 2010, L.P.- USA - Fund

GV 2011 GP, L.L.C.- USA - Fund manager

GV 2011, L.P.- USA - Fund

GV 2012 GP, L.L.C.- USA - Fund manager

GV 2012, L.P.- USA - Fund

GV 2013 GP, L.L.C.- USA - Fund manager

GV 2013, L.P.- USA - Fund

GV 2014 GP, L.L.C.- USA - Fund manager

GV 2014, L.P.- USA - Fund

GV 2015 GP, L.L.C.- USA - Fund manager

GV 2015, L.P.- USA - Fund

GV 2016 GP, L.L.C.- USA - Fund manager

GV 2016, L.P.- USA - Fund

GV 2017 GP, L.L.C.- USA - Fund manager

GV 2017 GP, L.P.- USA - Fund manager

GV 2017, L.P.- USA - Fund

GV 2019 GP, L.L.C.- USA - Fund manager

GV 2019 GP, L.P.- USA - Fund manager

GV 2019, L.P.- USA - Fund

GV Management Company, L.L.C.- USA - Core management company for GV

GV UK Management Company LimitedGBRSmall UK based branch of “GV Management” (3 employees in 2018)

Sidewalk Labs LLC - USA - -Urban innovation organization whose goal is to improve urban infrastructure through technological solutions and tackle challenges of urban growth such as cost of living, efficient transportation, and energy - USA - ge.

Sidewalk Labs Management Company LLC - USA - -Urban innovation

Before 2015, there was no Alphabet, and Google Inc. was a publicly-traded company that you could directly own by buying its shares. All subsidiaries were subsidiaries to Google Inc. In 2015 Google transformed into Alphabet, where Alphabet Inc became the top parent company that was publicly traded. Google Inc. shareholders became overnight Alphabet Inc shareholders.

In reality, many “Other Bets” businesses still stayed as subsidiaries of Google LLC even after the 2015 transformation, and it was only recently when the whole transformation was finalized. Finally, “Other Bets” companies were moved from outside Google LLC.

The reasons for this complex transformation were described by Google management as an “increase in transparency and oversight,” That would be achieved by putting larger projects at the same level as Google LLC with their separate management, reporting directly to Alphabet Inc management. The proclaimed increase in transparency was only internal for Google management. Transparency for investors did not increase. Another reason behind the transformation was obviously limiting risk. By separating Google into different companies, each one of them is independent of each other. If someone gets arrested in one company, the others would be protected from it.

Double Irish & Dutch Sandwich is a very popular and publicized arrangement through which mostly US companies were optimizing their taxes from European businesses. It involved two Irish and one Dutch company. Wikipedia has a nice article on both Double Irish and Dutch Sandwich, explaining how it works.

In Alphabet/Google case. Companies involved in Double Irish with Dutch Sandwich arrangement are assumed to be:

Google Ireland Holding Unlimited (Irish company with Bermuda domicile)

Google Netherlands Holdings B.V. (Dutch “sandwich” company that serves as an intermediary between two Ireland companies)

Google Ireland Limited (Ireland company that is directly booking revenue from European business, and sends most of the revenue to the Netherlands as royalties for leasing Google’s intellectual property.

Aardvark- USA - Q&A service

Admeld Inc.- USA - Online advertising

AdMob, Inc.- USA - Mobile advertising

Adometry, Inc.- USA - Online advertising attribution

AdScape Media, Inc.

AdScape Media (Canada), Inc.- USA -

CANIn-game advertising

Aegino Unlimited Company - IRL - Company was mentioned in some articles as owner of several other companies operating data centers.

Agawi Inc.- USA - Mobile application streaming

Agnilux Inc.- USA - CPUs design

AIMatter OOOBLRComputer vision

Akwan Information Technologies IncBRASearch engine

allPAY GmbHDEUMobile software developer

Alooma, Inc.ISRCloud migration

Alpental Technologies, Inc.- USA - Wireless Technology

Alphabet Capital Management LLC - USA - - -

Alphabet Capital US II LLC - USA - - -

Alphabet Capital US LLC - USA - - - it was one of only four companies that Google mentioned this one as “significant” in their annual report, which means this is not just an empty shell.

Alphabet Capital, LLC - USA - -Incorporated in 2018 in Delaware, otherwise no further details about it.

Android Inc.- USA - Mobile operating system

Angstro, Inc.- USA - Social networking service

Anvato Inc.- USA - Cloud-based video services

API.AI- USA - Natural language processing

Apigee Corporation (- USA -)

Apigee Technologies (India) Private Limited (IND)

Apigee Europe Limited (GBR)

Apigee Singapore Pte Ltd (SGP)

Apigee Australia Pty Ltd (AUS)

Apigee Japan K K (JPN)

Apigee Corporation (branch) (ARE)

InsightsOne Systems, Inc. (- USA -)Vario- USA - PI management and predictive analytics

AppBridge Inc.- USA - Google Cloud migration

Appetas- USA - Restaurant website creation

Applied Semantics, Inc.- USA - Online advertising

Appurify Inc.- USA - Automated application testing

Apture, Inc.- USA - Instantaneous search

Autofuss- USA - Art and Design

BandPage, Inc.- USA - Platform for musicians

BeatThatQuote.com LimitedGBRPrice comparison service

bebop Technologies, Inc.- USA - Cloud software

Behavio- USA - Social Prediction

Beijing Gu Xiang Information Technology Co. Limited (Join Venture)CHNInternet Search (Join Venture)

Bitium, Inc.- USA - Single sign-on and identity management

Bitspin GmbHCHETimely App for Android

BlindType IncGRCTouch typing

Bot & Dolly Inc.- USA - Robotic cameras

bruNET Holding AG

bruNET GmbH

bruNET Schweiz GmbHDEU

DEU

DEUMobile software

Bump Technologies- USA - Mobile software

Bump Technologies Inc. (BumpTop)CANDesktop environment

Cask Data Inc.- USA - Big data analytics

Ceann Nua Limited - IRL - Editorial control services

Channel Intelligence, Inc.- USA - Ecommerce services

Charleston Road Registry Inc.- USA - Company serving as top level Domain registrar, since rules required

it to be a separate company from Google.

Clever Sense, Inc.- USA - Local recommendations app

Cronologics Inc.- USA - Smart watches

Cwist, Inc. (Workbench)- USA - Online learning provider

DailyDeal GmbH DEU One deal a day service

Dealmap- USA - One deal a day service

Digisfera PRT 360-degree photography

Digital Advertising and Marketing Limited (GBR)

DoubleClick Asia Ltd. (HKG)

DoubleClick Australia Pty Ltd (AUS)

DoubleClick Europe Limited (GBR)

DoubleClick Hispania SL (ESP)

DoubleClick International Asia BV (NLD)

DoubleClick International Holding LLC (- USA -)

DoubleClick International Internet Advertising Limited (- IRL -)

DoubleClick International TechSolutions Limited (- IRL -)

DoubleClick Internet Ireland Limited (- IRL -)

DoubleClick Real Property LLC (- USA -)

DoubleClick Sweden AB (SWE)

DoubleClick Technology Pte. Ltd. (SGP)

DoubleClick TechSolutions (Beijing) Co. Ltd. (CHN)

Falk eSolutions GmbH (CHE)

Falk eSolutions Ltd. (GBR)

Google Affiliate Network Inc. (- USA -)

MessageMedia Europe BV (SWE)

MessageMedia GmbH (DEU)

MessageMedia US/Europe Inc. (- USA -) Various Group of subsidiaries that are part of DoubleClick Holding

Directr Inc.- USA - Mobile video app

Divide, Inc.- USA - App splitting phone into two modes, personal & work.

dMarc Broadcasting, Inc.

Scott Concepts, LLC

Scott Studios, LLC - USA - -

- USA - Radio advertising software

DNNresearch Inc.CAN Deep Neural Networks (image recognition)

DocVerse, Inc.- USA - Microsoft Office files sharing site

DoubleClick International Asia Holding NVNLD Holding company

DrawElements OYFIN Graphics compatibility testing

eBook Technologies, Inc.- USA - E-book distribution

Emu- USA - IM client

Endoxon AG

Endoxon (Deutschland) GmbH

Endoxon (India) Private Ltd.CHE

The Deadly Cell Phone Promotions Of Facebook/Instagram Are Also Disturbing

Third party news and regulatory investigations of Facebook/Instagram, which T-Mobile sends users to, and sends user private data back and forth about, have publicly revealed the following:

Regarding Facebook/Instagram AKA 'META' or 'Meta Platforms, Inc, the issues, that the public and the news media have complained about include: producing child suicides and classroom shootings, racism, misogyny, child mental health threats, domestic spying, data harvesting, sex trafficking, election manipulation, tax evasion, Fusion GPS/Media Matters/ Black Cube hit jobs on competitors, censorship, contrived market monopolization, intellectual property theft, political bribery and many other social crimes! FACEBOOK PROFITS OFF THE CLICKS FROM SCHOOL SHOOTINGS ---- MOST OF THE BIDEN AND OBAMA STAFF OWN PARTS OF FACEBOOK!!!

Scrutinizing Sandberg's Use of Resources Over Years...

---- An unusually large number of their staff have been arrested for, or charged with, sex crimes, including under-age trafficking.

---- This entity is one of the largest operators of bribes to public officials. Some of those bribes include billions of dollars of, non-FEC reported, search engine rigging for the political campaigns of the very politicians who are supposed to regulate them.

---- Facebook-Meta engaged in the bribery of public officials.

---- Facebook-Meta is a front for actions and planning in the Obama and Biden White House.

--- Facebook-Meta is part of a criminal Big Tech Cartel.

---- Facebook-Meta is an illicit monopoly that violates anti-trust laws.

---- Facebook-Meta operates a digital news and information "protection racket".

---- Facebook-Meta attacks competitors who cannot defend themselves.

---- Facebook-Meta uses public officials to blockade competitors.

---- Facebook-Meta manipulates the stock market illegally and unethically.

---- Facebook-Meta operates like a private, unregulated, government.

---- Facebook-Meta abuses CIA, NSA and DIA resources for unjust gains.

---- Facebook-Meta uses Stazi-like mind and ideology manipulation tricks on it's site to try to get you to agree with Mark Zuckerbergs ideologies.

- Facebook-Meta investors and investment bankers conspire in a Mafia-like manner.
- Facebook-Meta steals patents and technology from others and refuses to pay for it.
- Facebook-Meta's Sandberg pretends to be the goddess of women's rights yet she is screwing the CEO of Activision, the biggest female sexual abusing company in America.
- Facebook-Meta's stock is owned by almost all of the California politicians and their families and that is why Facebook-Meta is never regulated and always protected by them for their political and profiteering manipulations.
- Facebook-Meta is Pro Israel and anti-Arab and anti-Muslim.
- Facebook-Meta's runs tens of millions of dollars of defamation attacks against competitors.
- Facebook-Meta hides all media and news coverage for competitors of Larry Page and Elon Musk.
- Facebook-Meta lies to the public about what they really do with the public's data.
- Facebook-Meta receives millions of dollars of payments from government spy agencies each month.
- Facebook-Meta promotes illegal immigration in order to get cheap labor and control votes.
- Facebook-Meta runs VC funding back-lists against start-ups that are competitive.
- Facebook-Meta bribes thousands of politicians in order to steer policy to their advantage.
- Facebook-Meta is a criminal RICO-violating monopoly.
- Facebook-Meta rigs the stock market with Flash-boy, Pump/Dump and Microblast SEC violating computer tricks.
- Facebook-Meta pays bribes to politicians in Facebook-Meta stock.
- Facebook-Meta manipulates who gets to see what web-sites, globally, for competitor black-lists.
- Facebook-Meta has a "no poaching" Silicon Valley jobs blacklist.
- Facebook-Meta bosses sexually abuse women and young boys.
- Facebook-Meta bosses run sex trafficking operations in the Epstein and NXVIUM cults.
- Facebook-Meta bosses control the NVCA financing cartel over start-ups.
- Facebook-Meta scheme to take over the VR and AR markets is based on spying on the public with VR sensors and cameras.
- Facebook-Meta controls national elections for anti-competitive purposes.
- Facebook-Meta's law firms are corrupt conduits for payola and political conduit-relays.
- David Plouffe and the Zuckerberg's were recording in meetings planning a take-over of the United States Government.
- Facebook-Meta bribes some politicians with revolving door jobs.

- Facebook-Meta is primarily responsible for destroying the Bay Area Housing opportunities.
- Facebook-Meta runs DDoS attacks on competitors by massively crawling their sites.
- Facebook-Meta has paid covert bribes, PAC funds, real estate and search rigging payola to every California Senator.
- Facebook-Meta has paid bribes, through its lobby fronts, to halt FBI, SEC, FEC and FTC investigations of Facebook-Meta crimes.
- Facebook-Meta gets millions of dollars of taxpayer cash for spying on Americans inside the USA.
- Nancy Pelosi and Dianne Feinstein have promised to “protect” Facebook-Meta because their families profit off Facebook-Meta stocks.
- Facebook-Meta VC’s and bosses have spent \$30M+ rigging the U.S. Patent Office to protect Facebook-Meta and harm Facebook-Meta competitors.
- Facebook-Meta bribed it’s lawyer into position on the board of the U.S. Patent office in order to have him protect Facebook-Meta.
- Facebook-Meta rarely likes, or hires, black employees per federal and news media investigations.
- Facebook-Meta hired most of the Washington, DC K Street lobby firms and told them to “do what ever they could” to control public policy for Zuckerberg. The film: “Miss Sloane” depicts only 2% of the illicit lobbying tactics Facebook-Meta employs daily.
- There are hundreds of millions of people in America. The same 120 of them are all involved in operating the same crimes and corruption including: the Sony Pictures corruption; the Afghanistan rare earth mine scandals operated through The Energy Department political slush fund that involves the lithium battery cover-ups (headed by Elon Musk); the Big Tech Brotopia rape, sex trafficking, bribery, exclusionism, racism and misogyny issues they were taught at Stanford University; The Facebook – Meta – Google – Alphabet – Netflix, et al, coordinated news manipulation and domestic spying that they engage in; the hiring of Fusion GPS – Black Cube – Gizmodo/Gawker assassins; the destruction of the housing market by their mass real estate manipulations; patent theft and industrial espionage; and the bribery of almost every politician all the way up to the Oval Office.
- So, while the categories covered in this investigation may seem diverse. They are connected through an enterprise of criminality and illicit, coordinated operations. We list, by name, the 120 most complicit individuals organizing these crimes, in the evidence documents already submitted to the FBI, FINCEN, DOJ, FTC, SEC, FEC, Congress, InterPol and other authorities. Digital financial tracking of those persons and all of their family members should be assumed to have been under way for some time. Wire-taps and device taps of those persons and all of their family members should be assumed to have been under way for some time.
- Twitter, Splunk, Google, Facebook, Netflix, YouTube and the Silicon Valley internet Cartel serve you custom manipulated content by automatically creating a covert digital dossier on you reflecting the content consumption preferences they have spied on about you. They continually evolve their dossier on you in

order to steer you towards their ideology and their Democrat political party. At these companies, “data mining”, “machine learning” and “AI” means computerized propaganda processing for certain political entities. They began hiring off-shore people (because they would work so cheap) but most of those people turned out to be Muslim. This created conflicts with the entire southern part of the United States (which is anti-Muslim) because those workers steered content to pro-Muslim positions.

---- Their spy dossier on you uses abstract content-specific features of the consumed content, such as categories, topic models, and entities, which they automatically extract using natural language processing by comparing every word you use to a giant computer library of what those words might mean about your psychology. So it’s like you are getting “mind-raped” without any penis use. Their assessment of what your words might mean is based on what rich, white male, \$200K/year, DNC-promoting programmers think they might mean. Their computers scale and expand their tools with algorithmic software created by those politically and socially biased frat white boys that wrote the code.

It is all biased as hell. They never hire blacks or women in system creation roles so everything these companies do only supports rich white soyboy snowflake type gamer thinking. ---- Because their Silicon Valley VC’s told them to spy on billions of people, even for these web giants, it is impractical to store the entire dynamic history of a user’s interaction features. They, thus, out of greed, use algorithms that selectively decay information in order to generalize users and populations. To them, you are just a generalized data point, like cattle on a ranch, to be harvested and fed upon by Silicon Valley.

I an online article, directed to T-Mobile, called: **“Your Phone Is Killing You And Destroying Your Life”**, By Donna Lawson, she writes:

Did you know that the electronics in your phone, AND, 99% of the ‘Apps’ on your phone are tracking you, spying on you, tricking you, and reporting to others when you:

- *Get an abortion*
- *Have sex*
- *Get pregnant*
- *Don’t go to work*
- *Enter, or leave, any building*
- *Get into, or out of, your car*
- *Have a sex worker take Uber, Lyft or any taxi or ride service to where you are*
- *Receive money*
- *Buy anything*
- *Are depressed*
- *Breath heavy*
- *Are located at any location on Earth*

- Move from any location on Earth to another location
- Take anything out of your wallet with a chip in it
- Vote
- Express a political opinion
- Use a dating site (Axciom and Equifax make psych profiles on you from your date data)
- Use any 'gay' code words
- Use any 'political' code words
- Speak, or listen, to anyone within 20 feet
- And thousands of other invasions of privacy...

It does these things even if you pushed the button to 'turn it off'. Most phones don't actually turn off when you think they are off because 'spies-gotta-spy'.

COVID is doing a great job of killing off all of the idiot people who grab the door-knob, bare-handed, at the post office, the Starbucks and the grocery store. COVID waits on public surfaces to kill the sheep of society.

Silicon Valley is doing a great job of killing off all the lives of the rest of the sheep who are too dumb to take the battery out of their phone. The people that walk around with a phone, or tablet, always powered on are committing digital suicide. If you buy a phone that you can't take the battery out of, you are just an idiot.

You may not want to face the truth but I can show you thousands of court records, Congressional investigations and university studies proving that every single assertion in this report is true.

Everybody in Congress knows this is all true but they do nothing because Silicon Valley is bribing almost every single one of them to do nothing. Silicon Valley's largest source of income is your privacy!

This is a digital world that T-Mobile should be ashamed of being an enabler of!

What Proof Exists To Confirm The Veracity Of These Charges

PROOF ITEM SETS #1. - Proof that T-Mobile and State and Federal employees, contractors and their Silicon Valley tech oligarchs engage in a RICO racketeering law-violating organized crime which applicant was helping to interdict and that the crime group still exists, operates and attacks Plaintiffs up to this date.

PROOF ITEM SETS # 2. - Legal precedents and industry comps proving that the minimum income and/or losses and or damages to victims per their experience, accomplishments and industry awards and prestigious letters of recommendation have a minimum quantifiable metric of value.

PROOF ITEM SETS # 3. - Proof that the political whistle-blower reprisal, vendetta, revenge attacks against Plaintiffs were so substantial and sophisticated that they could only have been undertaken by a Fortune 500 corporation working with a state-sponsored entity and that officials, at a high level had to have participated in these illegal retribution attacks on Plaintiff.

PROOF ITEM SETS # 4. - Banking records which show payments between T-Mobile, certain lobbyists, hit job services and Silicon Valley big tech cartel entities.

PROOF ITEM SETS # 5. - Proof that a state-wide/national black-list economic no-hire/no-fund list exists and that the financiers of the charged actions run that list against whistle-blowers and crime witnesses such as Plaintiffs.

PROOF ITEM SETS # 6. - Proof that T-Mobile and state and federal employees, contractors and their Silicon Valley tech oligarchs engage in a RICO racketeering law-violating organized crime which Plaintiffs was helping to interdict and that that crime group still exists, operates and attacks Plaintiffs to this date through corporate and public offices. Proof that part of these racketeering crimes involve trillions of dollars of internet markets. Personal and corporate emails for the last decade between every lobbyist and operative hired by T-Mobile employees and contractors prove the assertion.

PROOF ITEM SETS # 7. - Proof that T-Mobile was informed of massive security risks and took no action.

PROOF ITEM SETS # 8. - Proof of the severity of the crimes that public officials, influenced by T-Mobile, who were supposed to serve Plaintiffs, engaged in against Plaintiffs. The profits and benefits of Plaintiffs attackers pass through both senior federal and state agency officials and Silicon Valley tech oligarchs. proves that public officials also have liability for Plaintiffs damages by direct and indirect harm to Plaintiffs validated by forensic accounting of campaign finances, PACs, revolving door jobs and other incriminating data. Further, White House staff and Senator stock market holdings of any securities asset owned, or affected by any T-Mobile entity can be shown by the FEC, FINCEN, The SEC and the NSA records to have direct quid pro quo beneficiaries who received unjust profiteering gains as incentives for political favors. Plaintiffs have requested those agencies join this case either as witnesses and/or co-Plaintiffs on behalf of the public.

PROOF ITEM SETS # 9. - How the damages and losses against applicant are legally calculated using industry and case metrics

PROOF ITEM SETS # 10. - Conflict-of-interest data, and quid-pro-quo proofs on Defendant related parties from: - <http://www.pogo.org> - <http://www.sunlightfoundation.com> - <http://followthemoney.org> - <http://www.icij.org> - <https://freenetproject.org> - <http://www.anticorruptionparty.org> - <http://www.icij.org> - <http://www.transparency.org>

PROOF ITEM SETS # 11. - Proof that Plaintiffs were attacked by Defendant agents orders using Google/Youtube and Gawker/Gizmodo who are the partners, financiers, media outlets, staff providers, employee/contractors and federal funds beneficiaries of the U.S. Government and California Government taxpayer funded treasuries.

PROOF ITEM SETS # 12. - Proof that various Attorney General offices have incriminating investigation records on T-Mobile and requests for said records in this case.

PROOF ITEM SETS # 13. - Proof that T-Mobile knew it was providing a network to harvest consumers of their basic rights and assets without properly informing them in a manner that the average consumer could comprehend the danger of.

PROOF ITEM SETS # 14. - Proof that T-Mobile executives hired illicit persons to engage in illicit deeds including sex workers, media assassins, political operatives, DNS manipulators and 'spoofers' and other such 'dark arts' personnel.

PROOF ITEM SETS # 15. - Proof that White House staff, and candidates, had, and have direct participation. Proof that the nature of the crimes Plaintiffs are testifying about account for a reasonable validation of potential harm or death

PROOF ITEM SETS # 16. - Proof that T-Mobile lied on its taxes.

PROOF ITEM SETS # 17. - Proof that T-Mobile hired shill reporters.

PROOF ITEM SETS # 18. - Proof that every server, file and adjacent network in the T-Mobile network and on every T-Mobile network system has been hacked and can easily be manipulated, deleted and spoofed in a matter of minutes proving the ease with which attackers could have harmed Plaintiffs .

PROOF ITEM SETS # 19. - Surveillance videos produced in the T-Mobile retail stores in T-Mobile in-store security camera's, customer cell phones and customer 'pen cameras'.

PROOF ITEM SETS # 20. - Proof that the cash, profits and benefits of T-Mobile pass through both senior federal and state agency officials and Silicon Valley tech oligarchs. This proves that public officials have liability for Plaintiffs damages by direct and indirect harm to applicant validated by forensic accounting of campaign finances, PACs, revolving door jobs and other incriminating data

PROOF ITEM SETS # 21. - Proof of the degree of social toxicity common-place in the male dominated executive suites at T-Mobile via the text messages, voicemails and emails of T-Mobile officials.

PROOF ITEM SETS # 22. - Proof that the Telecommunications industry is, in part, operated by bribery.

PROOF ITEM SETS # 23.- Proof that the users of T-Mobile Assurance "Obama Phones" are spied on.

PROOF ITEM SETS # 24 - Proof that Plaintiffs were harrassed, cut-off from service, lied to and violated inside T-Mobile retail store facilities.

PROOF ITEM SETS # 25. - DATA DVD's with video evidence on them including film: **'POLITICAL CORRUPTION 101 - OPENING – MEDIUM.m4v'** and **multiple folders of evidence items**

And such additional evidence sets as shall be required in the course of this case...

Additional corroborating evidence is also posted at:

<http://www.majestic111.com>

<http://vcrocket.weebly.com>

<https://www.transparency.org>

<https://www.judicialwatch.org>
<https://wikileaks.org>
<https://causeofaction.org>
<https://fusion4freedom.com/about-gcf/>
<http://peterschweizer.com/>
<http://globalinitiative.nethttps://fusion4freedom.com/the-green-corruption-files-archive/>
<https://propublica.org>
<https://www.allsides.com/unbiased-balanced-news>
<http://wearethenewmedia.com>
http://ec.europa.eu/anti_fraud/index_en.html
<http://gopacnetwork.org/>
<http://www.iaaca.org/News/>
<http://www.interpol.int/Crime-areas/Corruption/Corruption>
<http://www.icac.nsw.gov.au/>
<http://www.traceinternational.org/>
<http://www.oge.gov/>
<https://ogc.commerce.gov/>
<https://anticorruptionact.org/>
<http://www.anticorruptionintl.org/>
<https://represent.us/>
http://www.giacentre.org/dealing_with_corruption.php
<http://www.acfe.com/>
<https://www.oas.org/juridico/english/FightCur.html>
<https://www.opus.com/international-anti-corruption-day-businesses/>
<https://www.opengovpartnership.org/theme/anti-corruption>
<https://www.ethicalsystems.org/content/corruption>
<https://sunlightfoundation.com/>
<http://www.googletransparencyproject.org/>
<http://xyzcase.weebly.com>
<https://en.wikipedia.org/wiki/Angelgate>
<https://www.opensecrets.org/>
https://en.wikipedia.org/wiki/High-Tech_Employee_Antitrust_Litigation
<http://www.projectveritasaction.com>
and a host of other transparency organizations...

T-MOBILE SECURITY ISSUES

T-Mobile has been informed, each year since 1999, that their network was not secure.

T-Mobile has issued written assurance to users that its network IS secure....according to T-Mobile marketing people.

T-Mobile was offered security technologies and architecture from third-party supplies that T-Mobile rejected because:

- 1. It was cheaper not to use the high-end systems and,**
- 2. Using better security would cut off the ability of T-Mobile to spy on consumers and to relay spy data back and forth from Silicon Valley data harvesting social media companies.**

T-Mobile was not only aware of the IT Security standard: “IF IT HAS A PLUG, IT HAS A BUG”; but the company exploited this reality for profiteering while causing the deaths and permanent mental health loss to millions of teenagers.

University, Federal, Forensic Researcher and Journalism sources provided in the links below, prove every assertion in this report many times over. A simple web-search by any college-educated person, on the top 5 search engines, can turn up hundreds of additional credible, verifying sources. Expert jury trial and Congressional hearing witnesses have proven these facts over and over.

The following security issues have been found on T-Mobile devices, Smart TV's and devices connected to the “T-Mobile Network” and computers connected to the T-Mobile Network. Additionally, T-Mobile's entire administrative and user network files have been targeted by international hackers in a ‘Black Hat’ contest to see who can hack T-Mobile the best.

The Russian FSB agency has been known to have a direct connection, covertly, into the T-Mobile corporate systems in Germany. Teen hackers hunt “Instagram Models” who have T-Mobile accounts via a shared info system. China pays a ‘bounty’ for keys into the T-Mobile network. When the CIA's and NSA's hacking tools were released to the public, it was found that they were, at first, tested on T-Mobile devices by spy agency programmers.

T-Mobile's failure to report these known issues to consumers and their failure to use encrypted torrent segments, each segment having a different key, as T-Mobile was advised to do in 1999, are causes for concern and class action. T-Mobile's assertions that these solutions were ‘inconvenient’ and ‘cumbersome’ should be weighed against the inconvenience of every consumer getting hacked and the cumbersome-ness of multi-billion dollar class action lawsuits.

You probably can't imagine the [second-by-second dangers](#) and harms that T-Mobile electronics, like your phone, PC and tablet are using, are causing to your life, your income, your privacy, your beliefs, your human rights, your bank account records, your political data, your job, your brand name, your medical data, your dating life, your reputation and other [crucial parts of your life](#).

Any use of a dating site, Google or Facebook product, social media site, movie site, or anything that you log in to, puts you at substantial risk. Remember: "[if it has a plug, it has a bug](#)". Every electronic device that T-Mobile sells can be easily made to spy on you in ways you cannot possibly imagine.

The Take-Aways:

- Stalkers can find you by zooming in on your pupil reflection images in your online photos (<https://www.kurzweilai.net/reflected-hidden-faces-in-photographs-revealed-in-pupil>)
- If you send email overseas or make phone calls overseas all of your communications, and those with anybody else, are NSA monitored (<https://www.privacytools.io/>)
- Bad guys take a single online photo of you and put it in software that instantly builds a dossier on you by finding where every other photo of you is that has ever been posted online (<https://www.aclu.org/blog/privacy-technology/surveillance-technologies/apples-use-face-recognition-new-iphone>)
- Face-tracking software for stalking you on Match.com and OK Cupid is more effective than even FBI software for hunting bank robbers (<https://www.cnet.com/news/clearview-app-lets-strangers-find-your-name-info-with-snap-of-a-photo-report-says/>)
- Any glass, metal or ceramic object near you can be reflecting your voice or image to digital beam scanners that can relay your voice or image anywhere in the world
- All your data from any hotel you stay at will eventually be hacked and leaked ([Info of 10 MILLION MGM guests including Justin Bieber and TWITTER CEO leaked online!](#))
- Your voting data will be used to spy on you and harm you ([Every voter in Israel just had their data leaked in 'grave' security breach...](#))
- Lip-reading software can determine what you are saying from over a mile away (<https://www.telegraph.co.uk/news/2020/01/20/russian-police-use-spy-camera-film-opposition-activist-bedroom/>)
- Every Apple iPhone and other smart-phone has over 1000 ways to bug you, listen to you, track you and record your daily activities even when you think you have turned off the device. Never leave your battery in your phone. ([LEAKED DOCS: Secretive Market For Your Web History...](#)) ([Every Search. Every Click. On Every Site...](#))
- Elon Musk's SpaceX StarLink satellites are spy satellites that send your data to Google and other tech companies (<https://www.chieftain.com/news/20200118/first-drones-now-unexplained-lights-reported-in-horsetooth>)
- Google and Facebook have all of your medical records and they are part of a political operation (<https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200>)
- Every dating site, comments section and social media site sends your private data, covertly, to

government, political campaigns and corporate analysis groups and can also be hacked by anyone.

- Any hacker can hack ANY network with even a single Intel, Cisco, Juniper Networks or AMD motherboard on it and nobody can stop them unless they destroy the motherboard because the back-doors are built into the hardware. Many of the companies you think are providing security are secretly owned by the Chinese government spy agencies or the CIA (<https://boingboing.net/2020/02/11/cia-secretly-owned-worlds-to.html>)

- Warehouses in Nigeria, Russia, Ukraine, Sao Paolo, China and hundreds of other regions, house tens of thousands of hackers who work around the clock to try to hack you and manipulate your data.

- Every red light camera, Walmart/Target/Big Box camera and every restaurant camera goes off to networks that send your activities to credit companies, collection companies, political parties and government agencies (['Homeland Security' using location data from apps to track millions of people...](#))

- Match.com, OKCupid and Plenty of Fish are also DNC voter analysis services that read your texts and keep your profiles forever

- If you don't put fake ages, addresses, phone numbers and disposable email addresses on ANY form you fill out electronically, it will haunt you forever (<https://www.the-sun.com/news/284784/pornstar-data-breach-massive-leak-bank-details/>)

- Every train, plane and cruise line records you constantly and checks the covert pictures they take of you against global databases. Corporations grab your collateral private data that those Princess Cruises and United Airlines companies take and use them to build files on you (

<https://www.silive.com/news/2020/01/report-new-app-can-id-strangers-with-a-single-photo.html>)

- The people who say "nobody would be interested in me" are the most at risk because their naiveté puts them at the top-of-the-list for targeting and harvesting (<https://www.cnet.com/news/clearview-app-lets-strangers-find-your-name-info-with-snap-of-a-photo-report-says/>)

- Silicon Valley tech companies don't care about your rights, they care about enough cash for their executives to buy hookers and private islands with. Your worst enemy is the social media CEO. They have a hundred thousand programmers trying to figure out more and more extreme ways to use your data every day and nobody to stop them

- The government can see everywhere you went to in the last year (<https://www.protocol.com/government-buying-location-data>)

There have been over 15,000 different types of hacks used against over 3 billion "average" consumers. EVERY one of them thought they were safe and that nobody would hack them because "nobody cared about them". History has proven every single one of them to have been totally wrong!

If you are smart, and you read the news, you will know that you should ditch all of your electronic devices and "data-poison" any information about you that touches a network by only putting fake info in all conceivable forms and entries on the internet. You, though, may be smart but lazy, like many, and not willing to step outside of the bubble of complacency that corporate advertising has surrounded you with.

Did you know that almost every dating and erotic site sends your most private life experiences and chat messages to Google's and Facebook's investors? <https://www.businessinsider.com/facebook-google-quietly-tracking-porn-you-watch-2019-7>

Do you really want all of those Silicon Valley oligarchs that have been charged with sexual abuse and sex trafficking to know that much about you?

Never, Ever, put your real information on Youtube, Netflix, Linkedin, Google, Twitter, Comcast, Amazon and any similar online service because it absolutely, positively will come back and harm you!

Always remember: Anybody that does not like you can open, read and take any photo, data, email or text on EVERY phone, computer, network or electronic device you have ever used no matter how "safe" you think your personal or work system is! They can do this in less than a minute. Also: Hundreds of thousands of hackers scan every device, around the clock, even if they never heard of you, and will like your stuff just for the fun of causing trouble. Never use an electronic device unless you encrypt, hide and code your material! One of the most important safety measures you can take is to review the security info at: <https://www.privacytools.io/>

Those people who think: "I have nothing to worry about..I am not important" ARE the people who get hacked the most. Don't let naivete be your downfall. (<https://www.eff.org/deeplinks/2019/07/when-will-we-get-full-truth-about-how-and-why-government-using-facial-recognition>)

All of your info on Target, Safeway, Walgreens has been hacked and read by many outsiders. NASA, The CIA, The NSA, The White House and all of the federal background check files have been hacked. The Department of Energy has been hacked hundreds of times. All of the dating sites have been hacked and their staff read all of your messages. Quest labs blood test data and sexual information reports have been hacked and published to the world. There is no database that can't be easily hacked. Every computer system with Intel, AMD, Juniper Networks, Cisco and other hardware in it can be hacked in seconds with the hardware back-doors soldered onto their electronic boards. All of the credit reporting bureaus have been hacked. Wells Fargo bank is constantly hacked. YOU ARE NOT SAFE if you put information on a network. NO NETWORK is safe! No Silicon Valley company can, or will, protect your data; mostly because they make money FROM your data!

Every single modern cell phone and digital device can be EASILY taken over by any hacker and made to spy on you, your family, your business and your friends in thousands of different ways. Taking over the microphone is only a small part of the ways a phone can be made to spy on you. Your phone can record your location, you voice vibrations, your mood, your thoughts, your sexual activity, your finances, your photos, your contacts (who it then goes off and infects) and a huge number of other things that you don't want recorded.

[Privacy watchdog under pressure to recommend facial recognition ban...](#)

[Alarming Rise of Smart Camera Networks...](#)

[AMAZON's Ring Doorbell Secretly Shares Private User Data With](#)

FACEBOOK . . .

The worst abusers of your privacy, personal information, politics and psychological information intentions are: Google, Facebook, LinkedIn, Amazon, Netflix, Comcast, AT&T, Xfinity, Match.com & the other IAC dating sites, Instagram, Uber, Wells Fargo, Twitter, Paypal, Hulu, Walmart, Target, YouTube, PG&E, The DNC, Media Matters, Axiom, and their subsidiaries. Never, ever, put accurate information about yourself on their online form. Never, ever, sign in to their sites using your real name, phone, address or anything that could be tracked back to you.

If you don't believe that every government hacks citizens in order to destroy the reputation of anyone who makes a public statement against the current party in power then read the public document at:

<https://www.cia.gov/library/readingroom/docs/CIA-RDP89-01258R000100010002-4.pdf>

That document shows you, according to the U.S. Congress, how far things can go.

A program called ACXIX hunts down all of your records from your corner pharmacy, your taxi rides, your concert tickets, your grocery purchases, what time you use energy at your home, your doctor records...and all kinds of little bits of info about you and puts that a file about you. That file about you keeps growing for the rest of your life. That file sucks in other files from other data harvesting sites like Facebook and Google: FOREVER. The information in that file is used to try to control your politics and ideology.

In recent science studies cell phones were proven to exceed radiation safety limits by as high as 11 times the 2-decade old allowable U.S. radiation limits when phones touch the body. This is one of thousands of great reasons to always remove the battery from your cell phone when you are not talking on it. A phone without a battery in it can't spy on you and send your data to your enemies.

If you are reading this notice, the following data applies to you:

1. EVERY network is known to contain Intel, Cisco, Juniper Networks, AMD, Qualcomm and other hardware which has been proven to contain back-door hard-coded access to outside parties. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.
2. Chinese, Russian FSB, Iranian and other state-sponsored hacking services as well as 14 year old domestic boys are able to easily enter your networks, emails and digital files because of this. They can enter your network at any time, with less than 4 mouse clicks, using software available to anyone. This is a proven, inarguable fact based on court records, FISA data, IT evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.
3. Your financial office is aware of these facts and has chosen not to replace all of the at-risk equipment, nor sue the manufacturers who sold your organization this at risk equipment. They believe that the hassle and cost of replacement and litigation is more effort than the finance department is willing to undertake. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts,

Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

4. In addition to the existing tools that were on the internet, in recent years, foreign hackers have released all of the key hacking software that the CIA, DIA and NSA built to hack into any device. These software tools have already been used hundreds of times. Now the entire world has access to these tools which are freely and openly posted across the web. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

5. The computers, servers, routers, cell phones, IP cameras, IP microphones, Smart Meters, Tesla's, "Smart Devices:", etc. and other devices openly broadcast their IP data and availability on the internet. In other words, many of your device broadcast a "HERE I AM" signal that can be pinged, scanned, spidered, swept or, otherwise, seen, like a signal-in-the-dark from anywhere on Earth and from satellites overhead. Your devices announce that they are available to be hacked, to hackers. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

6. It is bad policy for your organization, or any organization, to think they are immune or have IT departments that can stop these hacks. NASA, The CIA, The White House, EQUIFAX, The Department of Energy, Target, Walmart, American Express, etc. have been hacked hundreds of times. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

7. The thinking: "Well, nobody would want to hack us", or "We are not important enough to get hacked" is the most erroneous and negligent thinking one could have in the world today. Chinese, Russian and Iranian spy agencies have a global "Facebook for blackmail" and have been sucking up the data of every entity on Earth for over a decade. If the network was open, they have the data and are always looking for more. The same applies to Google and Facebook who have based their entire business around domestic spying and data re-sale. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

8. You are a "Stepping Stone" doorway to other networks and data for targeted individuals and other entities. Your networks provide routes into other people's networks. The largest political industry today is called "Doxing" and "Character Assassination". Billions of dollars are expended by companies such as IN-Q-Tel - (DNC); Gawker Media - (DNC); Jalopnik - (DNC); Gizmodo Media - (DNC); K2 Intelligence - (DNC); WikiStrat - (DNC); Podesta Group - (DNC); Fusion GPS - (DNC/GOP); Google - (DNC); YouTube - (DNC); Alphabet - (DNC); Facebook - (DNC); Twitter - (DNC); Think Progress - (DNC); Media Matters - (DNC); Black Cube - (DNC); Mossad - (DNC); Correct The Record - (DNC); Sand Line - (DNC/GOP); Blackwater - (DNC/GOP); Stratfor - (DNC/GOP); ShareBlue - (DNC); Wikileaks

(DNC/GOP); Cambridge Analytica - (DNC/GOP); Sid Blumenthal- (DNC); David Brock - (DNC); PR Firm Sunshine Sachs (DNC); Covington and Burling - (DNC), BuzzFeed - (DNC) Perkins Coie - (DNC); Wilson Sonsini - (DNC) and hundreds of others to harm others that they perceive as political, personal or competitive threats. Do not under-estimate your unintended role in helping to harm others. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

9. NEVER believe that you are too small to be noticed by hackers. Parties who believe that are the hackers favorite targets. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

10. NEVER believe that because the word "DELL" or "IBM" or "CISCO" is imprinted on the plastic cover of some equipment that you are safe. Big brands are targeted by every spy agency on Earth and are the MOST compromised types of equipment. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

11. YOU may not personally care about getting exposed but the person, or agency, you allow to get exposed will be affected for the rest of their lives and they will care very much and could sue you for destroying them via negligence. Be considerate of others in your "internet behavior". Do not put anything that could hurt another on any network, ever. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

12. Never post your real photograph online, or on a dating site social media or on any network. There are thousands of groups who scan every photo on the web and cross check those photos in their massive databases to reveal your personal information via every other location your photo is posted. These "image harvesters" can find out where you, who your friends and enemies are and where your kids are in minutes using comparative image data that they have automated and operating around the clock. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

13. If you think using web security measures like this makes you "paranoid", then think again. Cautious and intelligent people use these security measures because these dangers are proven in the news headlines daily. Uninformed, naive and low IQ people are the types of people who do not use good web hygiene and who suffer because they are not cautious and are not willing to consider the consequences of their failure to read the news and stay informed.

‘Gotham’ software written by Palantir shows how government agencies, or anybody, can use very little information to obtain quick access to anyone’s personal minutiae.

VICE NEWS *Motherboard* via public records request has [revealed](#) shocking details of capabilities of California law enforcement involved in Fusion Centers, once deemed to be a conspiracy theory like the National Security Agency (NSA) which was founded in 1952, and its existence hidden until the mid-1960s. Even more secretive is the National Reconnaissance Office (NRO), which was founded in 1960 but remained completely secret for 30 years.

Some of the documents instructing California law enforcement (Northern California Regional Intelligence Center) “Fusion Center” are now online, and they show just how much information the government can quickly access with little or no knowledge of a person of interest.

“The guide doesn’t just show how Gotham works. It also shows how police are instructed to use the software,” writes [Caroline Haskins](#).

“This guide seems to be specifically made by Palantir for the California law enforcement because it includes examples specific to California.”

According to DHS, “Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners” like Palantir. Further, Fusion Centers are locally owned and operated, arms of the “[intelligence community](#),” i.e. the 17 intelligence agencies coordinated by the [National Counterterrorism Center \(NCTC\)](#). However, sometimes the buildings are staffed by trained NSA personnel like what [happened](#) in Mexico City, according to a 2010 [Defense Department \(DOD\) memorandum](#).

Palantir is a private intelligence data management company mapping relationships between individuals and organizations alike founded by Peter Thiel and CEO Alex Karp and accused rapist Joe Lonsdale. You may remember Palantir from journalist Barrett Brown, Anonymous’ hack of HBGary, or [accusations](#) that the company provided the technology that enables NSA’s mass surveillance PRISM. Founded with early investment from the CIA and heavily used by the military, Palantir is a subcontracting company in its own right. The company has even been featured in the Senate’s grilling of Facebook, when Washington State Senator Maria Cantwell [asked](#) CEO Mark Zuckerberg, “Do you know who Palantir is?” due to Peter Thiel sitting on Facebook’s board.

In 2011, Anonymous’ breach [exposed](#) HBGary’s plan, conceived along with data intelligence firm Palantir, and Berico Technologies, to retaliate against WikiLeaks with cyber attacks and threaten the journalism institutions supporters. Following the hack and exposure of the joint plot, Palantir [attempted](#) to distance itself from HBGary, which it blamed for the plot.

Bank of America/Palintir/HBGary combined WikiLeaks attack plan. You can find more here: <https://t.co/85yECxFmZu> pic.twitter.com/huNtfJp8gl

— WikiLeaks (@wikileaks) [November 29, 2016](#)

This was in part because Palantir had in 2011 [scored \\$250 million in deals](#) ; its customers included the CIA, FBI, US Special Operations Command, Army, Marines, Air Force, LAPD and even the NYPD. So the shady contractor had its reputation to lose at the time being involved in arguably criminal activity against WikiLeaks and its supporters.

Palantir describes itself as follows based on its [website](#):

Palantir Law Enforcement supports existing case management systems, evidence management systems, arrest records, warrant data, subpoenaed data, RMS or other crime-reporting data, Computer Aided Dispatch (CAD) data, federal repositories, gang intelligence, suspicious activity reports, Automated License Plate Reader (ALPR) data, and unstructured data such as document repositories and emails.

Palantir's software, *Bloomberg reports*,

combs through disparate data sources—financial documents, airline reservations, cellphone records, social media postings—and searches for connections that human analysts might miss. It then presents the linkages in colorful, easy-to-interpret graphics that look like spider webs.

Motherboard shows how Fusion Center police can now utilize similar technology to track citizens beyond social media and online web accounts with people record searches, vehicle record searches, a Histogram tool, a Map tool, and an Object Explorer tool. (For more information on each and the applicable uses see the *Vice News* article [here](#).)

Police can then click on an individual in the chart within Gotham and see every personal detail about a target and those around them, from email addresses to bank account information, license information, social media profiles, etc., according to the documents.

Palantir's software in many ways is similar to the Prosecutor's Management Information System (PROMIS) stolen software Main Core and may be the next evolution in that code, which allegedly [predated](#) PRISM. In 2008, Salon.com [published](#) details about a top-secret government database that might have been at the heart of the Bush administration's domestic spying operations. The database known as "Main Core" reportedly collected and stored vast amounts of personal and financial data about millions of Americans in event of an emergency like Martial Law.

The only difference is, again, this technology is being allowed to be deployed by Fusion Center designated police and not just the National Security Agency. Therefore, this expands the power that Fusion Center police — consisting of local law enforcement, other local government employees, as well as Department of Homeland Security personnel — have over individual American citizens.

This is a huge leap from allowing NSA agents to access PRISM database search software or being paid by the government to [mine social media for "terrorists."](#)

Fusion Centers have become a long-standing target of civil liberties groups like the [EFF](#), [ACLU](#), and others because they collect and aggregate data from so many different public and private sources.

On a deeper level, when you combine the capabilities of Palantir's Gotham software, the [abuse](#) of the Department of Motor Vehicles (DMV) database for Federal Bureau of Investigations/Immigration and Customs Enforcement, and facial recognition technology, you have the formula for a nightmarish surveillance state. Ironically, or perhaps not, that nightmare is the reality of undocumented immigrants as Palantir is one of several companies helping sift through data for the raids planned by ICE, [according](#) to journalist Barrett Brown.

YOU HAVE BEEN WARNED:

According to the world's top internet security experts: "...Welcome to the new digital world. Nobody can ever type anything on the internet without getting scanned, hacked, privacy abused, data harvested for some political campaign, spied on by the NSA and Russian hackers and sold to marketing companies. You can't find a corporate or email server that has not already been hacked. For \$5000.00, on the Dark Web, you can now buy a copy of any person's entire dating files from match.com, their social security records and their federal back-ground checks. These holes can never be patched because they exist right in the hardware of 90% of the internet hardware on Earth. Any hacker only needs to find one hole in a network in order to steal everything in your medical records, your Macy's account, your credit records and your dating data. Be aware, these days, Mr. & Ms. Consumer. Facebook, Google, Twitter and Amazon have turned out to be not-what-they-seem. They manipulate you and your personal information in quite illicit manners and for corrupt purposes. Avoid communicating with anybody on the internet because you will never know who you are really talking to. Only communication with people live and in-person..."

SPREAD THE WORD. TELL YOUR FRIENDS. COPY AND PASTE THIS TO YOUR SOCIAL MEDIA. SEE MORE PROOF IN THESE ARTICLES:

<https://www.i-programmer.info/news/149-security/12556-google-says-spectre-and-meltdown-are-too-difficult-to-fix.html>

<https://sputniknews.com/us/201902231072681117-encryption-keys-dark-overlord-911-hack/>

<https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2>

<https://thehill.com/policy/technology/430779-google-says-hidden-microphone-was-never-intended-to-be-a-secret>

<https://www.blacklistednews.com/article/71200/smartphone-apps-sending-intensely-personal-information-to-facebook--whether-or-not-you-have-an.html>

<https://www.bleepingcomputer.com/news/security/microsoft-edge-secret-whitelist-allows-facebook-to-autorun-flash/>

<https://news.ycombinator.com/item?id=19210727>

<https://www.davidicke.com/article/469484/israel-hardware-backdoored-everything>

<https://www.scmp.com/economy/china-economy/article/2186606/chinas-social-credit-system-shows-its-teeth-banning-millions>

<https://youtu.be/lwoyesA-vlM>

<https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-popular-password-managers/>

<https://files.catbox.moe/jopll0.pdf>

<https://files.catbox.moe/ugqngv.pdf>

<https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/>

<https://arstechnica.com/tech-policy/2019/02/att-t-mobile-sprint-reportedly-broke-us-law-by-selling-911-location-data/>

<https://theintercept.com/2019/02/08/jeff-bezos-protests-the-invasion-of-his-privacy-as-amazon-builds-a-sprawling-surveillance-state-for-everyone-else/>

<https://www.blacklistednews.com/article/71200/smartphone-apps-sending-intensely-personal-information-to-facebook--whether-or-not-you-have-an.html>

<https://www.stripes.com/news/us/feds-share-watch-list-with-1-400-private-groups-1.569308>

<https://voat.co/v/news/3053329>

<https://www.zdnet.com/article/all-intel-chips-open-to-new-spoiler-non-spectre-attack-dont-expect-a-quick-fix/>

<https://voat.co/v/technology/3075724>

https://www.theregister.co.uk/2019/02/26/malware_ibm_powershell/

<https://fossbytes.com/facebook-lets-anyone-view-your-profile-using-your-phone-number/>

<https://www.iottectrends.com/vulnerability-ring-doorbell-fixed/>

<https://voat.co/v/technology/3077896>

<https://www.mintpressnews.com/whistleblowers-say-nsa-still-spies-american-phones-hidden-program/256208/>

<https://www.wionews.com/photos/how-israel-spyware-firm-nso-operates-in-shadowy-cyber-world-218782#hit-in-mexico-218759>

<https://sg.news.yahoo.com/whatsapp-hack-latest-breach-personal-data-security-135037749.html>

<https://metro.co.uk/2019/05/14/whatsapp-security-attack-put-malicious-code-iphones-androids-9523698/>

<https://www.thesun.co.uk/tech/9069211/whatsapp-surveillance-cyber-attack-glitch/>

THE PROMIS BACKDOOR

Beyond embedded journalists, news blackouts, false flag events, blacklisted and disappeared Internet domains the plotline of America's "free press" there are now ISP-filtering programs subject to Homeland Security guidelines that sift through emails and toss some into a black hole. Insiders and the NSA-approved, however, can get around such protections of networks by means of the various hybrids of the PROM IS backdoor. The 1980s theA of the Prosecutor's Management Information System (PROMIS) software handed over the golden key that would grant most of the world to a handful of criminals. In fact, this one crime may have been the final deal with the devil that consigned the United States to its present shameful descent into moral turpitude. PROMIS began as a COBOL-based program designed to track multiple offenders through multiple databases like those of the DOJ, CIA, U.S. Attorney, IRS, etc. Its creator was a former NSA analyst named William Hamilton. About the time that the October Surprise Iranian hostage drama was stealing the election for former California governor Ronald Reagan and former CIA director George H.W. Bush in 1980, Hamilton was moving his Inslaw Inc. from non-profit to for-profit status.

His intention was to keep the upgraded version of PROM IS that Inslaw had paid for and earmark a public domain version funded by a Law Enforcement Assistance Administration (LEAA) grant for the government. With 570,000 lines of code, PROMIS was able to integrate innumerable databases without any reprogramming and thus turn mere data into information.

With Reagan in the White House, his California cronies at the DOJ offered Inslaw a \$9.6 million contract to install public-domain PROMIS in prosecutors' offices, though it was really the enhanced PROM IS that the good-old-boy network had set its sights on. In February 1983, the chief of Israeli antiterrorism intelligence was sent to Inslaw under an alias to see for himself the DEC VAX enhanced

version. He recognized immediately that this software would revolutionize Israeli intelligence and crush the Palestine Intifada. Enhanced PROMIS could extrapolate nuclear submarine routes and destinations, track assets, trustees, and judges. Not only that, but the conspirators had a CIA genius named Michael Riconosciuto who could enhance the enhanced version one step further, once it was in their possession. To install public domain PROMIS in ninety-four U.S. Attorney offices as per contract, Inslaw had to utilize its enhanced PROMIS.

The DOJ made its move, demanding temporary possession of enhanced PROMIS as collateral to ensure that all installations were completed and that only Inslaw money had gone into the enhancements. Naïvely, Hamilton agreed. The rest is history: the DOJ delayed payments on the \$9.6 million and drove Inslaw into bankruptcy. With Edwin Meese III as Attorney General, the bankruptcy system was little more than a political patronage system, anyway. The enhanced PROMIS was then passed to the brilliant multivalent computer and chemical genius Riconosciuto, son of CIA Agent Marshall Riconosciuto.⁵ Recruited at sixteen, Michael had studied with Nobel Prize-winning physicist and co-inventor of the laser Arthur Schawlow. Michael was moved from Indio to Silver Springs to Miami as he worked to insert a chip that would broadcast the contents of whatever database was present to collection satellites and monitoring vans like the Google Street View van, using a digital spread spectrum to make the signal look like computer noise. This Trojan horse would grant key-club access to the backdoor of any person or institution that purchased PROMIS software as long as the backdoor could be kept secret. Meanwhile, the drama between Hamilton and the conspirators at DOJ continued. A quiet offer to buy out Inslaw was proffered by the investment banking firm Allen & Co., British publisher (Daily Mirror) Robert Maxwell, the Arkansas corporation Systematics, and Arkansas lawyer (and Clinton family friend) Webb Hubbell.

Hamilton refused and filed a \$50 million lawsuit in bankruptcy court against the DOJ on June 9, 1986. Bankruptcy Judge George F. Bason, Jr. ruled that the DOJ had indeed stolen PROMIS through trickery, fraud, and deceit, and awarded Inslaw \$6.8 million. He was unable to bring perjury charges against government officials but recommended to the House Judiciary Committee that it conduct a full investigation of the DOJ. The DOJ's appeal failed, but the Washington, D.C. Circuit Court of Appeals reversed everything on a technicality. Under then-President George H.W. Bush (1989 — 1993), Inslaw's petition to the Supreme Court in October 1991 was scorned. When the IRS lawyer requested that Inslaw be liquidated in such a way that the U.S. Trustee program (AG Meese's feeding trough between the DOJ and IRS) could name the trustee who would convert the assets, oversee the auction, and retain the appraisers, Judge Bason refused.

Under then-President William Jefferson Clinton (1993 — 2001), the Court of Federal Claims whitewashed the DOJ's destruction of Inslaw and the A of PROMIS on July 31, 1997. Judge Christine Miller sent a 186-page advisory opinion to Congress claiming that Inslaw's complaint had no merit a somber message to software developers seeking to do business with Attorney Generals and their DOJ. For his integrity, Judge Bason lost his bench seat to the IRS lawyer. T

Throughout three administrations, the mainstream Mockingbird media obediently covered up the Inslaw affair, enhanced PROMIS being a master tool of inference extraction able to track and eavesdrop like

nothing else. Once enhanced PROMIS was being sold domestically and abroad so as to steal data from individuals, government agencies, banks, and corporations everywhere, intelligence-connected Barry Kumnick~ turned PROMIS into an artificial intelligence (AI) tool called SMART (Special Management Artificial Reasoning Tool) that revolutionized surveillance. The DOJ promised Kumnick \$25 million, then forced him into bankruptcy as it had Hamilton. (Unlike Hamilton, Kumnick settled for a high security clearance and work at military contractors Systematics and Northrop.) Five Eyes / Echelon and the FBI's Carnivore / Data Collection System 1000 were promptly armed with SMART, as was closed circuit satellite highdefinition (HD) television. With SMART, Five Eyes / Echelon intercepts for UKUSA agencies became breathtaking.

The next modification to Hamilton's PROMIS was Brainstorm, a behavioral recognition software, followed by the facial recognition soAware Flexible Research System (FRS); then Semantic Web, which looks not just for link words and embedded code but for what it means that this particular person is following this particular thread. Then came quantum modification. The Department of Defense paid Simulex, Inc. to develop Sentient World Simulation (SWS), a synthetic mirror of the real world with automated continuous calibration with respect to current real-world information. The SEAS (Synthetic Environment for Analysis and Simulations) soAware platform drives SWS to devour as many as five million nodes of breaking news census data, shiAing economic indicators, real world weather patterns, and social media data, then feeds it proprietary military intelligence and fictitious events to gauge their destabilizing impact. Research into how to maintain public cognitive dissonance and learned helplessness (psychologist Martin Seligman) help SEAS deduce human behavior.

There are legitimate reasons (<http://www.learnliberty.org/videos/edward-snowden-surveillance-is-about-power/>)to want to avoid being tracked and spied-on while you're online. But aside from that, doesn't it feel creepy knowing you're probably being watched every moment that you're online and that information about where you go and what you do could potentially be sold to anyone at any time--to advertisers, your health insurance company, a future employer, the government, even a snoopy neighbor? Wouldn't you feel better not having to worry about that on top of everything else you have to worry about every day?

You can test to what extent your browser is transmitting unique information using these sites: panopticlick.com, Shieldsup, and ip-check.info.

<https://panopticlick.eff.org/>

<https://www.grc.com/shieldsup>

<https://cheapskatesguide.org/articles/ip-check.info/?lang=en>

These sites confirm that browsers transmit a lot of data that can be used for fingerprinting. From playing around with these sites, I have noticed that turning off javascript in my browser does help some. Also the

TOR browser seems to transmit less data than most, but even it is not completely effective. The added benefit that you get from the TOR browser and especially the TAILS operating system is that they block your IP address from the websites you visit. You want to try several browsers to see which one transmits the least information. Perhaps you will be lucky enough to find a browser that transmits less information than the TOR browser.

The next thing to be aware of is that corporations have methods other than tracking to spy on you. There is a saying that if a corporation is offering you their product for free, you are their product. This means that corporations that offer you free services are selling the data they collect from you in order to be able to provide you with these services. So, chances are that companies that provide you with free email are reading your email. We know that, in addition to tracking you, Facebook reads your posts and knows who your friends are, and that is just the beginning of Facebook's spying methods. Free online surveys are just ways of collecting more data from you. Companies also monitor your credit card transactions and sell your online dating profiles. If you have a Samsung TV that is connected to the internet, it's probably recording what you watch and may even be listening to your private conversations in your home. In fact, anything that you have in your home that is connected to the internet may be spying on you, right down to your internet-connected light bulb. With a few exceptions, online search engines monitor and log your searches. One of the exceptions is the ixquick.com search engine, which is headquartered in Europe. The steps to counter the nearly ubiquitous activities of free service providers would be to pay for services you receive online, read website privacy agreements, and not buy products that are known to be spying on you. However, the only way to be really secure from corporations using the internet to spy on you is to never connect to the internet or buy any internet-connected appliances. Welcome back to the 1980's.

Protecting yourself from government spying while you are on the internet is the hardest and requires the most knowledge. The biggest problem is that unless a whistle-blower like Edward Snowden tells us, we have no way of knowing how governments may potentially be spying on us. That means that we have no way of protecting ourselves 100% of the time from government spying. Some things whistle-blowers have revealed (<https://secureswissdata.com/9-ways-government-spying-on-internet-activity/>) are that the US government logs the meta data from all phone calls (who calls who and when), secretly forces internet service providers and providers of other services to allow it to "listen in on" and record all traffic going through their servers, reads nearly all email sent from everywhere in the world, and tracks the locations of all cell phones (even when they're turned off). And, although I am not aware of any specific whistle-blower revelations on this, there is every reason to believe that the US government (and perhaps others, including China's) has backdoors built into all computer hardware and operating system software for monitoring everything we do on our cell phones, tablets, laptops, desktop computers, and routers. (<https://www.eteknix.com/nsa-may-backdoors-built-intel-amd-processors/>) See also this. Because Lenovo computers are manufactured in China, the US government has issued warnings to all US government agencies and subcontractors to strongly discourage them from using Lenovo computers. And the US government probably has backdoors (<https://www.atlasobscura.com/articles/a-brief-history-of-the-nsa-attempting-to-insert-backdoors-into-encrypted-data>) into all commercially-available encryption software, with the possible exception of Truecrypt version 7.1a. I hope you are understanding now the magnitude of the lengths that governments are going to (using your tax money) to spy on you. In truth, we are now

approaching the level of government spying that George Orwell warned about in his book, 1984

So what can we practically do to protect ourselves from government spying? Seriously, there isn't much, if we want to use cell phones, credit cards, and the internet. About all we can do, if we absolutely need to have a private conversation, is to have a face-to-face meeting without any electronics within microphone range. That includes cell phones, Samsung TV's, video cameras, computers, or land-line telephones. And don't travel to the meeting place using long-distance commercial transportation.

Sending a letter through the US mail is the next best, although it is known that the outsides of all mail sent through the US mail are photographed, and the pictures are stored. So, don't put your return address on the envelope. (

http://www.abajournal.com/news/article/new_york_times_post_office_photocopies_envelopes_of_all_mail_sent_in_the_us/) As far as surfing the internet is concerned, begin with all the precautions that I outlined above to protect yourself from corporate spying (except HTTPS and VPN's). Then, add the TAILS operating system on a USB stick. As I said, TAILS will not prevent you from being identified and tracked via the fingerprinting method. And who can be sure whether the government has a backdoor in TAILS? As far as I know, the super-paranoid, hooded and sunglasses method I outlined above is the next step.

Experts warns of 'epidemic' of bugging devices used by stalkers - By James Hockaday

Stalkers are using cheap bugging devices hidden in everyday household items

More funding and legal powers are needed for police to stop a surge of stalkers using eavesdropping devices to spy on victims, experts have warned.

Firms paid to detect the bugs say they're finding more and more of the devices which are readily available on online marketplaces like Amazon and eBay.

Jack Lazzereschi, Technical Director of bug sweeping company Shapestones, says cases of stalking and victims being blackmailed with intimate footage shot in secret has doubled in the past two years.

He told Metro.co.uk: 'The police want to do something about it, they try to, but usually they don't have the legal power or the resources to investigate.

'For us it's a problem. We try to protect the client, we want to assure that somebody has been protected.'
Advert for a hidden camera device planted inside a fire/smoke alarm sold on Amazon

People are paying as little as £15 for listening devices and spy cameras hidden inside desk lamps, wall sockets, phone charger cables, USB sticks and picture frames.

Users insert a sim card into a hidden slot and call a number to listen in on their unwitting targets.

People using hidden cameras can watch what's happening using an apps on their phones.

Jack says the devices are so effective, cheap and hard to trace to their users, law enforcement prefer using them over expensive old-school devices.

Although every case is different, in situations where homeowners plant devices in their own properties, Jack says there's usually a legal 'grey area' to avoid prosecution.

The devices themselves aren't illegal and they are usually marketed for legitimate purposes like protection, making it difficult for cops to investigate.

There is no suggestion online marketplaces like eBay and Amazon are breaking the law by selling them.

But in some instances, images of women in their underwear have been used in listings – implying more sinister uses for the devices.

Even in cases when people are more clearly breaking the law, Jack says it's unlikely perpetrators will be brought to justice as overstretched police will prioritise resources to stop violent crime.

Jack's says around 60 per cent of his firm's non-corporate cases cases involve stalking or blackmail.

He says it's become an 'epidemic' over the past couple of years with the gadgets more readily available than ever before.

Jack Lazzereschi says he's seen stalking cases double in a few years

Victims are often filmed naked or having sex and threatened with the threat of footage being put online and in the worst cases children are also recorded.

Jack says UK law is woefully unprepared to deal with these devices compared to countries in the Asian-Pacific region.

In South Korea authorities have cracked down on a scourge of perverts planting cameras in public toilets.

James Williams, director of bug sweepers QCC Global says snooping devices used to be the preserve of people with deep pockets and technological know-how.

He said: 'It's gone from that to really being at a place where anybody can just buy a device from the internet.

‘Anything you can possibly think of you can buy with a bug built into it. I would say they’re getting used increasingly across the board.’

Suky Bhaker, Acting CEO of the Suzy Lamplugh Trust, which runs the National Stalking Helpline, warned using these gadgets could be a prelude to physical violence.

She said: ‘We know that stalking and coercive control are extremely dangerous and can cause huge harm to the victim, both in terms of their psychological wellbeing and the potential for escalation to physical violence or even murder.’

‘The use of surveillance devices or spyware apps by stalkers, must be seen in the context of a pattern of obsessive, fixated behaviour which aims at controlling and monitoring the victim.’

She added: ‘There should be clarity for police forces that the use of surveillance equipment by stalkers to monitor their victim’s location or communications is a sign that serious and dangerous abuse may be present or imminent.’

‘All cases of stalking or coercive control should be taken seriously and investigated when reported to police.’

The charity is calling for all police forces across the country to train staff in this area.

Earlier this month a policeman known only by his surname Mills was barred from the profession for life for repeatedly dismissing pleas for help from 19-year-old Shana Grice who was eventually murdered by her stalker ex-boyfriend Michel Lane.

A spokesman for eBay said: ‘The listing of mini cameras on eBay is permitted for legitimate items like baby monitors or doorbell cameras.’

‘However, items intended to be used as spying devices are banned from eBay’s UK platform in accordance with the law and our policy.’

‘We have filters in place to block prohibited items, and all the items flagged by Metro have now been removed.’

Face-tracking harvesters grab one picture of you and then use AI to find every other digital picture of you on Earth and open every social media post, resume, news clipping, dating account etc. and sell the full dossier on you to Axiom, the NSA, Political manipulators etc. and hack your bank accounts and credit cards. Never put an unsecured photo of yourself online.

=====

Who's Watching Your WebEx? Webex has many back-door spy paths built in

KrebsOnSecurity spent a good part of the past week working with **Cisco** to alert more than four dozen companies — many of them household names — about regular corporate [WebEx](#) conference meetings that lack passwords and are thus open to anyone who wants to listen in.



Department of Energy's WebEx meetings.

At issue are recurring video- and audio conference-based meetings that companies make available to their employees via WebEx, a set of online conferencing tools run by Cisco. These services allow customers to password-protect meetings, but it was trivial to find dozens of major companies that do not follow this basic best practice and allow virtually anyone to join daily meetings about apparently internal discussions and planning sessions.

Many of the meetings that can be found by a cursory search within an organization's "Events Center" listing on Webex.com seem to be intended for public viewing, such as product demonstrations and presentations for prospective customers and clients. However, from there it is often easy to discover a host of other, more proprietary WebEx meetings simply by clicking through the daily and weekly meetings listed in each organization's "Meeting Center" section on the Webex.com site.

Some of the more interesting, non-password-protected recurring meetings I found include those from **Charles Schwab, CSC, CBS, CVS, The U.S. Department of Energy, Fannie Mae, Jones Day, Orbitz, Paychex Services, and Union Pacific**. Some entities even also allowed access to archived event recordings.

Cisco began reaching out to each of these companies about a week ago, and today released an [all-customer alert](#) (PDF) pointing customers to a [consolidated best-practices document](#) written for Cisco WebEx site administrators and users.

“In the first week of October, we were contacted by a leading security researcher,” Cisco wrote. “He showed us that some WebEx customer sites were publicly displaying meeting information online, including meeting Time, Topic, Host, and Duration. Some sites also included a ‘join meeting’ link.”

=====

Quest Diagnostics Says All 12 Million Patients May Have Had Financial, Medical, Personal Information Breached. It includes credit card numbers and bank account information, according to a filing... HOW MANY TIMES DO YOU NEED TO BE TOLD: "NEVER, EVER, GIVE TRUE INFORMATION TO ANY COMPANY THAT USES A NETWORK OR MAKES YOU SIGN-IN TO ANYTHING ONLINE!"

<https://khn.org/news/a-wake-up-call-on-data-collecting-smart-beds-and-sleep-apps/>

=====

<https://www.wsj.com/articles/hackers-may-soon-be-able-to-tell-what-youre-typing-just-by-hearing-you-type-11559700120>

<https://sputniknews.com/science/201906051075646555-chinese-cyborg-future-chip/>

<https://www.emarketer.com/content/average-us-time-spent-with-mobile-in-2019-has-increased>

<https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-20190603-story.html>

<https://thehill.com/homenews/media/447532-news-industry-joins-calls-for-more-scrutiny-of-big-tech>

<https://www.bnnbloomberg.ca/the-future-will-be-recorded-on-your-smart-speaker-1.1270598>

<https://www.washingtontimes.com/news/2019/jun/9/robert-mueller-exploited-cell-phone-gps-track-trum/>

<https://www.theorganicprepper.com/the-unholy-alliance-between-dna-sites-and-facial-recognition/>

Google still keeps a list of everything you ever bought using Gmail, even if you delete all your emails, and provides that data to political parties, the NSA and marketing companies so they can manipulate you

ToddHaselton@robotodd

Key Points

- Google Gmail keeps a log of everything you buy.
- Google says this is so you can ask Google Assistant about the status of an order or reorder something.
- It also says you can delete this log by deleting the email, but three weeks after we deleted all email, the list is still there.

Google CEO Sundar Pichai

Google

Google and other tech companies have been under fire recently for a variety of issues, including failing to protect [user data](#), [failing to disclose](#) how data is collected and used and [failing to police the content](#) posted to their services.

Companies such as Google have embedded themselves in our lives with useful services including Gmail, Google Maps and Google Search, as well as smart products such as the Google Assistant which can answer our questions on a whim. The benefits of these tools come at the cost of our privacy, however, because while Google says that privacy should not be a “[luxury good](#),” it’s still going to great lengths to collect as much detail as possible about its users and making it more difficult than necessary for users to track what’s collected about them and delete it.

Here’s the latest case in point.

In May, I wrote up something weird I spotted on [Google’s](#) account management page. I noticed that Google uses Gmail to store a list of [everything you’ve purchased](#), if you used Gmail or your Gmail address in any part of the transaction.

If you have a confirmation for a prescription you picked up at a pharmacy that went into your Gmail account, Google logs it. If you have a receipt from Macy’s, Google keeps it. If you bought food for delivery and the receipt went to your Gmail, Google stores that, too.

You get the idea, and you can see your own purchase history by going to [Google's Purchases page](#).

Google says it does this so you can use Google Assistant to track packages or reorder things, even if that's not an option for some purchases that aren't mailed or wouldn't be reordered, like something you bought at a store.

At the time of my original story, Google said users can delete everything by tapping into a purchase and removing the Gmail. It seemed to work if you did this for each purchase, one by one. This isn't easy — for years worth of purchases, this would take hours or even days of time.

So, since Google doesn't let you bulk-delete this purchases list, I decided to delete everything in my Gmail inbox. That meant removing every last message I've sent or received since I opened my Gmail account more than a decade ago.

Despite Google's assurances, it didn't work.

Like a horror movie villain that just won't die

On Friday, three weeks after I deleted every Gmail, I checked my purchases list.

I still see receipts for things I bought years ago. Prescriptions, food deliveries, books I bought on Amazon, music I purchased from iTunes, a subscription to Xbox Live I bought from Microsoft -- it's all there.

A list of my purchases Google pulled in from Gmail.

Todd Haselton | CNBC

Google continues to show me purchases I've made recently, too.

I can't delete anything and I can't turn it off.

When I click on an individual purchase and try to remove it — it says I can do this by deleting the email, after all — it just redirects to my inbox and not to the original email message for me to delete, since that email no longer exists.

So Google is caching or saving this private information somewhere else that isn't just tied to my Gmail account.

When I wrote my original story, a Google spokesperson insisted this list is only for my use, and said the company views it as a convenience. Later, the company followed up to say this data is used to “help you get things done, like track a package or reorder food.”

But it's a convenience I never asked for, and the fact that Google compiles and stores this information regardless of what I say or do is a bit creepy.

A spokesperson was not immediately available to comment on this latest development.

But it shows once again how tech companies often treat user privacy as a low-priority afterthought and will only make changes if user outrage forces their hand.

<https://archive.is/WXOD5>

https://www.theregister.co.uk/2019/07/11/google_assistant_voice_eavesdropping_creepy/

<https://www.technowize.com/google-home-is-sending-your-private-recordings-to-google-workers/>

<https://phys.org/news/2019-07-malicious-apps-infect-million-android.html>

<https://archive.fo/RrnuL#selection-1489.0-1489.170>

<https://www.zdnet.com/article/microsoft-stirs-suspicious-by-adding-telemetry-files-to-security-only-update/>

<https://www.bostonglobe.com/news/nation/2019/07/07/fbi-ice-use-driver-license-photos-without-owners-knowledge-consent/WmDbiCrNNWaWQrVrp7q3CL/story.html>

<https://www.telegraph.co.uk/technology/2019/07/08/tfl-begins-tracking-london-underground-commuters-using-wi-fi/>

<https://www.msn.com/en-us/news/us/fbi-ice-find-state-drivers-license-photos-are-a-gold-mine-for-facial-recognition-searches/ar-AADZk0d>

EVERYTHING IN AMERICA HAS BEEN HACKED OR SOON WILL BE:

In a country of just 7 million people, the [scale of the hack](#) means that just about every working adult has been affected.

"We should all be angry. ... The information is now freely available to anyone. Many, many people in Bulgaria already have this file, and I believe that it's not only in Bulgaria," said Genov, a blogger and political analyst. He knows his data was compromised because, though he's not an IT expert, he managed to find the stolen files online.

[Microsoft says foreign hackers still actively targeting US political targets](#)

The attack is extraordinary, but it is [not unique](#).

Government databases are gold mines for hackers. They contain a huge wealth of information that can be "useful" for years to come, experts say. "You can make (your password) longer and more sophisticated, but the information the government holds are things that are not going to change," said Guy Bunker, an information security expert and the chief technology officer at Clearswift, a cybersecurity company. "Your date of birth is not going to change, you're not going to move house tomorrow," he said. "A lot of the information that was taken was valid yesterday, is valid today, and will probably be valid for a large number of people in five, 10, 20 years' time."

Hackers' paradise

Data breaches used to be spearheaded by highly skilled hackers. But it increasingly doesn't take a sophisticated and carefully planned operation to break into IT systems. Hacking tools and malware that are available on the dark web make it possible for amateur hackers to cause enormous damage. A [strict data protection law](#) that came into effect last year across the European Union has placed new burdens on

anyone who collects and stores personal data. It also introduced hefty fines for anyone who mismanages data, potentially opening the door for the Bulgarian government to fine itself for the breach.

[Slack is resetting thousands of passwords after 2015 hack](#)

Still, attacks against government systems are on the rise, said Adam Levin, the founder of CyberScout, another cybersecurity firm. "It's a war right now -- one we will win if we make cybersecurity a front-burner issue," he said. The notion that governments urgently need to step up their cybersecurity game is not new. Experts have been ringing alarm bells for years.

The US Department of Veterans Affairs suffered one of the first major data breaches in 2006, when personal data of more than 26 million veterans and military personnel were compromised. "And it was all, 'Oh, this is dreadful. We must do things to stop it.' ... And here we are, 13 years later, and an entire country's data has been compromised, and in between, there's been incidents of large swathes of citizen data being compromised in different countries," Bunker said. Out-of-date systems are often the problem. Some governments may have used private companies to manage the data they collected before the array of hacks and breaches brought their attention to cybersecurity. "In many cases, our data was sent to third-party contractors years ago," Levin said. "The way we looked at data management 10 years ago seems antiquated today, yet that old data is still out there being managed by third parties, using legacy systems."

[Chinese spies stole NSA hacking tools, report finds](#)

If the "old data" hasn't changed, it's still valuable to hackers.

The Bulgaria incident is concerning, said Desislava Krusteva, a Bulgarian privacy and data protection lawyer who advises some of the world's biggest tech companies on how to keep their clients' information safe.

"These kinds of incidents should not happen in a state institution. It seems like it didn't require huge efforts, and it's probably the personal data of almost all Bulgarian citizens," said Krusteva, a partner at Dimitrov, Petrov & Co., a law firm in Sofia.

The Bulgarian Commission for Personal Data Protection has said it would launch an investigation into the hack.

A National Revenue Agency spokesman would not comment on whether the data was properly protected.

"As there is undergoing investigation, we couldn't provide more details about reasons behind the hack," Communications Director Rossen Bachvarov said.

'Very embarrassing for the government'

A 20-year-old cybersecurity worker has been arrested by the Bulgarian police in connection with the hack. The computer and software used in the attack led police to the suspect, according to the Sofia prosecutor's office.

The man has been detained, and the police seized his equipment, including mobile phones, computers and drives, the prosecutor's office said in a statement. If convicted, he could spend as long as eight years in prison.

-
[US indicts two people in China over hacks](#)

"It's still too early to say what exactly happened, but from political perspective, it is, of course, very embarrassing for the government," Krusteva said.

The embarrassment is made worse by the fact that this was not the first time the Bulgarian government was targeted. The country's Commercial Registry was brought down less than a year ago by an attack. "So, at least for a year, the Bulgarian society, politicians, those who are in charge of the country, they knew quite well about the serious cybersecurity problems in the government infrastructures," Genov said, "and they didn't do anything about it."

Hackers posted screenshots of the company's servers on Twitter and later shared the stolen data with Digital Revolution, another hacking group [who last year breached Quantum, another FSB contractor](#).

This second hacker group shared the stolen files in greater detail on their Twitter account, on Thursday, July 18, and with Russian journalists afterward.

Alexa and Google Home eavesdrop and phish passwords

Amazon- and Google-approved apps turned both voice-controlled devices into "smart spies."

[Dan Goodin](#) -



[Enlarge](#)
[Aurich Lawson / Amazon](#)

By now, the privacy threats posed by Amazon Alexa and Google Home are common knowledge. Workers for both companies routinely [listen](#) to [audio](#) of users—recordings of which can be [kept forever](#)—and the sounds the devices capture can be [used in criminal trials](#).

Now, there's a new concern: malicious apps developed by third parties and hosted by Amazon or Google. The threat isn't just theoretical. Whitehat hackers at Germany's Security Research Labs developed eight apps—four Alexa "skills" and four Google Home "actions"—that all passed Amazon or Google security-vetting processes. The skills or actions posed as simple apps for checking horoscopes, with the exception of one, which masqueraded as a random-number generator. Behind the scenes, these "smart spies," as the researchers call them, surreptitiously eavesdropped on users and phished for their passwords.

"It was always clear that those voice assistants have privacy implications—with Google and Amazon receiving your speech, and this possibly being triggered on accident sometimes," Fabian Bräunlein, senior security consultant at SRLabs, told me. "We now show that, not only the manufacturers, but... also hackers can abuse those voice assistants to intrude on someone's privacy."

The malicious apps had different names and slightly different ways of working, but they all followed similar flows. A user would say a phrase such as: "Hey Alexa, ask My Lucky Horoscope to give me the horoscope for Taurus" or "OK Google, ask My Lucky Horoscope to give me the horoscope for Taurus." The eavesdropping apps responded with the requested information while the phishing apps gave a fake error message. Then the apps gave the impression they were no longer running when they, in fact, silently waited for the next phase of the attack.

As the following two videos show, the eavesdropping apps gave the expected responses and then went silent. In one case, an app went silent because the task was completed, and, in another instance, an app went silent because the user gave the command "stop," which Alexa uses to terminate apps. But the apps quietly logged all conversations within earshot of the device and sent a copy to a developer-designated server.

The phishing apps follow a slightly different path by responding with an error message that claims the skill or action isn't available in that user's country. They then go silent to give the impression the app is no longer running. After about a minute, the apps use a voice that mimics the ones used by Alexa and Google Home to falsely claim a device update is available and prompts the user for a password for it to be installed.

SRLabs eventually took down all four apps demoed. More recently, the researchers developed four German-language apps that worked similarly. All eight of them passed inspection by Amazon and Google. The four newer ones were taken down only after the researchers privately reported their results to Amazon and Google. As with most skills and actions, users didn't need to download anything. Simply saying the proper phrases into a device was enough for the apps to run.

All of the malicious apps used common building blocks to mask their malicious behaviors. The first was exploiting a flaw in both Alexa and Google Home when their text-to-speech engines received instructions to speak the character "◆." (U+D801, dot, space). The unpronounceable sequence caused both devices to remain silent even while the apps were still running. The silence gave the impression the apps had terminated, even when they remained running.

The apps used other tricks to deceive users. In the parlance of voice apps, "Hey Alexa" and "OK Google" are known as "wake" words that activate the devices; "My Lucky Horoscope" is an "invocation" phrase used to start a particular skill or action; "give me the horoscope" is an "intent" that tells the app which function to call; and "taurus" is a "slot" value that acts like a variable. After the apps received initial approval, the SRLabs developers manipulated intents such as "stop" and "start" to give them new functions that caused the apps to listen and log conversations.

Others at SRLabs who worked on the project include security researcher Luise Frerichs and Karsten Nohl, the firm's chief scientist. In a [post documenting the apps](#), the researchers explained how they developed the Alexa phishing skills:

1. Create a seemingly innocent skill that already contains two intents:
 - an intent that is started by "stop" and copies the stop intent
 - an intent that is started by a certain, commonly used word and saves the following words as slot values. This intent behaves like the fallback intent.
2. After Amazon's review, change the first intent to say goodbye, but then keep the session open and extend the eavesdrop time by adding the character sequence "(U+D801, dot, space)" multiple times to the speech prompt.
3. Change the second intent to not react at all

When the user now tries to end the skill, they hear a goodbye message, but the skill keeps running for several more seconds. If the user starts a sentence beginning with the selected word in this time, the intent will save the sentence as slot values and send them to the attacker.

To develop the Google Home eavesdropping actions:

1. Create an Action and submit it for review.

2. After review, change the main intent to end with the Bye [earcon](#) sound (by playing a recording using the Speech Synthesis Markup Language (SSML)) and set `expectUserResponse` to true. This sound is usually understood as signaling that a voice app has finished. After that, add several `noInputPrompts` consisting only of a short silence, using the SSML element or the unpronounceable Unicode character sequence "◆."

3. Create a second intent that is called whenever an `actions.intent.TEXT` request is received. This intent outputs a short silence and defines several silent `noInputPrompts`.

After outputting the requested information and playing the earcon, the Google Home device waits for approximately 9 seconds for speech input. If none is detected, the device "outputs" a short silence and waits again for user input. If no speech is detected within 3 iterations, the Action stops.

When speech input is detected, a second intent is called. This intent only consists of one silent output, again with multiple silent reprompt texts. Every time speech is detected, this Intent is called and the reprompt count is reset.

The hacker receives a full transcript of the user's subsequent conversations, until there is at least a 30-second break of detected speech. (This can be extended by extending the silence duration, during which the eavesdropping is paused.)

In this state, the Google Home Device will also forward all commands prefixed by "OK Google" (except "stop") to the hacker. Therefore, the hacker could also use this hack to imitate other applications, man-in-the-middle the user's interaction with the spoofed Actions, and start believable phishing attacks.

SRLabs privately reported the results of its research to Amazon and Google. In response, both companies removed the apps and said they are changing their approval processes to prevent skills and actions from having similar capabilities in the future. In a statement, Amazon representatives provided the following statement and FAQ (emphasis added for clarity):

Customer trust is important to us, and we conduct security reviews as part of the skill certification process. We quickly blocked the skill in question and put mitigations in place to prevent and detect this type of skill behavior and reject or take them down when identified.

On the record Q&A:

1) Why is it possible for the skill created by the researchers to get a rough transcript of what a customer says after they said "stop" to the skill?

This is no longer possible for skills being submitted for certification. We have put mitigations in place to prevent and detect this type of skill behavior and reject or take them down when identified.

2) Why is it possible for SR Labs to prompt skill users to install a fake security update and then ask them to enter a password?

We have put mitigations in place to prevent and detect this type of skill behavior and reject or take them down when identified. This includes preventing skills from asking customers for their Amazon passwords.

It's also important that customers know we provide automatic security updates for our devices, and will never ask them to share their password.

Google representatives, meanwhile, wrote:

All Actions on Google are required to follow our developer [policies](#), and we prohibit and remove any Action that violates these policies. We have review processes to detect the type of behavior described in this report, and we removed the Actions that we found from these researchers. We are putting additional mechanisms in place to prevent these issues from occurring in the future.

Google didn't say what these additional mechanisms are. On background, a representative said company employees are conducting a review of all third-party actions available from Google, and during that time, some may be paused temporarily. Once the review is completed, actions that passed will once again become available.

It's encouraging that Amazon and Google have removed the apps and are strengthening their review processes to prevent similar apps from becoming available. But the SRLabs' success raises serious concerns. Google Play has a long history of hosting malicious apps that [push sophisticated surveillance malware](#)—in at least one case, researchers said, so that [Egypt's government could spy on its own citizens](#). Other malicious Google Play apps have [stolen users' cryptocurrency](#) and [executed secret payloads](#). These kinds of apps have routinely slipped through Google's vetting process for years.

There's little or no evidence third-party apps are actively threatening Alexa and Google Home users now, but the SRLabs research suggests that possibility is by no means farfetched. I've long remained convinced that the risks posed by Alexa, Google Home, and other always-listening apps outweigh their benefits. SRLabs' Smart Spies research only adds to my belief that these devices shouldn't be trusted by most people.

[Dan Goodin](#) Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.



Figure 1: AMERICAN'S CAN NO LONGER TOLERATE THE CONSTANT DIGITAL ABUSE OF THEIR MIND'S BY T-MOBILE, AT&T, ASSURANCE, APPLE ET AL...

FSB's secret projects

Per the different reports in Russian media, the files indicate that SyTech had worked since 2009 on a multitude of projects since 2009 for FSB unit 71330 and for fellow contractor Quantum. Projects include:

- **Nautilus** - a project for collecting data about EVERY social media and dating site user (such as Facebook, Match.com, OKCUPID, Plenty of Fish)MySpace, and LinkedIn).
- **Nautilus-S** - a project for deanonymizing Tor traffic with the help of rogue Tor servers.
- **Reward** - a project to covertly penetrate P2P networks, like the one used for torrents.
- **Mentor** - a project to monitor and search email communications on the servers of Russian companies.
- **Hope** - a project to investigate the topology of the Russian internet and how it connects to other countries' network.
- **Tax-3** - a project for the creation of a closed intranet to store the information of highly-sensitive state figures, judges, and local administration officials, separate from the rest of the state's IT networks.

BBC Russia, who received the full trove of documents, claims there were other older projects for researching other network protocols such as Jabber (instant messaging), ED2K (eDonkey), and OpenFT (enterprise file transfer).

Other files posted on the Digital Revolution Twitter account claimed that the FSB was also tracking students and pensioners.

Additional Academic, Federal and Journalism sources providing the citations, assertions, and the evidence proving, the above points herein:

- *Anne Broache. ["FBI wants widespread monitoring of 'illegal' Internet activity"](#). CNET. Retrieved 25 March 2014.*
- *["Is the U.S. Turning Into a Surveillance Society?"](#). American Civil Liberties Union. Retrieved March 13, 2009.*
- *["Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society"](#) (PDF). American Civil Liberties Union. January 15, 2003. Retrieved March 13, 2009.*
- *["Anonymous hacks UK government sites over 'draconian surveillance' "](#), Emil Protalinski, ZDNet, 7 April 2012, retrieved 12 March 2013*
- *[Hacktivists in the frontline battle for the internet](#) retrieved 17 June 2012*
- *Diffie, Whitfield; Susan Landau (August 2008). ["Internet Eavesdropping: A Brave New World of Wiretapping"](#). Scientific American. Retrieved 2009-03-13.*
- *["CALEA Archive -- Electronic Frontier Foundation"](#). Electronic Frontier Foundation (website). Archived from [the original](#) on 2009-05-03. Retrieved 2009-03-14.*
- *["CALEA: The Perils of Wiretapping the Internet"](#). Electronic Frontier Foundation (website). Retrieved 2009-03-14.*

- ["CALEA: Frequently Asked Questions"](#). Electronic Frontier Foundation (website). Retrieved 2009-03-14.
- Kevin J. Connolly (2003). *Law of Internet Security and Privacy*. [Aspen Publishers](#). p. 131. [ISBN](#) .
- [American Council on Education vs. FCC Archived](#) 2012-09-07 at the [Wayback Machine](#), Decision, United States Court of Appeals for the District of Columbia Circuit, 9 June 2006. Retrieved 8 September 2013.
- Hill, Michael (October 11, 2004). ["Government funds chat room surveillance research"](#). *USA Today*. Associated Press. Retrieved 2009-03-19.
- McCullagh, Declan (January 30, 2007). ["FBI turns to broad new wiretap method"](#). *ZDNet News*. Retrieved 2009-03-13.
- ["First round in Internet war goes to Iranian intelligence"](#), [Debkafile](#), 28 June 2009. (subscription required)
- O'Reilly, T. (2005). *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*. O'Reilly Media, 1-5.
- Fuchs, C. (2011). *New Media, Web 2.0 and Surveillance*. *Sociology Compass*, 134-147.
- Fuchs, C. (2011). *Web 2.0, Presumption, and Surveillance*. *Surveillance & Society*, 289-309.
- Anthony Denise, Celeste Campos-Castillo, Christine Horne (2017). *"Toward a Sociology of Privacy"*. *Annual Review of Sociology*. **43**: 249–269. [doi:10.1146/annurev-soc-060116-053643](#).
- Muise, A., Christofides, E., & Demsmarais, S. (2014). "Creeping" or just information seeking? Gender differences in partner monitoring in response to jealousy on Facebook. *Personal Relationships*, 21(1), 35-50.
- ["How Stuff Works"](#). Retrieved November 10, 2017.
- [\[electronics.howstuffworks.com/gadgets/high-tech-gadgets/should-smart-devices-automatically-call-cops.htm. "How Stuff Works"\]](#) Check `|ur l= value` ([help](#)). Retrieved November 10, 2017.
- [\[time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues "Time Alexa Takes the Stand Listening Devices Raise Privacy Issues"\]](#) Check `|ur l= value` ([help](#)). Retrieved November 10, 2017.
- Story, Louise (November 1, 2007). ["F.T.C. to Review Online Ads and Privacy"](#). *New York Times*. Retrieved 2009-03-17.
- Butler, Don (January 31, 2009). ["Are we addicted to being watched?"](#). *The Ottawa Citizen*. *canada.com*. Archived from [the original](#) on 22 July 2013. Retrieved 26 May 2013.
- Soghoian, Chris (September 11, 2008). ["Debunking Google's log anonymization propaganda"](#). *CNET News*. Retrieved 2009-03-21.
- Joshi, Priyanki (March 21, 2009). ["Every move you make, Google will be watching you"](#). *Business Standard*. Retrieved 2009-03-21.
- ["Advertising and Privacy"](#). *Google (company page)*. 2009. Retrieved 2009-03-21.
- ["Spyware Workshop: Monitoring Software on Your OC: Spywae, Adware, and Other Software"](#), Staff Report, U.S. Federal Trade Commission, March 2005. Retrieved 7 September 2013.
- Aycock, John (2006). *Computer Viruses and Malware*. *Springer*. [ISBN](#) .
- ["Office workers give away passwords for a cheap pen"](#), John Leyden, *The Register*, 8 April 2003. Retrieved 7 September 2013.
- ["Passwords are passport to theft"](#), *The Register*, 3 March 2004. Retrieved 7 September 2013.

- ["Social Engineering Fundamentals, Part I: Hacker Tactics"](#), Sarah Granger, 18 December 2001.
- ["Stuxnet: How does the Stuxnet worm spread?"](#). *Antivirus.about.com*. 2014-03-03. Retrieved 2014-05-17.
- Keefe, Patrick (March 12, 2006). ["Can Network Theory Thwart Terrorists?"](#). *New York Times*. Retrieved 14 March 2009.
- Albrechtslund, Anders (March 3, 2008). ["Online Social Networking as Participatory Surveillance"](#). *First Monday*. **13** (3). Retrieved March 14, 2009.
- Fuchs, Christian (2009). [Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance](#) (PDF). Salzburg and Vienna: Forschungsgruppe Unified Theory of Information. ISBN . Archived from [the original](#) (PDF) on February 6, 2009. Retrieved March 14, 2009.
- Ethier, Jason (27 May 2006). ["Current Research in Social Network Theory"](#) (PDF). Northeastern University College of Computer and Information Science. Retrieved 15 March 2009.[\[permanent dead link\]](#)
- Marks, Paul (June 9, 2006). ["Pentagon sets its sights on social networking websites"](#). *New Scientist*. Retrieved 2009-03-16.
- Kawamoto, Dawn (June 9, 2006). ["Is the NSA reading your MySpace profile?"](#). *CNET News*. Retrieved 2009-03-16.
- Ressler, Steve (July 2006). ["Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research"](#). *Homeland Security Affairs*. **II** (2). Retrieved March 14, 2009.
- McNamara, Joel (4 December 1999). ["Complete, Unofficial Tempest Page"](#). Archived from [the original](#) on 1 September 2013. Retrieved 7 September 2013.
- Van Eck, Wim (1985). ["Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?"](#) (PDF). *Computers & Security*. **4** (4): 269–286. *CiteSeerX* [10.1.1.35.1695](#). doi:[10.1016/0167-4048\(85\)90046-X](#).
- Kuhn, M.G. (26–28 May 2004). ["Electromagnetic Eavesdropping Risks of Flat-Panel Displays"](#) (PDF). 4th Workshop on Privacy Enhancing Technologies. Toronto: 23–25.
- Asonov, Dmitri; Agrawal, Rakesh (2004), [Keyboard Acoustic Emanations](#) (PDF), IBM Almaden Research Center
- Yang, Sarah (14 September 2005), ["Researchers recover typed text using audio recording of keystrokes"](#), *UC Berkeley News*
- ["LA Times"](#). Retrieved November 10, 2017.
- Adi Shamir & Eran Tromer. ["Acoustic cryptanalysis"](#). Blavatnik School of Computer Science, Tel Aviv University. Retrieved 1 November 2011.
- Jeremy Reimer (20 July 2007). ["The tricky issue of spyware with a badge: meet 'policeware'"](#). *Ars Technica*.
- Hopper, D. Ian (4 May 2001). ["FBI's Web Monitoring Exposed"](#). *ABC News*.
- ["New York Times"](#). Retrieved November 10, 2017.
- ["Stanford University Clipper Chip"](#). Retrieved November 10, 2017.

- "[Consumer Broadband and Digital Television Promotion Act](#)" [Archived](#) 2012-02-14 at the [Wayback Machine](#), U.S. Senate bill S.2048, 107th Congress, 2nd session, 21 March 2002. Retrieved 8 September 2013.
- "[Swiss coder publicises government spy Trojan](#)". *News.techworld.com*. Retrieved 25 March 2014.
- Basil Cupa, [Trojan Horse Resurrected: On the Legality of the Use of Government Spyware \(Govware\)](#), LISS 2013, pp. 419-428
- "[FAQ – Häufig gestellte Fragen](#)". *Ejpd.admin.ch*. 2011-11-23. [Archived from the original](#) on 2013-05-06. Retrieved 2014-05-17.
- "[Censorship is inseparable from surveillance](#)", Cory Doctorow, *The Guardian*, 2 March 2012
- "[Trends in transition from classical censorship to Internet censorship: selected country overviews](#)"
- [The Enemies of the Internet Special Edition : Surveillance](#) [Archived](#) 2013-08-31 at the [Wayback Machine](#), Reporters Without Borders, 12 March 2013
- "[When Secrets Aren't Safe With Journalists](#)", Christopher Soghoian, *New York Times*, 26 October 2011
- [Everyone's Guide to By-passing Internet Censorship](#), The Citizen Lab, University of Toronto, September 2007
- [Stalker used pop idol's pupil image reflections in selfie to find location...](#)
- <https://www.slashfilm.com/netflix-physical-activity-tracking/>
- <https://www.technologyreview.com/s/614034/facebook-is-funding-brain-experiments-to-create-a-device-that-reads-your-mind/>
- <https://www.stratfor.com/>
- <https://www.acxiom.com/what-we-do/risk-solutions/>
- <https://www.cisco.com/c/en/us/products/contact-center/unified-intelligence-center/index.html>
- <https://www.fireeye.com/>
- Diffie, Whitfield; Susan Landau (August 2008). "[Internet Eavesdropping: A Brave New World of Wiretapping](#)". *Scientific American*. Retrieved March 13, 2009.
- "[CALEA Archive – Electronic Frontier Foundation](#)". *Electronic Frontier Foundation (website)*. [Archived from the original](#) on May 3, 2009. Retrieved March 14, 2009.
- "[CALEA: The Perils of Wiretapping the Internet](#)". *Electronic Frontier Foundation (website)*. Retrieved March 14, 2009.
- "[CALEA: Frequently Asked Questions](#)". *Electronic Frontier Foundation (website)*. September 20, 2007. Retrieved March 14, 2009.
- Hill, Michael (October 11, 2004). "[Government funds chat room surveillance research](#)". *USA Today*. Associated Press. Retrieved March 19, 2009.
- McCullagh, Declan (January 30, 2007). "[FBI turns to broad new wiretap method](#)". *ZDNet News*. Retrieved September 26, 2014.
- "[FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats](#)". *Wired Magazine*. July 18, 2007.

- Van Eck, Wim (1985). ["Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?"](#) (PDF). *Computers & Security*. 4 (4): 269–286. [CiteSeerX 10.1.1.35.1695](#). doi:[10.1016/0167-4048\(85\)90046-X](#).
- Kuhn, M.G. (2004). ["Electromagnetic Eavesdropping Risks of Flat-Panel Displays"](#) (PDF). 4th Workshop on Privacy Enhancing Technologies: 23–25.
- Risen, James; Lichtblau, Eric (June 16, 2009). ["E-Mail Surveillance Renews Concerns in Congress"](#). *New York Times*. pp. A1. Retrieved June 30, 2009.
- Ambinder, Marc (June 16, 2009). ["Pinwale And The New NSA Revelations"](#). *The Atlantic*. Retrieved June 30, 2009.
- Greenwald; Ewen, Glen; MacAskill (June 6, 2013). ["NSA Prism program taps in to user data of Apple, Google and others"](#) (PDF). *The Guardian*. Retrieved February 1, 2017.
- Sottek, T.C.; Kopfstein, Janus (July 17, 2013). ["Everything you need to know about PRISM"](#). *The Verge*. Retrieved February 13, 2017.
- Singel, Ryan (September 10, 2007). ["Rogue FBI Letters Hint at Phone Companies' Own Data Mining Programs – Updated"](#). *Threat Level*. *Wired*. Retrieved March 19, 2009.
- Roland, Neil (March 20, 2007). ["Mueller Orders Audit of 56 FBI Offices for Secret Subpoenas"](#). *Bloomberg News*. Retrieved March 19, 2009.
- Piller, Charles; Eric Lichtblau (July 29, 2002). ["FBI Plans to Fight Terror With High-Tech Arsenal"](#). *LA Times*. Retrieved March 14, 2009.
- Schneier, Bruce (December 5, 2006). ["Remotely Eavesdropping on Cell Phone Microphones"](#). *Schneier On Security*. Retrieved December 13, 2009.
- McCullagh, Declan; Anne Broache (December 1, 2006). ["FBI taps cell phone mic as eavesdropping tool"](#). *CNet News*. Archived from [the original](#) on November 10, 2013. Retrieved March 14, 2009.
- Odell, Mark (August 1, 2005). ["Use of mobile helped police keep tabs on suspect"](#). *Financial Times*. Retrieved March 14, 2009.
- ["Telephones"](#). *Western Regional Security Office (NOAA official site)*. 2001. Retrieved March 22, 2009.
- ["Can You Hear Me Now?"](#). *ABC News: The Blotter*. Archived from [the original](#) on August 25, 2011. Retrieved December 13, 2009.
- Coughlin, Kevin (December 13, 2006). ["Even if they're off, cellphones allow FBI to listen in"](#). *The Seattle Times*. Retrieved December 14, 2009.
- Hampton, Brittany (2012). ["From Smartphones to Stingrays: Can the Fourth Amendment Keep up with the Twenty-First Century Note"](#). *University of Louisville Law Review*. Fifty One: 159–176 – via *Law Journal Library*.
- ["Tracking a suspect by mobile phone"](#). *BBC News*. August 3, 2005. Retrieved March 14, 2009.
- Miller, Joshua (March 14, 2009). ["Cell Phone Tracking Can Locate Terrorists – But Only Where It's Legal"](#). *FOX News*. Archived from [the original](#) on March 18, 2009. Retrieved March 14, 2009.
- Samuel, Ian (2008). "Warrantless Location Tracking". *N.Y.U. Law Review*. [SSRN 1092293](#).
- Zetter, Kim (December 1, 2009). ["Threat Level Privacy, Crime and Security Online Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year"](#). *Wired Magazine: Threat Level*. Retrieved December 5, 2009.

- ["Greenstone Digital Library Software"](http://snowdenarchive.cjfe.org). snowdenarchive.cjfe.org. Retrieved June 3, 2017.
- Sanger, David (September 26, 2014). ["Signaling Post-Snowden Era, New iPhone Locks Out N.S.A"](#). New York Times. Retrieved November 1, 2014.
- Gellman, Barton (December 4, 2013). ["NSA tracking cellphone locations worldwide, Snowden documents show"](#). The Washington Post. Retrieved November 1, 2014.
- Nye, James (October 26, 2014). ["British spies can go through Americans' telephone calls and emails without warrant reveals legal challenge in the UK"](#). Mail Online. Retrieved November 1, 2014.
- ["Rise of Surveillance Camera Installed Base Slows"](#). May 5, 2016. Retrieved January 5, 2017.
- ["Smart cameras catch man in 60,000 crowd"](#). BBC News. April 13, 2018. Retrieved April 13, 2018.
- Spielman, Fran (February 19, 2009). ["Surveillance cams help fight crime, city says"](#). Chicago Sun Times. Retrieved March 13, 2009.[[permanent dead link](#)]
- Schorn, Daniel (September 6, 2006). ["We're Watching: How Chicago Authorities Keep An Eye On The City"](#). CBS News. Retrieved March 13, 2009.
- ["The Price of Privacy: How local authorities spent £515m on CCTV in four years"](#) (PDF). Big Brother Watch. February 2012. p. 30. Retrieved February 4, 2015.
- ["FactCheck: how many CCTV cameras?"](#). Channel 4 News. June 18, 2008. Retrieved May 8, 2009.
- ["You're being watched: there's one CCTV camera for every 32 people in UK – Research shows 1.85m machines across Britain, most of them indoors and privately operated"](#). The Guardian. March 2, 2011. Retrieved January 7, 2017; ["In the press: How the media is reporting the 1.85 million cameras story"](#). Security News Desk. March 3, 2011. Retrieved January 7, 2017.
- ["CCTV in London"](#) (PDF). Retrieved July 22, 2009.
- ["How many cameras are there?"](#). CCTV User Group. June 18, 2008. Archived from [the original](#) on October 23, 2008. Retrieved May 8, 2009.
- Den Haag. ["Camera surveillance"](#). Archived from [the original](#) on October 8, 2016. Retrieved December 2, 2016.
- Klein, Naomi (May 29, 2008). ["China's All-Seeing Eye"](#). Rolling Stone. Archived from [the original](#) on March 26, 2009. Retrieved March 20, 2009.
- ["Big Brother To See All, Everywhere"](#). CBS News. Associated Press. July 1, 2003. Retrieved September 26, 2014.
- Bonsor, K. (September 4, 2001). ["How Facial Recognition Systems Work"](#). Retrieved June 18, 2006.
- McNealy, Scott. ["Privacy is \(Virtually\) Dead"](#). Retrieved December 24, 2006.
- Roebuck, Kevin (October 24, 2012). [Communication Privacy Management](#). ISBN .
- ["WIKILEAKS: Surveillance Cameras Around The Country Are Being Used In A Huge Spy Network"](#). Retrieved October 5, 2016.
- ["EPIC Video Surveillance Information Page"](#). EPIC. Retrieved March 13, 2009.
- Hedgecock, Sarah (August 14, 2012). ["TrapWire: The Less-Than-Advertised System To Spy On Americans"](#). The Daily Beast. Retrieved September 13, 2012.
- Keefe, Patrick (March 12, 2006). ["Can Network Theory Thwart Terrorists?"](#). New York Times.
- Albrecht, Anders (March 3, 2008). ["Online Social Networking as Participatory Surveillance"](#). First Monday. **13** (3). Retrieved March 14, 2009.

- Fuchs, Christian (2009). [Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance](#) (PDF). Salzburg and Vienna: Forschungsgruppe Unified Theory of Information. ISBN . Retrieved July 28, 2012.
- Ethier, Jason. ["Current Research in Social Network Theory"](#). Northeastern University College of Computer and Information Science. Archived from the original on November 16, 2004. Retrieved March 15, 2009.
- Marks, Paul (June 9, 2006). ["Pentagon sets its sights on social networking websites"](#). New Scientist. Retrieved March 16, 2009.
- Kawamoto, Dawn (June 9, 2006). ["Is the NSA reading your MySpace profile?"](#). CNET News. Retrieved March 16, 2009.
- Ethier, Jason. ["Current Research in Social Network Theory"](#). Northeastern University College of Computer and Information Science. Archived from [the original](#) on February 26, 2015. Retrieved March 15, 2009.
- Ressler, Steve (July 2006). ["Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research"](#). Homeland Security Affairs. II (2). Retrieved March 14, 2009.
- ["DyDAn Research Blog"](#). DyDAn Research Blog (official blog of DyDAn). Retrieved December 20, 2009.
- Singel, Ryan (October 29, 2007). ["AT&T Invents Programming Language for Mass Surveillance"](#). Threat Level. Wired. Retrieved March 19, 2009.
- Singel, Ryan (October 16, 2007). ["Legally Questionable FBI Requests for Calling Circle Info More Widespread than Previously Known"](#). Threat Level. Wired. Retrieved March 19, 2009.
- Havenstein, Heather (September 12, 2008). ["One in five employers uses social networks in hiring process"](#). Computer World. Archived from [the original](#) on September 23, 2008. Retrieved March 14, 2009.
- Woodward, John; Christopher Horn; Julius Gatune; Aryn Thomas (2003). [Biometrics: A Look at Facial Recognition](#). RAND Corporation. ISBN . Retrieved March 15, 2009.
- Frank, Thomas (May 10, 2007). ["Face recognition next in terror fight"](#). USA Today. Retrieved March 16, 2009.
- Vlahos, James (January 2008). ["Surveillance Society: New High-Tech Cameras Are Watching You"](#). Popular Mechanics. Archived from [the original](#) on December 19, 2007. Retrieved March 14, 2009.
- Nakashima, Ellen (December 22, 2007). ["FBI Prepares Vast Database Of Biometrics: \\$1 Billion Project to Include Images of Irises and Faces"](#). Washington Post. pp. A01. Retrieved May 6, 2009.
- Arena, Kelly; Carol Cratty (February 4, 2008). ["FBI wants palm prints, eye scans, tattoo mapping"](#). CNN. Retrieved March 14, 2009.
- Gross, Grant (February 13, 2008). ["Lockheed wins \\$1 billion FBI biometric contract"](#). IDG News Service. InfoWorld. Retrieved March 18, 2009.
- ["LAPD: We Know That Mug"](#). Wired Magazine. Associated Press. December 26, 2004. Retrieved March 18, 2009.
- Mack, Kelly. ["LAPD Uses Face Recognition Technology To Fight Crime"](#). NBC4 TV (transcript from Officer.com). Archived from [the original](#) on March 30, 2010. Retrieved December 20, 2009.

- Willon, Phil (September 17, 2009). "[LAPD opens new high-tech crime analysis center](#)". *LA Times*. Retrieved December 20, 2009.
- Dotinga, Randy (October 14, 2004). "[Can't Hide Your Lying ... Face?](#)". *Wired Magazine*. Retrieved March 18, 2009.
- Boyd, Ryan. "[MQ-9 Reaper](#)". Retrieved October 5, 2016.
- Friedersdorf, Conor (March 10, 2016). "[The Rapid Rise of Federal Surveillance Drones Over America](#)". Retrieved October 5, 2016.
- Edwards, Bruce, "[Killington co-founder Sargent dead at 83](#)" [Archived](#) September 4, 2015, at the [Wayback Machine](#), *Rutland Herald*, November 9, 2012. Retrieved December 10, 2012.
- McCullagh, Declan (March 29, 2006). "[Drone aircraft may prowl U.S. skies](#)". *CNet News*. Retrieved March 14, 2009.
- Warwick, Graham (June 12, 2007). "[US police experiment with Insitu, Honeywell UAVs](#)". *FlightGlobal.com*. Retrieved March 13, 2009.
- La Franchi, Peter (July 17, 2007). "[UK Home Office plans national police UAV fleet](#)". *Flight International*. Retrieved March 13, 2009.
- "[No Longer Science Fiction: Less Than Lethal & Directed Energy Weapons](#)". *International Online Defense Magazine*. February 22, 2005. Retrieved March 15, 2009.
- "[HART Overview](#)" (PDF). IPTO (DARPA) – Official website. August 2008. Archived from [the original](#) (PDF) on December 5, 2008. Retrieved March 15, 2009.
- "[BAA 04-05-PIP: Heterogeneous Airborne Reconnaissance Team \(HART\)](#)" (PDF). Information Processing Technology Office (DARPA) – Official Website. December 5, 2003. Archived from [the original](#) (PDF) on November 27, 2008. Retrieved March 16, 2009.
- Sirak, Michael (November 29, 2007). "[DARPA, Northrop Grumman Move Into Next Phase of UAV Control Architecture](#)". *Defense Daily*. Archived from [the original](#) on March 9, 2012. Retrieved March 16, 2009.
- Saska, M.; Chudoba, J.; Preucil, L.; Thomas, J.; Loianno, G.; Tresnak, A.; Vonasek, V.; Kumar, V. Autonomous Deployment of Swarms of Micro-Aerial Vehicles in Cooperative Surveillance. In Proceedings of 2014 International Conference on Unmanned Aircraft Systems (ICUAS). 2014.
- Saska, M.; Vakula, J.; Preucil, L. [Swarms of Micro Aerial Vehicles Stabilized Under a Visual Relative Localization](#). In ICRA2014: Proceedings of 2014 IEEE International Conference on Robotics and Automation. 2014.
- Anthony, Denise (2017). "Toward a Sociology of Privacy". *Annual Review of Sociology*. **43** (1): 249–269. doi:10.1146/annurev-soc-060116-053643.
- [Hildebrandt, Mireille](#); Serge Gutwirth (2008). *Profiling the European Citizen: Cross Disciplinary Perspectives*. Dordrecht: Springer. [ISBN](#) .
- Clayton, Mark (February 9, 2006). "[US Plans Massive Data Sweep](#)". *Christian Science Monitor*. Retrieved March 13, 2009.
- Flint, Lara (September 24, 2003). "[Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power](#)". *The Center For Democracy & Technology* (official site). Archived from [the original](#) on March 8, 2009. Retrieved March 20, 2009.
- "[National Network of Fusion Centers Raises Specter of COINTELPRO](#)". *EPIC Spotlight on Surveillance*. June 2007. Retrieved March 14, 2009.

- anonymous (January 26, 2006). ["Information on the Confidential Source in the Auburn Arrests"](#). Portland Indymedia. Archived from [the original](#) on December 5, 2008. Retrieved March 13, 2009.
- Myers, Lisa (December 14, 2005). ["Is the Pentagon spying on Americans?"](#). NBC Nightly News. msnbc.com. Retrieved March 13, 2009.
- ["The Use of Informants in FBI Domestic Intelligence Investigations"](#). Final Report: Book III, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. April 23, 1976. pp. 225–270. Retrieved March 13, 2009.
- ["Secret Justice: Criminal Informants and America's Underground Legal System | Prison Legal News"](#). www.prisonlegalnews.org. Retrieved October 5, 2016.
- Ross, Brian (July 25, 2007). ["FBI Proposes Building Network of U.S. Informants"](#). Blotter. ABC News. Retrieved March 13, 2009.
- ["U.S. Reconnaissance Satellites: Domestic Targets"](#). National Security Archive. Retrieved March 16, 2009.
- Block, Robert (August 15, 2007). ["U.S. to Expand Domestic Use Of Spy Satellites"](#). Wall Street Journal. Retrieved March 14, 2009.
- Gorman, Siobhan (October 1, 2008). ["Satellite-Surveillance Program to Begin Despite Privacy Concerns"](#). The Wall Street Journal. Retrieved March 16, 2009.
- ["Fact Sheet: National Applications Office"](#). Department of Homeland Security (official website). August 15, 2007. Archived from [the original](#) on March 11, 2009. Retrieved March 16, 2009.
- Warrick, Joby (August 16, 2007). ["Domestic Use of Spy Satellites To Widen"](#). Washington Post. pp. A01. Retrieved March 17, 2009.
- Shrader, Katherine (September 26, 2004). ["Spy imagery agency watching inside U.S."](#) USA Today. Associated Press. Retrieved March 17, 2009.
- Kappeler, Victor. ["Forget the NSA: Police May be a Greater Threat to Privacy"](#).
- ["Section 100i – IMS I-Catcher"](#) (PDF), The German Code Of Criminal Procedure, 2014, pp. 43–44, archived from [the original](#) (PDF) on September 25, 2015, retrieved November 27, 2015
- ["Two Stories Highlight the RFID Debate"](#). RFID Journal. July 19, 2005. Retrieved March 23, 2012.
- Lewan, Todd (July 21, 2007). ["Microchips in humans spark privacy debate"](#). USA Today. Associated Press. Retrieved March 17, 2009.
- McCullagh, Declan (January 13, 2003). ["RFID Tags: Big Brother in small packages"](#). CNET News. Retrieved July 24, 2012.
- Gardener, W. David (July 15, 2004). ["RFID Chips Implanted In Mexican Law-Enforcement Workers"](#). Information Week. Retrieved March 17, 2009.
- Campbell, Monica (August 4, 2004). ["Law enforcement in Mexico goes a bit bionic"](#). Christian Science Monitor. Retrieved March 17, 2009.
- Lyman, D., Micheal. *Criminal Investigation: The Art and the Science*. 6th ed. Pearson, 2010. p249
- Crowder, Stan, and Turvery E. Brent. *Ethical Justice: Applied Issues for Criminal Justice Students and Professionals*. 1st ed. Academic Press, 2013. p150. Print.
- Claburn, Thomas (March 4, 2009). ["Court Asked To Disallow Warrantless GPS Tracking"](#). Information Week. Retrieved March 18, 2009.

- Hilden, Julie (April 16, 2002). ["What legal questions are the new chip implants for humans likely to raise?"](#). CNN.com (FindLaw). Retrieved March 17, 2009.
- Wolf, Paul. ["COINTELPRO"](#). (online collection of historical documents). Retrieved March 14, 2009.
- ["U.S. Army Intelligence Activities"](#) (PDF). Archived from [the original](#) (PDF) on August 8, 2015. Retrieved 25 May 2015.
- ["Domestic CIA and FBI Mail Opening Programs"](#) (PDF). Final Report: Book III, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. April 23, 1976. pp. 559–678. Archived from [the original](#) (PDF) on May 5, 2011. Retrieved March 13, 2009.
- Goldstein, Robert (2001). [Political Repression in Modern America](#). [University of Illinois Press](#). ISBN .
- Hauser, Cindy E.; McCarthy, Michael A. (July 1, 2009). "Streamlining 'search and destroy': cost-effective surveillance for invasive species management". *Ecology Letters*. **12** (7): 683–692. doi:[10.1111/j.1461-0248.2009.01323.x](#). ISSN 1461-0248. PMID [19453617](#).
- Holden, Matthew H.; Nyrop, Jan P.; Ellner, Stephen P. (June 1, 2016). "The economic benefit of time-varying surveillance effort for invasive species management". *Journal of Applied Ecology*. **53** (3): 712–721. doi:[10.1111/1365-2664.12617](#). ISSN 1365-2664.
- Flewwelling, Peter; Nations, Food and Agriculture Organization of the United (January 1, 2003). [Recent Trends in Monitoring Control and Surveillance Systems for Capture Fisheries](#). Food & Agriculture Org. ISBN .
- Yang, Rong; Ford, Benjamin; Tambe, Milind; Lemieux, Andrew (January 1, 2014). [Adaptive Resource Allocation for Wildlife Protection Against Illegal Poachers](#). Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems. AAMAS '14. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems. pp. 453–460. ISBN .
- Mörner, T.; Obendorf, D. L.; Artois, M.; Woodford, M. H. (April 1, 2002). "Surveillance and monitoring of wildlife diseases". *Revue Scientifique et Technique (International Office of Epizootics)*. **21** (1): 67–76. doi:[10.20506/rst.21.1.1321](#). ISSN 0253-1933. PMID [11974631](#).
- [Deviant Behaviour – Socially accepted observation of behaviour for security](#), Jeroen van Rest
- Sprenger, Polly (January 26, 1999). ["Sun on Privacy: 'Get Over It'"](#). Wired Magazine. Retrieved March 20, 2009.
- Baig, Edward; Marcia Stepanek; Neil Gross (April 5, 1999). ["Privacy"](#). Business Week. Archived from [the original](#) on October 17, 2008. Retrieved March 20, 2009.
- [Solove, Daniel](#) (2007). "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy". *San Diego Law Review*. **44**: 745. SSRN [998565](#).
- ["Is the U.S. Turning Into a Surveillance Society?"](#). American Civil Liberties Union. Retrieved March 13, 2009.
- ["Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society"](#) (PDF). American Civil Liberties Union. January 15, 2003. Retrieved March 13, 2009.
- ["Against the collection of private data: The unknown risk factor"](#). March 8, 2012.
- ["Privacy fears over online surveillance footage broadcasts in China"](#). December 13, 2017.

- Marx, G. T., & Muschert, G. W. (2007). [Personal information, borders, and the new surveillance studies Archived](#) August 11, 2017, at the [Wayback Machine](#). *Annual Review of Law and Social Science*, 3, 375–395.
- Agre, Philip E. (2003), "[Your Face is not a bar code: arguments against automatic face recognition in public places](#)". Retrieved November 14, 2004.
- Foucault, Michel (1979). *Discipline and Punish*. New York: Vintage Books. pp. 201–202.
- Chayko, Mary (2017). *Superconnected: the internet, digital media, and techno-social life*. New York, NY: Sage Publications.
- Nishiyama, Hidefumi (2017). "[Surveillance as Race Struggle: On Browne's Dark Matters](#)". *Theory & Event*. Johns Hopkins University Press. 20 (1): 280–285 – via Project MUSE.
- Browne, Simone (October 2, 2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press Books. p. 224. [ISBN](#) .
- Court of Appeal, Second District, Division 6, California. (July 30, 2008). "[People vs. Diaz](#)". FindLaw. Retrieved February 1, 2017.
- California Fourth District Court of Appeal (June 25, 2014). "[Riley v. California](#)". Oyez – IIT Chicago-Kent College of Law. Retrieved February 1, 2013.
- "[The Secrets of Countersurveillance](#)". *Security Weekly*. June 6, 2007.
- Birch, Dave (July 14, 2005). "[The age of sousveillance](#)". *The Guardian*. London. Retrieved August 6, 2007.
- Eggers, David (2013). *The Circle*. New York: Alfred A. Knopf, McSweeney's Books. pp. 288, 290–291, 486. [ISBN](#) .

How Artists And Fans Stopped Facial Recognition From Invading Music Festivals

The surveillance dystopia of our nightmares is not inevitable — and the way we kept it out of concerts and festivals is a lesson for the future.

Imagine showing up at a music festival or concert and being required to stand in front of a device that scans and analyzes your face.

Once your facial features are mapped and stored in a database, a computer algorithm could then decide that you are drunk and should be denied entry, or that you look “suspicious” and should be flagged for additional screening. If you make it through security, facial recognition technology could then be used to track the minute details of your movements once inside.

Face scanning software could be used to police behavior — constantly scanning the crowd for drug use or rule-breaking — or for strictly commercial purposes, like showing you targeted ads, monitoring which artists you came to see, or tracking how many times you go to the bar or the bathroom. Festival organizers could be forced to hand this trove of sensitive biometric data over to law enforcement or immigration authorities, and armed officers could pull people out of the crowd because they have an outstanding

warrant or a deportation order. If you're a person of color, or your gender presentation doesn't conform to the computer's stereotypes, you'd be [more likely](#) to be falsely flagged by the system.

This surveillance nightmare almost became a reality at US music events. Industry giants like Ticketmaster [invested](#) money in companies like Blink Identity, a startup run by ex-defense contractors who [helped build](#) the US military's facial recognition system in Afghanistan. These vendors, and the venture capitalists who backed them, saw the live music industry as a huge potential market for biometric surveillance tech, marketed as a convenient ticketing option to concertgoers.

But now, it seems they'll be sorely disappointed — and there's a lesson in the story of how we dashed their dystopian profit dreams. A future where we are constantly subjected to corporate and government surveillance is not inevitable, but it's coming fast unless we act now.

Over the last month, artists and fans waged a grassroots war to stop Orwellian surveillance technology from invading live music events. Today we declare victory. [Our campaign](#) pushed more than 40 of the world's largest music festivals — like Coachella, Bonnaroo, and SXSW — to go on the record and state clearly that they have no plans to use facial recognition technology at their events. Facing backlash, Ticketmaster [all but](#) threw Blink Identity under the bus, distancing itself from the surveillance startup it boasted about partnering with just a year ago. This victory is the first major blow to the spread of commercial facial recognition in the United States, and its significance cannot be overstated.

In a few short weeks, using basic grassroots activism tactics like online petitions, social media pressure, and an [economic boycott](#) targeting festival sponsors, artists and fans killed the idea of facial recognition at US music festivals. Now we need to do the same for sporting events, transportation, public housing, schools, law enforcement agencies, and all public places. And there's no time to lose.

Facial recognition is spreading like an epidemic. It's being [deployed](#) by police departments in cities like Detroit, disproportionately targeting low-income people of color. Immigration and Customs Enforcement (ICE) are [using it](#) to systematically comb through millions of driver's license photos and target undocumented people for apprehension and deportation. Cameras equipped with facial recognition software are [scanning](#) thousands of people's faces right now in shopping malls, casinos, big box stores, and hotels. Schools are [using it](#) to police our children's attendance and behavior, with black and Latinx students most likely to end up on watch lists. Major airlines are rapidly [adopting it](#) as part of the boarding process. France is [about to](#) institute a national facial recognition database. Police and corporate developers in the UK are defending their use of the tech. In China, where authorities have already used facial recognition [to arrest](#) people out of crowds at music festivals, the government is [making](#) a face scan mandatory to access the Internet.

But in almost all of these cases, facial recognition is still in its early stages. It's an experiment. And we're the test subjects. If we accept ubiquitous biometric monitoring and normalize the idea of getting our faces scanned to get on a plane or pick up our kids from school, the experiment works and our fate is sealed. But if we organize — if we refuse to be lab rats in a digital panopticon — we can avert a future where all human movements and associations are tracked by artificial intelligence algorithms trained to look for and punish deviations from authoritarian norms.

Opposition to facial recognition is spreading almost as quickly as the tech itself. More than 30 organizations, ranging from the Council on American Islamic Relations to Greenpeace, have endorsed Fight for the Future's [BanFacialRecognition.com](#) campaign, pushing lawmakers at the local, state, and federal level to halt face surveillance. [Four cities](#) have already banned government use of biometric spy tech. California [banned](#) its use in police body cameras. States like Michigan, Massachusetts and New York are [considering](#) legislation. Sweden recently [banned](#) facial recognition in schools after getting slapped with a fine under the GDPR data privacy regime. Leading 2020 candidates like Bernie Sanders and Beto O'Rourke have [echoed](#) grassroots calls for a ban, and there's rare [bipartisan](#) agreement in Congress, where lawmakers as diametrically opposed as Alexandria Ocasio-Cortez and Jim Jordan agree that facial recognition poses a unique threat to privacy and civil liberties.

When it comes to automated and insidious invasions of our personal lives and most basic rights, tech lobbyists and politicians sell a calculated brand of cynicism. They want us to believe that the widespread use of deeply creepy technology like facial recognition is a forgone conclusion, that we should get used to it, and that the only questions to address are how, where, and how quickly to roll it out. We can prove them wrong, by channeling our ambient anxiety and online outrage into meaningful action and political power.

Surveillance profiteers who hope to make a lot of money selling facial recognition software to governments and private interests are now on high alert. They're watching closely for public reactions, running tests to see just how much intrusive monitoring we're willing to put up with. They're manipulatively [calling for regulation](#) — a trap intended to assuage public fears while hastening adoption. They're promising that facial recognition can be done in an “opt-in,” manner, [ignoring](#) the inherent [dangers](#) in corporate harvesting and storing of biometric data. But we can draw a line in the sand now, and shut down this unethical human experiment by pushing for legislation to ban facial recognition, and refusing to support corporations who use it.

We have a chance to stop the proliferation of surveillance technology that rivals nuclear weapons in the threat that it poses to the future of humanity. The clock is ticking.

THE LATEST DANGERS OF FACE-TRACKING

Face-tracking harvesters grab one picture of you and then use AI to find every other digital picture of you on the web. They open every social media post, resume, news clipping, dating account etc. and sell the full dossier on you to Axiom, the NSA, Political manipulators etc. and hack your bank accounts and credit cards. Never put an unsecured photo of yourself online. Anybody can take a screen grab of your photo on here, put it in Google's or Palantir's reverse image search, find all your other images and social media accounts online and get into your bank account or medical records in 30 minutes. The fact of the internet's failed security is in the headlines every day. The danger of posting pictures on the web is pretty clearly covered in every major newspaper. Fusion GPS, Black Cube and political operatives harvest every photo on here every hour and use the data to spy on people for political dirty tricks. The FBI, CIA, NSA and most 3-letter law enforcement spy operations copy everything on this site and analyze it. Don't you wonder why you never see anybody famous, political, in public service or in law on a dating site? Read Edward Snowden's book 'Permanent Record' or any weekly report at Krebs On Security. Huge numbers of

the profiles on here are fake Nigerian scammer type things. 2D pictures have no bearing on 3D experiences of people in person. I am only interested in meeting people in person. Nobody has ever been killed at a Starbucks! There is nothing unsafe about meeting at a highly public Starbucks or Peets. I learned my lessons. There are hundreds of thousands of bait profiles on here. The real people show up for the coffee. The fake ones in Nigeria, and the political spies never show up in person and have a million carefully prepared excuses why not.

For example: Yandex is by far the best reverse image search engine, with a scary-powerful ability to recognize faces, landscapes, and objects. This Russian site draws heavily upon user-generated content, such as tourist review sites (e.g. FourSquare and TripAdvisor) and social networks (e.g. dating sites), for remarkably accurate results with facial and landscape recognition queries. To use Yandex, go to images.yandex.com, then choose the camera icon on the right. From there, you can either upload a saved image or type in the URL of one hosted online.

If you get stuck with the Russian user interface, look out for Выберите файл (Choose file), Введите адрес картинки (Enter image address), and Найти (Search). After searching, look out for Похожие картинки (Similar images), and Ещё похожие (More similar). The facial recognition algorithms used by Yandex are shockingly good. Not only will Yandex look for photographs that look similar to the one that has a face in it, but it will also look for other photographs of the same person (determined through matching facial similarities) with completely different lighting, background colors, and positions. Google and Bing also look for other photographs showing a person with similar clothes and general facial features, Yandex will search for those matches, and also other photographs of a facial match.

Any stranger could snap your picture on the sidewalk or on Match.com then use an app to quickly discover your name, address and other details? A startup called Clearview AI has made that possible, and its app is currently being used by hundreds of law enforcement agencies in the US, including the FBI, says a report in The New York Times.

The app, says the Times, works by comparing a photo to a database of more than 3 billion pictures that Clearview says it's scraped off Facebook, Venmo, YouTube and other sites. It then serves up matches, along with links to the sites where those database photos originally appeared. A name might easily be unearthed, and from there other info could be dug up online.

The size of the Clearview database dwarfs others in use by law enforcement. The FBI's own database, which taps passport and driver's license photos, is one of the largest, with over 641 million images of US citizens.

Political spies have even better programs than this do...watch out! The web is not safe!

-
You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. PrivacyTools provides services, tools and knowledge to protect your privacy against global mass surveillance.

Privacy Tools

[Prefer the classic site? View a single-page layout.](#)

Providers

Discover privacy-centric online services, including email providers, VPN operators, DNS administrators, and more!

Web Browsers

Find a web browser that respects your privacy, and discover how to harden your browser against tracking and leaks.

Software

Discover a variety of open source software built to protect your privacy and keep your digital data secure.

Operating Systems

Find out how your operating system is compromising your privacy, and what simple alternatives exist.

PrivacyTools Services

The PrivacyTools team is proud to launch a variety of privacy-centric online services, including a Mastodon instance, search engine, and more!

Privacy? I don't have anything to hide.

Over the last 16 months, as I've debated this issue around the world, every single time somebody has said to me, "I don't really worry about invasions of privacy because I don't have anything to hide." I always say the same thing to them. I get out a pen, I write down my email address. I say, "Here's my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting. After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." **Not a single person has taken me up on that offer.**

[Why privacy matters - TED Talk](#)

The primary reason for window curtains in our house, is to stop people from being able to see in. The reason we don't want them to see in is because we consider much of what we do inside our homes to be private. Whether that be having dinner at the table, watching a movie with your kids, or even engaging in intimate or sexual acts with your partner. None of these things are illegal by any means but even knowing this, we still keep the curtains and blinds on our windows. We clearly have this strong desire for privacy when it comes to our personal life and the public.

[The Crypto Paper](#)

[...] But saying that you don't need or want privacy because you have nothing to hide is to assume that no one should have, or could have, to hide anything -- including their immigration status, unemployment history, financial history, and health records. You're assuming that no one, including yourself, might object to revealing to anyone information about their religious beliefs, political affiliations, and sexual activities, as casually as some choose to reveal their movie and music tastes and reading preferences.

[Permanent Record](#)

Read also:

- [Nothing to hide argument \(Wikipedia\)](#)
- [How do you counter the "I have nothing to hide?" argument? \(reddit.com\)](#)
- ['I've Got Nothing to Hide' and Other Misunderstandings of Privacy \(Daniel J. Solove - San Diego Law Review\)](#)

Quotes

Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say. Or that you don't care about freedom of the press because you don't like to read. Or that you don't care about freedom of religion because you don't believe in God. Or that you don't care about the freedom to peacefully assemble because you're a lazy, antisocial agoraphobe.

[Permanent Record](#)

The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards. I don't want to live in a society that does these sort of things... I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under.

[The Guardian](#)

We all need places where we can go to explore without the judgmental eyes of other people being cast upon us, only in a realm where we're not being watched can we really test the limits of who we want to be. It's really in the private realm where dissent, creativity and personal exploration lie.

[Huffington Post](#)

More Privacy Resources

Guides

- [Surveillance Self-Defense by EFF](#) - Guide to defending yourself from surveillance by using secure technology and developing careful practices.
- [The Crypto Paper](#) - Privacy, Security and Anonymity for Every Internet User.
- [Email Self-Defense by FSF](#) - A guide to fighting surveillance with GnuPG encryption.
- [The Ultimate Privacy Guide](#) - Excellent privacy guide written by the creators of the bestVPN.com website.
- [IVPN Privacy Guides](#) - These privacy guides explain how to obtain vastly greater freedom, privacy and anonymity through compartmentalization and isolation.
- [The Ultimate Guide to Online Privacy](#) - Comprehensive "Ninja Privacy Tips" and 150+ tools.

Information

- [Freedom of the Press Foundation](#) - Supporting and defending journalism dedicated to transparency and accountability since 2012.
- [Erfahrungen.com](#) - German review aggregator website of privacy-related services.
- [Open Wireless Movement](#) - a coalition of Internet freedom advocates, companies, organizations, and technologists working to develop new wireless technologies and to inspire a movement of Internet openness.
- [privacy.net](#) - What does the US government know about you?
- [r/privacytoolsIO Wiki](#) - Our Wiki on reddit.com.
- [Security Now!](#) - Weekly Internet Security Podcast by Steve Gibson and Leo Laporte.
- [TechSNAP](#) - Weekly Systems, Network, and Administration Podcast. Every week TechSNAP covers the stories that impact those of us in the tech industry.
- [Terms of Service; Didn't Read](#) - "I have read and agree to the Terms" is the biggest lie on the web. We aim to fix that.
- [The Great Cloudwall](#) - Critique and information on why to avoid Cloudflare, a big company with a huge portion of the internet behind it.

Tools

- [ipleak.net](#) - IP/DNS Detect - What is your IP, what is your DNS, what informations you send to websites.

- [The ultimate Online Privacy Test Resource List](#) - A collection of Internet sites that check whether your web browser leaks information.
- [PRISM Break](#) - We all have a right to privacy, which you can exercise today by encrypting your communications and ending your reliance on proprietary services.
- [Security in-a-Box](#) - A guide to digital security for activists and human rights defenders throughout the world.
- [SecureDrop](#) - An open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. It was originally created by the late Aaron Swartz and is currently managed by Freedom of the Press Foundation.
- [Reset The Net - Privacy Pack](#) - Help fight to end mass surveillance. Get these tools to protect yourself and your friends.
- [Security First](#) - Umbrella is an Android app that provides all the advice needed to operate safely in a hostile environment.
- [Osalt](#) - A directory to help you find open source alternatives to proprietary tools.
- [AlternativeTo](#) - A directory to help find alternatives to other software, with the option to only show open source software

Note: Just being open source does not make software secure!

Participate with suggestions and constructive criticism

It's important for a website like PrivacyTools to stay up-to-date. Keep an eye on software updates for the applications listed on our site. Follow recent news about providers that we recommend. We try our best to keep up, but we're not perfect and the internet is changing fast. If you find an error, or you think a provider should not be listed here, or a qualified service provider is missing, or a browser plugin is not the best choice anymore, or anything else... **Talk to us please.** You can also find us on [our own Mastodon instance](#) or on [Matrix](#) at `#general:privacytools.io`.

WASHINGTON (AP) — A government watchdog is launching a nationwide probe into how marketers may be getting seniors' personal Medicare information aided by apparent misuse of a government system, officials said Friday.

The audit will be formally announced next week said Tesia Williams, a spokeswoman for the Health and Human Services inspector general's office. It follows a narrower probe which found that an electronic system for pharmacies to verify Medicare coverage was being used for potentially inappropriate searches seemingly tied to marketing. It raised red flags about possible fraud.

The watchdog agency's decision comes amid [a wave of relentlessly efficient telemarketing scams](#) targeting Medicare recipients and involving everything from back braces to [DNA cheek swabs](#).

For years, seniors have been admonished not to give out their Medicare information to people they don't know. But [a report on the inspector general's initial probe](#), also released Friday, details how sensitive details can still get to marketers. It can happen even when a Medicare beneficiary thinks he or she is dealing with a trustworthy entity such as a pharmacy or doctor's office.

Key personal details gleaned from Medicare's files can then be cross-referenced with databases of individual phone numbers, allowing marketers to home in with their calls.

The initial audit focused on 30 pharmacies and other service providers that were frequently pinged a Medicare system created for drugstores.

The electronic system is intended to be used for verifying a senior's eligibility at the sales counter. It can validate coverage and personal details on millions of individuals. Analyzing records that covered 2013-15, investigators discovered that most of the audited pharmacies, along with a software company and a drug compounding service also scrutinized, weren't necessarily filling prescriptions.

Instead, they appeared to have been tapping into the system for potentially inappropriate marketing.

Medicare stipulates that the electronic queries — termed “E1 transactions”— are supposed to be used to bill for prescriptions. But investigators found that some pharmacies submitted tens of thousands of queries that could not be matched to prescriptions. In one case, a pharmacy submitted 181,963 such queries but only 41 could be linked to prescriptions.

The report found that on average 98% of the electronic queries from 25 service providers in the initial audit “were not associated with a prescription.” The inspector general's office did not identify the pharmacies and service providers.

Pharmacies are able to access coverage data on Medicare recipients by using a special provider number from the government.

But investigators found that four of the pharmacies they audited allowed marketing companies to use their provider numbers to ping Medicare. “This practice of granting telemarketers access to E1 transactions, or using E1 transactions for marketing purposes puts the privacy of the beneficiaries' (personal information) at risk,” the report said.

Some pharmacies also used seniors' information to contact doctors treating those beneficiaries to see if they would write prescriptions. Citing an example, the report said, “The doctor often informed (one) provider that the beneficiary did not need the medication.”

The inspector general's office said it is investigating several health care providers for alleged fraud involving E1 transactions. Inappropriate use of Medicare's eligibility system is probably just one of many paths through which telemarketers and other sales outfits can get sensitive personal information about beneficiaries, investigators said.

A group representing independent drugstores expressed support for the investigation. “It's about time,” said Douglas Hoey, CEO of the National Community Pharmacists Association. “We welcome the effort to clean up this misbehavior.” Hoey said some local pharmacists have complained of what appear to be sophisticated schemes to poach customers who take high-cost drugs.

The watchdog agency began looking into the matter after the Centers for Medicare and Medicaid Services, or CMS, asked for an audit of a mail order pharmacy's use of Medicare's eligibility verification system.

In a formal response to the report, CMS Administrator Seema Verma said CMS retooled its verification system last year so it automatically kicks out queries that aren't coming from a pharmacy. More than a quarter-million such requests have been rejected, she wrote.

Medicare is committed to ensuring that the system is used appropriately, Verma added. The agency can revoke access for pharmacies that misuse the privilege and is exploring other enforcement options.

The inspector general's office acknowledged Medicare's countermeasures but said it wants to see how effective they've been.

Health care fraud is a pervasive problem that costs taxpayers tens of billions of dollars a year. Its true extent is unknown, and some cases involve gray areas of complex payment policies.

In recent years, Medicare has gotten more sophisticated, adapting techniques used by financial companies to try to head off fraud. Law enforcement coordination has grown, with strike forces of federal prosecutors and agents, along with state counterparts, specializing in health care investigations.

Officials gave no timetable for completing the audit.

<https://techcrunch.com/2022/04/22/lapsus-hackers-t-mobile/>

Lapsus\$ hackers targeted T-Mobile source code in latest data breach

Apr 22, 2022 ... A group of employees in a **T-Mobile** store in New York. ... The Lapsus\$ **hacking** group has claimed another victim: U.S. telecom giant **T-Mobile**. T- ...

<https://www.vice.com/en/article/k7w9mv/tmobile-hacked-bought-data-mandiant>

T-Mobile Secretly Bought Its Customer Data from Hackers to ... - VICE

Apr 12, 2022 ... After **hackers** targeted **T-Mobile** in August, **T-Mobile** hired a third-party firm that went undercover and bought exclusive access to the **data**.

<https://www.theverge.com/2022/4/23/23038570/lapsus-hackers-target-t-mobile-source-code-multiple-breaches-cybersecurity>

Lapsus\$ hackers breached T-Mobile's systems and stole its source ...

Apr 23, 2022 ... The Lapsus\$ **hacking** group stole **T-Mobile's** source code in a series of breaches that took place in March, as first reported by Krebs on ...

<https://www.cnet.com/tech/services-and-software/t-mobile-data-breach-2021-heres-what-it-means-for-securing-your-data/>

T-Mobile data breach 2021: Here's what it means for securing your ...

Sep 9, 2021 ... The alleged **hacker** behind **T-Mobile's** latest cyberattack has spoken out about the August **hack**. The breach includes names, driver's license ...

<https://www.wired.com/story/t-mobile-hack-data-phishing/>

The T-Mobile Data Breach Is One You Can't Ignore | WIRED

Aug 16, 2021 ... **T-Mobile** confirmed on Monday that a breach had occurred but not whether customer **data** had been compromised. "We have been working around the ...

<https://www.zdnet.com/article/t-mobile-hack-everything-you-need-to-know/>

T-Mobile hack: Everything you need to know - ZDNet

Aug 28, 2021 ... The investigation into the January incident found that **hackers** accessed around 200,000 customer details such as phone numbers, the number of ...

<https://www.washingtonpost.com/technology/2021/08/19/t-mobile-data-breach-what-to-do/>

What to do if you're concerned about the T-Mobile data breach

Aug 20, 2021 ... **T-Mobile** on Aug. 18 said an investigation into a **data** breach revealed that **hackers** obtained personal information belonging to more than 40 ...

<https://www.safehome.org/news/t-mobile-data-breach/>

T-Mobile Data Breach: Your T-Mobile Account Has Been Hacked ...

Dec 3, 2021 ... A little over two weeks ago, the news dropped like a bomb. **T-Mobile**, the global telecommunications giant, had been **hacked**. And **hacked** badly.

<https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/>

Leaked Chats Show LAPSUS\$ Stole T-Mobile Source Code

Apr 22, 2022 ... The logs show LAPSUS\$ breached **T-Mobile** multiple times in March, ... more than 50 terabytes of **data** stored on the ministry's **hacked** servers.

<https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105>

T-Mobile Hacker Who Stole Data on 50 Million Customers

Aug 27, 2021 ... The **hacker** who is

<https://www.idstrong.com/sentinel/the-saga-of-t-mobile-data-breach/>

T-Mobile Data breach: The infamous Cyber Attack - IDStrong

T-Mobile later admitted the **hackers** also got away with encrypted passwords. The in-house **T-Mobile** security team shut down the breach quickly and notified ...

<https://www.classlawgroup.com/consumer-protection/t-mobile-data-breach-lawsuit/>

T-Mobile Data Breach Lawsuit 2022 | Join 1000s of others

News of a massive **data** breach began to make waves on Sunday, August 15, when Vice.com reported that **hackers** posted on an underground forum claiming to have **data** ...

<https://www.wsj.com/articles/t-mobile-data-hack-what-we-know-and-what-you-need-to-do-11629404953>

T-Mobile Data Hack: What We Know and What You Need to Do - WSJ

Aug 20, 2021 ... The breach of **T-Mobile** US Inc. TMUS 1.92%△ allowed **hackers** to steal information about more than 54 million people and potentially sell the ...

<https://www.hackread.com/t-mobiles-hacked-lapsus-steals-source-code-systems-data/>

Lapsus\$ Hackers Stole T-Mobile's Source Code and Systems Data

Apr 25, 2022 ... **T-Mobile** has acknowledged the breach which occurred before police arrested some of the members of the Lapsus\$ **hacking** group last month.

<https://apnews.com/article/technology-business-hacking-fce56107ed5982bbbbc6b1acdefb5ebc>

T-Mobile CEO says "truly sorry" for hack of 50M users' data | AP News

Aug 27, 2021 ... BELLEVUE, Wash. (AP) — **T-Mobile** says it has notified nearly all of the millions of customers whose personal **data** was stolen and that it is ...

<https://www.securitymagazine.com/articles/97492-t-mobile-is-latest-lapsus-breach-victim>

T-Mobile is latest Lapsus\$ breach victim | Security Magazine

Apr 25, 2022 ... U.S. telecom **T-Mobile** has confirmed that it is the latest victim of the Lapsus\$ ransomware group. Security journalist Brian Krebs first revealed ...

<https://www.nytimes.com/2021/08/18/business/tmobile-data-breach.html>

T-Mobile Says Hack Exposed Personal Data of 40 Million People

Aug 18, 2021 ... A cyberattack on **T-Mobile** exposed the information of more than 40 million people, with stolen files including names, birthdays and social ...

<https://www.forthepeople.com/mass-arbitration-lawsuits/t-mobile-data-breach/>

[T-Mobile Data Breach Lawsuit | Morgan & Morgan Law Firm](#)

T-Mobile recently confirmed that their company was the subject of a malicious **data** breach that exposed the personal information of over 50 million people ...

<https://www.techradar.com/news/t-mobile-tried-to-buy-stolen-customer-data-back-but-failed>

[T-Mobile tried to buy stolen customer data back, but failed | TechRadar](#)

Apr 13, 2022 ... After being paid \$200k for the database, SubVirt and the other **hackers** behind the breach continued to try and sell the company's stolen customer ...

<https://www.pcgamer.com/that-nvidia-hacking-group-went-after-t-mobile-but-the-fbi-snagged-their-data-before-they-could-use-it/>

[That Nvidia-hacking group went after T-Mobile but the FBI snagged ...](#)

Apr 26, 2022 ... The **hacking** group is supposed to have tried to once again breach **T-Mobile's** systems and download the stolen **data**, however, found they were ...

<https://www.forthepeople.com/mass-arbitration-lawsuits/t-mobile-data-breach/>

[T-Mobile Data Breach Lawsuit | Morgan & Morgan Law Firm](#)

T-Mobile Data Breach Lawsuit ... **T-Mobile** recently confirmed that their company was the subject of a malicious data breach that exposed the personal information ...

<https://milberg.com/news/t-mobile-faces-class-action-lawsuits-following-data-breach-affecting-millions/>

[T-mobile Faces Class Action Lawsuits Following Data Breach ...](#)

Labeled as Tom's Guide's "overall best cell phone carrier," **T-mobile** now faces two **class action lawsuits** impacting millions of current and former network ...

<https://www.classaction.org/t-mobile-data-breach-lawsuit-2021>

[T-Mobile Data Breach Lawsuit 2021 | What To Do - ClassAction.org](#)

May 2, 2022 ... Attorneys working with **ClassAction.org** are gathering current and former **T-Mobile** customers to take action against the company over the 2021 data ...

<https://www.law.com/2022/01/25/t-mobile-significant-portion-of-data-breach-class-members-subject-to-arbitration/>

[T-Mobile: 'Significant Portion' of Data Breach Class Members ...](#)

Jan 25, 2022 ... **T-Mobile** already filed motions to arbitrate in at least two cases, which are now part of the proceeding that the U.S. Judicial Panel on ...

<https://fairshake.com/t-mobile/lawsuit/>

Lawsuits Against T-Mobile - FairShake

The **lawsuit**, filed by a **T-Mobile** customer on April 15 and seeking **class-action** status, alleges that the company's no-contract plans are deceptive. **T-Mobile** says ...

<https://lynchcarpenter.com/t-mobile-data-breach-class-action-lawsuit/>

T-Mobile Data Breach - Class Action Lawsuit - Lynch Carpenter LLP

On August 17, 2021, **T-Mobile** was alerted of an individual trying to sell stolen customer data in an online forum. This data breach affects more than 50 million ...

<https://topclassactions.com/case-tracker/t-mobile-data-breach-class-action/>

T-Mobile Data Breach Class Action

Jan 21, 2022 ... The **class action lawsuit** was filed October 7, 2021. Deadline to file a claim: TBD; Proof of Purchase Required: No; Potential Individual Reward: ...

<https://topclassactions.com/lawsuit-settlements/consumer-products/cellphones/t-mobile-class-action-claims-sprint-merger-costs-verizon-att-customers-due-to-declining-competition/>

T-Mobile class action claims Sprint merger costs Verizon, AT&T ...

3 days ago ... **T-Mobile**, Sprint merger **class action lawsuit** overview: ... The April 2020 merger between **T-Mobile** and Sprint was an anticompetitive acquisition ...

<https://www.classaction.com/t-mobile/lawsuit/>

Mass Arbitration Against T-Mobile - Class Action Lawsuits

Due to their terms and conditions and being a giant in mobile services, **T-Mobile** may be able to get around individual **lawsuits**. However, when faced with a ...

<https://www.classlawgroup.com/consumer-protection/t-mobile-data-breach-lawsuit/>

T-Mobile Data Breach Lawsuit 2022 | Join 1000s of others

T-Mobile Data Breach **Lawsuit** 2022 ... Our attorneys are pursuing claims on behalf of victims of the **T-Mobile** data breach. Many victims had their Social Security ...

PROVIDED TO: FBI, WHITE HOUSE, OSC, GAO, SEC, CFTC, CONGRESSIONAL CHIEF'S OF STAFF, ET AL

This document: Public Domain. Non-Commercial. Fair Use. Freedom of The Press. No Tracking Of Public Allowed. First Amendment Protections, SLAPP, UN Protected. GDPR Compliant. Section 203 protected. Privacy Tools At: <http://privacytools.io>, ACLU, ICIJ.ORG- supported.