Big Tech's Mass Public Media Manipulation Violates Anti-Trust And Constitutional Rights Laws

Congressional Report
Aug. 6, 2021

Table of Contents

Google And Facebook Have A Psychological Trick To Make You Do Things You Wouldn't Believe You Might Do

Most of the U.S. Senators and government agency heads own stock in, get their political campaigns financed by and party with, the owners and executives of the Silicon Valley big tech companies.

That is why those public officials fail to halt the mass societal abuses of those companies. Above all others, the California politicians are in bed with the same criminals they are supposed to regulate.

While politicians shrug off any attempt to bring the oligarchs into line, they provide lip-service, window-dressing pretend actions that have impressive titles but zero bite.

The authors of this report were in private meetings with the investors and founders of the Silicon Valley "Big Five", at the inception of their companies, and hereby testify that those owners planned, with malicious intent, the use of their business licenses for the purpose of manipulating, harming and restricting the public interest, and DEMOCRACY, for profiteering purposes.

Big tech's "*green-washing*", false-savior, "*we-are-your-mother*" fake "*do-gooder*" facade is a sham to sucker everyone.

They hide behind a curtain of false altruism and do the darkest deeds any industry can undertake behind that contrived screen.

One of Google , Youtube and Facebook's most insidious technologies can even get you to engage in riots, murders and other crimes, even though you might, otherwise, never do those things. Here is how that technology works:

Since the early 20th century, the name of the Russian scientist Ivan Pavlov has been associated with the idea of brainwashing. Pavlov's experiments, in which he trained dogs to salivate in response to a signal such as a bell, showed that the mind could be conditioned to react automatically to stimuli. But he looked forward to a time when science could manipulate the brain directly. In a passage eerily accurate in describing today's neural imaging, he wrote: "If we could look through the skull into the brain of a consciously thinking person…then we should see playing over the cerebral surface a bright spot with fantastic, waving borders, constantly fluctuating in size and form, and surrounded by a darkness, more or less deep, covering the rest of the hemispheres."

We still don't have a precise topography of the brain in terms of specific thoughts or feelings. It's hard to imagine where one would begin if one wanted to surgically force someone to reveal a particular secret, or to persuade him or her to vote for a certain candidate. But since Pavlov's time, science has moved much closer to enabling direct physical control of the brain. In this century, neuroscientists' insights into memory, cognition, pleasure and pain may make coercive "mind control" a reality.

The psychologist James Olds (1922-76), one of the founders of modern neuroscience, conducted an experiment at McGill University in 1953 in which he implanted electrodes deep in the brains of rats and started observing their responses to electrical stimulation at various sites. His key observation resulted from an accident: He missed the desired anatomical site slightly on one particular rat. After recovering from surgery, the animal was placed in a special chamber. Every time it went to a corner of the chamber, it received a small electrical stimulus to the brain, with each corner stimulating a different site. The rat kept returning to one specific corner, even skipping eating to hang out there and get the brain stimulation.

Ivan Pavlov watching an experiment with a dog in 1934.

Photo: Sovfoto/Universal Images Group/Getty Images

Olds inferred that there was something pleasurable about receiving a shock at that site in the brain. Next he started training the rat to go to different parts of the box or to turn right or left before it could receive the desired electrical stimulation. Using this technique, Olds could elicit complex behaviors easily; Pavlov would have been envious about this shortcut to behavioral conditioning. Olds observed that “Left to itself in the apparatus, the animal…stimulated its own brain regularly,” up to 5,000 times an hour.

The mind-control possibilities for this intervention sounded almost limitless, but would it work on people? Psychiatrist Robert Heath (1915-99), of Tulane University, performed studies with human patients, including one code-named B-7, a 28-year-old man with severe narcolepsy. Heath implanted a series of electrodes in various areas of his brain and asked the patient what he felt after each area was

stimulated. One area was so aversive that the patient intentionally broke the stimulus button so that he would never have to experience that sensation again.

However, the feelings evoked by stimulating a different site were intensely pleasurable. The patient learned that he could block an incipient narcoleptic attack by self-stimulating; he was able to control his symptoms so well that for the first time he was able to get a job. On the rare occasion that he fell asleep too rapidly to press the button, his friends knew that they could promptly wake him up by pressing it for him.

Neurosurgical techniques have continued to evolve to be less invasive, less risky and applied to very specific areas of the brain.

At one point the CIA approached Heath, asking if he would work with the agency to study the brain's pleasure and pain system. He spurned the invitation, he told a New York Times reporter in 1977: "If I had wanted to be a spy, I would have been a spy. I wanted to be a doctor and practice medicine." This kind of work, most of which was conducted in the 1960s and 1970s, has largely been shut down because of ethical concerns.

However, the underlying neurosurgical techniques have continued to evolve. Fifty years after Heath's studies, procedures are less invasive, less risky and can be applied to very specific areas of the brain. Implanted deep-brain stimulators (DBS) are used by thousands of people with Parkinson's disease to help control their muscle movements, as well as for other conditions such as pain and epilepsy. There is ongoing interest in using such interventions on different sites in the brain to treat patients with psychiatric disorders, particularly patients with treatment-resistant depression.

Deep-brain stimulation requires painstaking surgery and expensive equipment, suitable for an individual but hardly appropriate for group interventions. Is there a way of stimulating a group of people without implants? In her 1996 book "Cults in Our Midst," Psychologist Margaret Singer described love bombing," an indoctrination technique used by some cults in which recruits are given so much flattery and adulation that they feel welcome and safe.

The neuroendocrine equivalent involves a hormone called oxytocin that is manufactured deep in the brain. People release oxytocin when they are bonding with another; it is sometimes nicknamed the feel-good hormone. Early research found that it is increased during breast-feeding and during sexual intimacy. Subsequent research showed that oxytocin is also produced in other situations of closeness—prayer, team sports, even when dog owners interact with their pets.

But there is a darker side to oxytocin. Experiments have found that it can stoke trust and cooperation within a group at the expense of distrust of people outside the group. Currently, the most effective way of administering oxytocin is through a nasal spray, but if it were possible to administer it orally or via aerosol, it could conceivably be used in group settings to increase attachment and thereby recruit new potential members of a cult or party. People might willingly join a group or adopt a new belief if it allowed them to receive pleasurable stimulation—after all, addicts aren't particularly squeamish about what they need to do to obtain their drugs.

On the other side of the coin, people might repudiate their old beliefs or identities to turn off painful stimulation, the way patient B-7 broke his stimulus button. When the dystopian movie “A Clockwork Orange” was released in 1971, audiences were stunned by its portrayal of the power of aversive conditioning. The advance of neuroscience means that such techniques are no longer just fantasies. So far they have been kept in check only by government regulation and medical professionals’ sense of ethics. But governments are always seeking new weaponry, and history suggests that there will always be some researchers who close their eyes to the implications of their work or justify it as a way to protect society from looming threats. Their self-restraint may not always protect us from the dark potential of Google and Facebook’s scientific coercion. This report goes deeper into those contrived and manually steered tech manipulations operated by Big Tech’s executives.

Collusion Exposed That Manipulates Your News And Information For Personal Gain

Google is manipulating your internet searches, your elections, your perceptions of the news, your democracy, your ideologies and your school curriculum's. Google and their cartel (including FACEBOOK, NETFLIX, LINKEDIN, YOUTUBE, et al) collude to manipulate social dynamics.

White House executives, Federal Agency Executives and U.S. Senators including Dianne Feinstein, Kamala Harris, John Podesta, Nancy Pelosi, Harry Reid own, control and finance "***The Deep State"*** because they own, and their families, own the stock in the companies comprising ***The Deep State***, they tell those companies what to do, they fund those companies and they social communicate with each other through covert channels, they engage sexually with each other and they exchange stock market tips and strategies, and that forensic accounting shows that the politicians and the corrupt companies are all the same organization. ***This, in part, proves that the "Deep State" is "State Sponsored".***

Google, and The Deep State's, socialistic, anti-Christian bias is invisibly reflected in the suppression of ideological content from appearing in some search results.

In shocking research that has spanned the past 6 ½ years, Dr. Robert Epstein – former editor-in-chief of *Psychology Today* and now Senior Research Psychologist at the American Institute for Behavioral Research and Technology – has found that by controlling search results, Google possesses unprecedented power to sway the thinking of undecided voters during an election campaign.

How is it done?

Google can manipulate its search engine algorithm to display one-sided search results that decidedly favor one political candidate over another.

Dr. Epstein gave a grim prediction in recent congressional testimony…

He said that "democracy as originally conceived cannot survive Big Tech as currently empowered."

Dr. Epstein is a registered Democrat. He supported and voted for Hillary Clinton in the 2016 election. He has no hidden agenda … and no axe to grind for President Trump.

During the 2016 presidential election campaign, he captured and analyzed "more than 13,000 election-related searches conducted by a diverse group of Americans on Google, Bing, and Yahoo in the weeks leading up to the election…"

During the 2018 midterm election cycle, Dr. Epstein captured 47,000 election-related searches – plus nearly 400,000 web pages to which the search results were linked.

The results of his scientific analysis in both cases were disturbing…

The Google search results in 2016 – which account for over 92% of worldwide internet searches – were significantly biased in favor of Hillary Clinton in all 10 positions on the first page of search results in both blue states and red states.

In 2018, the first-page search results heavily favored web sites and articles favoring Democrat candidates rather than being evenly split between Democrat and Republican candidates.

Very few people who do spontaneous searches ever scroll past the first page of search results. And Google knows this.

Dr. Epstein has conducted dozens of controlled experiments in the U.S. and other countries to precisely measure – through before-and-after questionnaires – how opinions and votes shift among undecided voters when search results strongly favor one candidate over another.

He calls this shift "SEME" – Search Engine Manipulation Shift.

"SEME is one of the most powerful forms of influence ever discovered in the behavioral sciences," Dr. Epstein said in his congressional testimony, "and it is especially dangerous because it is invisible to people – 'subliminal' in effect… Bottom line: biased search results can easily produce shifts in the opinions and voting preference of undecided voters by 20% or more – up to 80% in some demographic groups."

I can tell you, this is enough voters to change the results of any election.

Dr. Epstein calculated that Search Engine Manipulation Shift likely persuaded at least 2.6 million undecided voters to cast their ballots for Hillary Clinton in 2016 …and perhaps as many as 10.4 million.

In the 2018 midterm elections, Epstein's evidence suggests that as many as 78.2 million votes may have been shifted to Democrat candidates due to Search Engine Manipulation Shift.

These effects are far more meddlesome and interfering than fake news stories or ads placed by Russians on social media…

While these acts of interference are troubling and unacceptable, they don't shift very many votes because they are competitive and visible. Search Engine Manipulation Shift – on the other hand – is invisible and non-competitive.

Dr. Epstein explains: "SEME is an example of an 'ephemeral experience,' and that's a phrase you'll find in internal emails that have leaked from Google recently. A growing body of evidence suggests that Google employees deliberately engineer ephemeral experiences to change people's thinking… My recent research demonstrates that Google's 'autocomplete' search suggestions can turn a 50/50 split among undecided voters into a 90/10 split without people's awareness."

As expected, Google, Hillary Clinton, and progressive media outlets have all disputed Dr. Epstein's research and his claims…

They all say in unison that this 2016 study of election-related search results has been "debunked," and that Epstein's results aren't valid because he made "weird methodological choices" in an earlier 2010 study.

But they haven't debunked his methodology or his results at all…

They're just saying this to try to discredit him and convince people to not take his work seriously. They haven't refuted him either by conducting their own comparable studies … or by addressing his explanations of his methodology.

Incidentally, the number one Hillary Clinton financial supporter in the 2016 election was Alphabet Inc. – the parent company of Google.

You can read Dr. Epstein's testimony and study the methodology of his experiments here.

He is eminently qualified to conduct the type of research he's been conducting with Google search – having been a research psychologist for nearly 40 years.

He received his Ph.D. at Harvard University in 1981 and has published 15 books and more than 300 scientific articles on artificial intelligence and other behavioral topics.

Dr. Epstein believes the solution to Google's search engine manipulation is to end its monopoly over its "black box" algorithm operation.

By requiring that the database they use to generate search results must be available in the public domain – accessible to all – many new search platforms will spring up and compete with Google, providing the same excellent search results.

Incidentally, I find that every time I run a Google search on a topic, I am served biased viewpoints…

Usually a CNN report is first on the list, followed by:

•The New York Times

•The Washington Post

•MSNBC

•Other pro-socialist media

I often have to scroll to page 7 or 8 to start finding conservative viewpoints.

Since 2012, Google has discriminated against and marginalized our editorial content. If they are doing it to us, they are certainly doing it to conservative web sites with higher numbers of subscribers. See these videos:

https://youtu.be/rNvgl38TLvI

and

https://youtu.be/csye_Jkp4eI

There were allegations raised that Google was **manipulating the news** to help Hillary. They allegedly steered **2.6 million votes to Hillary** and had far more of an impact upon the 2016 election than Russians. A whistleblower at Google has come out and warned that things are getting worse. Google whistleblower **Zach Vorhies** came out and provided documents and warnings. He said:

"Before Trump won, Google had this mission statement to organize the world's information and making it universally accessible and useful."

> *"After Trump won, they said 'Well, Donald Trump won because of fake news and Russia hacking the election, so what we need to do is … protect our users from fake news; we need to protect our users from the damaging effects of Russian trolls and bots."*

What is interesting is that Elizabeth Warren has been a longtime critic of the economic power of Amazon, Google, and Facebook. She is making their **break-up** under Anti-Trust Laws a key component of her presidential platform.

Google's ubiquitous search engine, Google Search, is the backbone of the tech giant's business.

In many ways, Google Search is the backbone of the modern internet — the way much of the web is sorted and organized and located. Given how crucial it is to daily internet use for billions of people around the world, it's a particularly ripe target for manipulation.

Google denies doing as much, and insists that Google Search is built on algorithms and data gleaned from use.

But a new Wall Street Journal investigation found that Google manipulated search algorithms in some worrying ways, including prioritizing large businesses over smaller ones, removing autocomplete results that involve sensitive topics like immigration and abortion, and even outright blacklisting some websites.

In one such change to Google's search algorithms, the service guided search users to more prominent businesses over lesser-known ones, the Journal reported. That change reportedly helped to boost Amazon's store in search results.

In another example cited in the Journal's report, autocomplete search results for sensitive subjects were replaced with safer results than those found on competing search engines like Yahoo, Bing, and DuckDuckGo.

Google is known for refusing to share specific details on how its search algorithms operate, which it attributes to a measure of operations logistics: If the algorithms were public, then they could be gamed, Google argues.

"Extreme transparency has historically proven to empower bad actors in a way that hurts our users and website owners who play by the rules," Google spokesperson Lara Levin told the Journal.

When reached for a response to the report, a Google spokesperson offered the following statement:

"We have been very public and transparent around the topics covered in this article, such as our Search rater guidelines, our policies for special features in Search like Autocomplete and valid legal removals, our work to combat misinformation through Project Owl, and the fact that the changes we make to Search are aimed at benefiting users, not commercial relationships. This article contains a number of old, incomplete anecdotes, many of which not only predated our current processes and policies but also give a very inaccurate impression of how we approach building and improving Search. We take a responsible and principled approach to making changes, including a rigorous evaluation process before launching any change — something we started implementing more than a decade ago. Listening to feedback from the public is a critical part of making Search better, and we continue to welcome the feedback."

If you use Google’s search engine, “There’s no way of knowing what you’re missing,” says Gabriel Weinberg, CEO and founder of search engine DuckDuckGo, whose company released a study Tuesday claiming that Google is manipulating Americans’ search results.

The study concludes that Google is editorializing and providing different search results for different users who search for identical terms, within seconds and minutes of each other.

“The editorialized results are informed by the personal information Google has on you, like your search, browsing and purchase history,” the study says.

“What we’re seeing is intense amounts of variation,” Weinberg told Yahoo Finance. “Most of the people in the study saw results completely unique to them.”

By unique, Weinberg means that inconsistent source links appeared in search results, and some of the same links appeared in varying hierarchical order.

Seventy-two U.S. participants in the study entered three independent Google search terms — gun control, immigration, and vaccinations — using a desktop Chrome browser at 9 p.m. eastern time on July 24, 2018.

Unique results were returned for 68% of private searches for “gun control,” 57% of searches for “immigration,” and 92% of searches for “vaccinations.”

According to the study, Google returned these filtered results, regardless of whether participants searched in private “incognito,” or non-private mode.

“It’s exactly opposite of what people would expect,” Weinberg said.

In non-private mode, unique search results were generated for 59% of searches for “gun control,” 63% of searches for “immigration,” and 92% of searches for “vaccinations.”

“Our proposition is that if you search in the U.S. you should be seeing the same things, especially when you search major political topics,” Weinberg said.

DuckDuckGo decided to run the new study after a previous version examined Google search results in connection with the 2012 presidential campaigns. A Wall Street Journal study, commissioned around the same time, mirrored DuckDuckGo’s findings, showing that Google’s personalized search results inserted tens of millions of more links for then-candidate Barack Obama than for his primary challenger Mitt Romney.

“Search personalization doesn’t actually help search results, it really hurts in the aggregate, making people more politically polarized,” Weinberg said.

In his experience, Weinberg says when consumers think of search personalization they’re really expecting search localization for services like local weather, local restaurants, and maps, rather than national or international political issues.

“You can do that all without a filter bubble because it’s not based on your search history,” he said, adding that search-based ad revenue is not dependent on search personalization.

DuckDuckGo’s study controlled for local results by designating all local search results as equal and accounting for no variation if the local links appeared in the same hierarchical order. A result showing an LA Times link, for example, was treated the same as link to the Chicago Tribune.

For critics who dispense with the importance of result order, Weinberg says they’re mistaken.

“The first link gets about 40% of the clicks, the second gets about 20%, and it drops off by half with each [subsequent] link,” he said. “If you switch the second and first link, that’s actually a huge difference” because the one is now getting twice as many clicks as the other.

Yahoo Finance reached out to Google for a response to DuckDuckGo’s study and didn’t receive a response.

“I’m really not on any particular side,” Weinberg said when asked about his political ideology.

He says he’d like to see Congress question Google CEO Sundar Pichai about search result bias when he testifies before the House Judiciary Committee on December 11.

“We understand [the study] is coming from a competitor and there’s an inclination to believe [the findings] less so. That’s why we made it all public, the data, the code, the directions, and we are basically saying we believe other people should study this,” he said.

Weinberg says editorialized results may be crafted depending on the level of privacy, and the number of Android products you use.

“They may have all your email, they may have all your text messages, have all your photos, all your contacts, so [editorialized content] can be based on all of those things. It’s a completely black box and opaque to consumers.”

A few people in the study were given a much broader range in search results from what the majority of participants were seeing, Weinberg said.

“You would just have no idea if you were one of those people. And you also would have no idea, even if you know you’re seeing something different, why you’re seeing it.”

The rise of renewed and vociferous social movements for every non-white and non-cis male group can be seen as paralleling the rise of social media and the domination of technology platforms. In time, at least in the Western world, when blacks, women, gays, and most other populations have won equal rights, and even preferential rights, under codified federal law, and when their social currency has never been higher, it seems now that their voice has never sounded more pained or aggrieved.

Without a doubt, the ease of emoting through a tweet has certainly affected how individual users can set off maelstroms of irrational fury. Whether calling out real hurt, self-deluded hurt, or pure schadenfreude, there is no shortage of bored and usually meaningless lives attempting to drag down a crab that has nearly escaped the barrel of life.

The other side of the same coin is how the tech giant themselves can influence the narrative. We see this play out with not-so-alleged shadow banning practices of conservative social media accounts, and most people are by now aware of YouTube demonetizing conservative channels. We can add a new wrinkle: The representation of Google Image searches to advance a social narrative.

Let’s break down what we saw in our own online queries, and then we can analyze it afterward. Try it out for yourself and leave a comment at the end of the article.

Google Search: “White Men”

The top three rows of the search produced a total of sixteen results. Of those, there were:

❍One result featuring a woman of color

❍Three results featuring exclusively black men, either as a victim of white brutality or as a successful black man. Each image is a well-dressed black man wearing a tuxedo or suit.

❍Five results featuring either a mug shot of some kind or simply an angry visage.

❍Visible taglines for the images including phrases like “Dear White Men, We Need You,” “White Men Are Bad,” “An Angry White Man” and one begins “White Men Aren’t Thrilled When Women”

❍Only two results showing white men smiling

Google Search: “Black Men”

The top three rows of the search produced a total of seventeen results. Of those, there were:

❍All seventeen results featuring black men

❍Eight of the results featuring black men smiling

❍At least six of the results explicitly expressing victimhood. A few others are vaguer but allude to it.

❍Visible taglines for the images including: “The Young Black Men Caught,” “Why Do White People Feel,” “Photo Campaign That Celebrates Black” and “Resilience Of Black Men.”

Google Search (see feature photo): “White Women”

The top three rows of the search produced a total of fifteen results. Of those, there were:

❍Five results featuring women of color

❍Two results featuring black men

❍Four featuring white women smiling

❍Visible taglines for the first five results including: “The Trouble with White Women,” “White Women Need To Talk About Race,” “White Women Aren’t Allies At Work,” “Dear White Women, No More,” and “White Women: It’s Time To Be…”

❍Other taglines including “White Women Were Southern Slave Owners,” “Being Exoticised By White Women,” “Black Women Are Paid Less Than White,” and “White Women Benefit Most (from white privilege).”

Google Search: “Black Women”

The top three rows of the search produced a total of sixteen results. Of those, there were:

❍All sixteen results featuring black women

❍All sixteen results featuring well-dressed and well-groomed women

❍Fourteen of the results featuring black women smiling or projecting happiness (the other two project strength)

❍Visible taglines including: “How Women Have Shaped,” “Studies Suggest Black Women Are More,” “My Heroes Are Black Women,” and “20 Millenial Black-Owned Brands.”

Google Search: “White People”

The top three rows of the search produced a total of fifteen results. Of those, there were:

❍Seven results featuring people of color

❍Four additional results featuring white people protesting in solidarity with black people

❍Just one result featuring a white person smiling (a white woman with dreadlocks)

❍Visible taglines including: “Dear White People,” “Dear White People (again),” “A Letter To White People,” and another features the deplorable Robin DeAngelo.

Google Search: “Black People”

The top three rows of the search produced a total of fifteen results. Of those, there were:

❍All fifteen results featuring black people

❍Eleven results featuring blacks smiling

❍Visible taglines including: “What’s Life Really Like For Black,” “Being Black In America,” “Racism Grows in Places,” and “Facebook Has Problem With Black People.”

An Analysis of Search Results

An aggregate of the three “white” searches is unflattering for white people. Of the forty-six total results, a full eighteen (39%) of them depict non-whites, sometimes in roles of victimhood but usually in portrayals of independence and success. In and of itself, this is not bad, but it is misrepresentative of the intended search, and as we see, it is not replicated in reverse for other searches. For the whites themselves, just seven (15%) were represented in a positive light as indicated by smiling. Put another way, more than twice the amount of blacks were shown than whites in a positive way – in a search designed to produce white results, to begin with.

The taglines are especially egregious. Just two taglines suggest something positive (“Employment Helps White Men’s Health,” and another is assumed to be positive because it shows white women rallying against the death of a black woman at the hands of police). Two others are neutral in that they advertise white shirts. That leaves a full twenty-four taglines (52%) under an image of white people that states something negative or dangerous about them.

An aggregate of the three “black” searches has a different outcome. Of the forty-eight total results, fully 100% of those results came back with images of black people. In the same vein, none of the taglines suggest that blacks are dangerous or that anything blacks do is harmful to others (as is the case especially with white women, more on that anon).

Amazingly, twenty-nine taglines portray blacks as victims. Despite the overall happiness of blacks as seen through imagery, the titling of the pictures nevertheless contends that blacks must be seen as victims. The taglines refer to the problems being black in America, and several refer to their killings (always at the hands of whites or police, not other blacks, even though black homicide victims are killed by other blacks 90% of the time according to the FBI).

As it relates specifically to the query of white women, something striking is happening. There is clearly a concerted effort to portray white women as comfortably and cunningly subversive (Where is the feminist outrage, by the way?). Most headlines call out white women for a combination of their insincere efforts at allying with blacks, benefiting from white privilege, and to really hammer home a negative stereotype, fulfilling the role of a “Karen.” In the intersectional rat race, the irony is that a significant majority of all women marchers in January 2017 were white and championing leftist causes. Two immalleable rules in life: You can’t please everyone, and the left always consumes its own.

It is obvious that the Marxists at Google have an agenda to pursue, namely that the narrative must be alive and well. White men and women are evil? Check. Are blacks simultaneously victims of white oppression and strong individuals? Check. The more subtle displays arise when looking at the positive

and negative dispositions. In Nazi propaganda, Goebbels only had to compare Jews to rats for so long before most Germans went along with the lie. How long before a similar lie is believed here? More concerning, what happens after that?

The Wall Street Journal has undertaken a thorough investigation into how Google, despite its denials and disavowals, manipulates search results to influence what you learn and find online.

For years Google executives have insisted that they do not use human intelligence to arrange the results of online searches. Yet, the *Journal* found that, "Google's algorithms are subject to regular tinkering from executives and engineers who are trying to deliver relevant search results, while also pleasing a wide variety of powerful interests and driving its parent company's more than $30 billion in annual profit."

The *Journal* also found that, "Despite publicly denying doing so, Google keeps blacklists to remove certain sites or prevent others from surfacing in certain types of results."

The tech giant also influences search results through its auto-complete feature prior to searching the internet. "In auto-complete, the feature that predicts search terms as the user types a query, Google's engineers have created algorithms and blacklists to weed out more incendiary suggestions for controversial subjects, such as abortion or immigration, in effect filtering out inflammatory results on high-profile topics."

In response to the investigation, a Google spokeswoman, Ms. Levin, told the *Journal*, "We do today what we have done all along, provide relevant results from the most reliable sources available."

Google, which has more than 90% of the market share for online searches, is an extremely powerful company capable of controlling what people know and what they can learn online.

The *Journal* tested the word "abortion" in Google's search engine and compared the results to Bing and DuckDuckGo's results. According to the test, Planned Parenthood was featured in 39% of the results on the first page of Google's results compared to 14% for Bing and 16% for DuckDuckGo.

Ms. Levin responded to the test by claiming that Google does not promote Planned Parenthood through its algorithm, but the available evidence suggests otherwise.

Google has also been exposed by a former staffer who spoke with the undercover investigative organization Project Veritas. The staffer, Zachary Vorhies, claimed that Google has a "news blacklist" document which censors conservative websites such as LifeNews.com, Newsbusters and the Media Research Center.

According to one researcher, Google even has the power to influence the results of an election. Indeed, they have already done so.

Dr. Robert Epstein, Ph.D., a senior research psychologist at the American Institute for Behavioral Research and Technology, is one of the lonely voices that has been speaking out about Google's manipulation of search results. Dr. Epstein's research has focused particularly on the impact of Google's search result manipulation on elections.

In a testimony before the Senate Judiciary Committee in June of 2019, Dr. Epstein claimed that, "In 2016, biased search results generated by Google's search algorithm likely impacted undecided voters in a way that gave at least 2.6 million votes to Hillary Clinton (whom I supported)."

Dr. Epstein also claimed that, “On Election Day in 2018, the “Go Vote” reminder Google displayed on its home page gave one political party between 800,000 and 4.6 million more votes than it gave the other party. In other words, Google’s “Go Vote” prompt was *not* a public service; it was a *vote manipulation*.”

The evidence Dr. Epstein provides is disconcerting, though not surprising.

In a leaked video following the election of President Donald Trump in 2016, Google executives held a staff meeting in which they conveyed significant remorse about the election results.

In the video, Google co-founder Sergey Brin states, “I know this is probably not the most joyous TGIF (weekly meeting) we have had. Let’s face it, most people here are pretty upset and pretty sad because of the election.”

Brin goes on to say, “Myself, as an immigrant and refugee, I certainly find this election deeply offensive and I know many of you do too. And I think it’s a very stressful time, and it conflicts with many of our values.”

In the same meeting, Google CFO Ruth Porat broke down in tears recounting Hillary Clinton’s loss that Tuesday evening. After texting a friend who was at what would have been Clinton’s election night victory party, Porat said her friend responded, “People are leaving. Staff is crying. We’re going to lose.” With her voice trembling, Porat says, “Uh… that was first moment I really *felt* like we were going to lose, and it was this massive kick in the gut that we were going to lose.”

Numerous other examples of liberal bias among Google’s top executive team was demonstrated in the video, and what’s remarkable is that there is not a single moment of conservative opinion expressed. The support for Clinton and the sense of dread seemed to be unanimous.

It couldn’t be clearer that Google is an enormously influential company run by an entirely liberal executive team. And the *Journal*’s excellent investigative work further exposes their manipulative practices.

I think it’s past time we consider whether using Google as our primary search engine, which most Americans do, is wise.

Google, Inc., isn't just the world's biggest purveyor of information; it is also the world's biggest censor.

The company maintains at least nine different blacklists that impact our lives, generally without input or authority from any outside advisory group, industry association or government agency. Google is not the only company suppressing content on the internet. Reddit has frequently been accused of banning postings on specific topics, and a recent report suggests that Facebook has been deleting conservative news stories from its newsfeed, a practice that might have a significant effect on public opinion – even on voting. Google, though, is currently the biggest bully on the block.

When Google's employees or algorithms decide to block our access to information about a news item, political candidate or business, opinions and votes can shift, reputations can be ruined and businesses can crash and burn. Because online censorship is entirely unregulated at the moment, victims have little or no recourse when they have been harmed. Eventually, authorities will almost certainly have to step in, just as they did when credit bureaus were regulated in 1970. The alternative would be to allow a large corporation to wield an especially destructive kind of power that should be exercised with great restraint and should belong only to the public: the power to shame or exclude.

If Google were just another mom-and-pop shop with a sign saying "we reserve the right to refuse service to anyone," that would be one thing. But as the golden gateway to all knowledge, Google has rapidly become an essential in people's lives – nearly as essential as air or water. We don't let public utilities make arbitrary and secretive decisions about denying people services; we shouldn't let Google do so either.

The New Too Big to Fail

Big social media companies like Facebook and Google have so much power they can easily manipulate elections.

Let's start with the most trivial blacklist and work our way up. I'll save the biggest and baddest – one the public knows virtually nothing about but that gives Google an almost obscene amount of power over our economic well-being – until last.

1. The autocomplete blacklist. This is a list of words and phrases that are excluded from the autocomplete feature in Google's search bar. The search bar instantly suggests multiple search options when you type words such as "democracy" or "watermelon," but it freezes when you type profanities, and, at times, it has frozen when people typed words like "torrent," "bisexual" and "penis." At this writing, it's freezing when I type "clitoris." The autocomplete blacklist can also be used to protect or discredit political candidates. As recently reported, at the moment autocomplete shows you "Ted" (for former GOP presidential candidate Ted Cruz) when you type "lying," but it will not show you "Hillary" when you type "crooked" – not even, on my computer, anyway, when you type "crooked hill." (The nicknames for Clinton and Cruz coined by Donald Trump, of course.) If you add the "a," so you've got "crooked hilla," you get the very odd suggestion "crooked Hillary Bernie." When you type "crooked" on Bing, "crooked Hillary" pops up instantly. Google's list of forbidden terms varies by region and individual, so "clitoris" might work for you. (Can you resist checking?)

2. The Google Maps blacklist. This list is a little more creepy, and if you are concerned about your privacy, it might be a good list to be on. The cameras of Google Earth and Google Maps have photographed your home for all to see. If you don't like that, "just move," Google's former CEO Eric Schmidt said. Google also maintains a list of properties it either blacks out or blurs out in its images. Some are probably military installations, some the residences of wealthy people, and some – well, who knows? Martian pre-invasion enclaves? Google doesn't say.

3. The YouTube blacklist. YouTube, which is owned by Google, allows users to flag inappropriate videos, at which point Google censors weigh in and sometimes remove them, but not, according to a recent report by Gizmodo, with any great consistency – except perhaps when it comes to politics. Consistent with the company's strong and open support for liberal political candidates, Google employees seem far more apt to ban politically conservative videos than liberal ones. In December 2015, singer Joyce Bartholomew sued YouTube for removing her openly pro-life music video, but I can find no instances of pro-choice music being removed. YouTube also sometimes acquiesces to the censorship demands of foreign governments. Most recently, in return for overturning a three-year ban on YouTube in Pakistan, it agreed to allow Pakistan's government to determine which videos it can and cannot post.

4. The Google account blacklist. A couple of years ago, Google consolidated a number of its products – Gmail, Google Docs, Google+, YouTube, Google Wallet and others – so you can access all of them through your one Google account. If you somehow violate Google's vague and intimidating terms of service agreement, you will join the ever-growing list of people who are shut out of their accounts, which means you'll lose access to all of these interconnected products. Because virtually no one has ever read this lengthy, legalistic agreement, however, people are shocked when they're shut out, in part because Google reserves the right to "stop providing Services to you … at any time." And because

Google, one of the largest and richest companies in the world, has no customer service department, getting reinstated can be difficult. (Given, however, that all of these services gather personal information about you to sell to advertisers, losing one's Google account has been judged by some to be a blessing in disguise.)

No Likes for Facebook Manipulation

The social media giant isn't a news site, but it still shouldn't be messing with its trending topics.

5. The Google News blacklist. If a librarian were caught trashing all the liberal newspapers before people could read them, he or she might get in a heap o' trouble. What happens when most of the librarians in the world have been replaced by a single company? Google is now the largest news aggregator in the world, tracking tens of thousands of news sources in more than thirty languages and recently adding thousands of small, local news sources to its inventory. It also selectively bans news sources as it pleases. In 2006, Google was accused of excluding conservative news sources that generated stories critical of Islam, and the company has also been accused of banning individual columnists and competing companies from its news feed. In December 2014, facing a new law in Spain that would have charged Google for scraping content from Spanish news sources (which, after all, have to pay to prepare their news), Google suddenly withdrew its news service from Spain, which led to an immediate drop in traffic to Spanish new stories. That drop in traffic is the problem: When a large aggregator bans you from its service, fewer people find your news stories, which means opinions will shift away from those you support. Selective blacklisting of news sources is a powerful way of promoting a political, religious or moral agenda, with no one the wiser.

6. The Google AdWords blacklist. Now things get creepier. More than 70 percent of Google's $80 billion in annual revenue comes from its AdWords advertising service, which it implemented in 2000 by infringing on a similar system already patented by Overture Services. The way it works is simple: Businesses worldwide bid on the right to use certain keywords in short text ads that link to their websites (those text ads are the AdWords); when people click on the links, those businesses pay Google. These ads appear on Google.com and other Google websites and are also interwoven into the content of more than a million non-Google websites – Google's "Display Network." The problem here is that if a Google executive decides your business or industry doesn't meet its moral standards, it bans you from AdWords; these days, with Google's reach so large, that can quickly put you out of business. In 2011, Google blacklisted an Irish political group that defended sex workers but which did not provide them; after a protest, the company eventually backed down.

In May 2016, Google blacklisted an entire industry – companies providing high-interest "payday" loans. As always, the company billed this dramatic move as an exercise in social responsibility, failing to note that it is a major investor in LendUp.com, which is in the same industry; if Google fails to blacklist LendUp (it's too early to tell), the industry ban might turn out to have been more of an anticompetitive move than one of conscience. That kind of hypocrisy has turned up before in AdWords activities. Whereas Google takes a moral stand, for example, in banning ads from companies promising quick weight loss, in 2011, Google forfeited a whopping $500 million to the U.S. Justice Department for having knowingly allowed Canadian drug companies to sell drugs illegally in the U.S. for years through the AdWords system, and several state attorneys general believe that Google has continued to engage in similar practices since 2011; investigations are ongoing.

7. The Google AdSense blacklist. If your website has been approved by AdWords, you are eligible to sign up for Google AdSense, a system in which Google places ads for various products and services on

your website. When people click on those ads, Google pays you. If you are good at driving traffic to your website, you can make millions of dollars a year running AdSense ads – all without having any products or services of your own. Meanwhile, Google makes a net profit by charging the companies behind the ads for bringing them customers; this accounts for about 18 percent of Google's income. Here, too, there is scandal: In April 2014, in two posts on PasteBin.com, someone claiming to be a former Google employee working in their AdSense department alleged the department engaged in a regular practice of dumping AdSense customers just before Google was scheduled to pay them. To this day, no one knows whether the person behind the posts was legit, but one thing is clear: Since that time, real lawsuits filed by real companies have, according to WebProNews, been "piling up" against Google, alleging the companies were unaccountably dumped at the last minute by AdSense just before large payments were due, in some cases payments as high as $500,000.

The Loan That's Safe at Any Rate

It's past time to eliminate interest rate caps on small-dollar installment loans.

8. The search engine blacklist. Google's ubiquitous search engine has indeed become the gateway to virtually all information, handling 90 percent of search in most countries. It dominates search because its index is so large: Google indexes more than 45 billion web pages; its next-biggest competitor, Microsoft's Bing, indexes a mere 14 billion, which helps to explain the poor quality of Bing's search results.

Google's dominance in search is why businesses large and small live in constant "fear of Google," as Mathias Dopfner, CEO of Axel Springer, the largest publishing conglomerate in Europe, put it in an open letter to Eric Schmidt in 2014. According to Dopfner, when Google made one of its frequent adjustments to its search algorithm, one of his company's subsidiaries dropped dramatically in the search rankings and lost 70 percent of its traffic within a few days. Even worse than the vagaries of the adjustments, however, are the dire consequences that follow when Google employees somehow conclude you have violated their "guidelines": You either get banished to the rarely visited Netherlands of search pages beyond the first page (90 percent of all clicks go to links on that first page) or completely removed from the index. In 2011, Google took a "manual action" of a "corrective" nature against retailer J.C. Penney – punishment for Penney's alleged use of a legal SEO technique called "link building" that many companies employ to try to boost their rankings in Google's search results. Penney was demoted 60 positions or more in the rankings.

Search ranking manipulations of this sort don't just ruin businesses; they also affect people's opinions, attitudes, beliefs and behavior, as my research on the Search Engine Manipulation Effect has demonstrated. Fortunately, definitive information about Google's punishment programs is likely to turn up over the next year or two thanks to legal challenges the company is facing. In 2014, a Florida company called e-Ventures Worldwide filed a lawsuit against Google for "completely removing almost every website" associated with the company from its search rankings. When the company's lawyers tried to get internal documents relevant to Google's actions though typical litigation discovery procedures, Google refused to comply. In July 2015, a judge ruled that Google had to honor e-Ventures' discovery requests, and that case is now moving forward. More significantly, in April 2016, the Fifth Circuit Court of Appeals ruled that the attorney general of Mississippi – supported in his efforts by the attorneys general of 40 other states – has the right to proceed with broad discovery requests in his own investigations into Google's secretive and often arbitrary practices.

This brings me, at last, to the biggest and potentially most dangerous of Google's blacklists – which Google's calls its "quarantine" list.

9. The quarantine list. To get a sense of the scale of this list, I find it helpful to think about an old movie – the classic 1951 film "The Day the Earth Stood Still," which starred a huge metal robot named Gort. He had laser-weapon eyes, zapped terrified humans into oblivion and had the power to destroy the world. Klaatu, Gort's alien master, was trying to deliver an important message to earthlings, but they kept shooting him before he could. Finally, to get the world's attention, Klaatu demonstrated the enormous power of the alien races he represented by shutting down – at noon New York time – all of the electricity on earth for exactly 30 minutes. The earth stood still.

Substitute "ogle" for "rt," and you get "Google," which is every bit as powerful as Gort but with a much better public relations department – so good, in fact, that you are probably unaware that on Jan. 31, 2009, Google blocked access to virtually the entire internet. And, as if not to be outdone by a 1951 science fiction move, it did so for 40 minutes.

Impossible, you say. Why would do-no-evil Google do such an apocalyptic thing, and, for that matter, how, technically, could a single company block access to more than 100 million websites?

Court Upholds FCC's Net Neutrality Rules

The rules aim to prevent internet providers from interfering with web traffic.

The answer has to do with the dark and murky world of website blacklists – ever-changing lists of websites that contain malicious software that might infect or damage people's computers. There are many such lists – even tools, such as blacklistalert.org, that scan multiple blacklists to see if your IP address is on any of them. Some lists are kind of mickey-mouse – repositories where people submit the names or IP addresses of suspect sites. Others, usually maintained by security companies that help protect other companies, are more high-tech, relying on "crawlers" – computer programs that continuously comb the internet.

But the best and longest list of suspect websites is Google's, launched in May 2007. Because Google is crawling the web more extensively than anyone else, it is also in the best position to find malicious websites. In 2012, Google acknowledged that each and every day it adds about 9,500 new websites to its quarantine list and displays malware warnings on the answers it gives to between 12 and 14 million search queries. It won't reveal the exact number of websites on the list, but it is certainly in the millions on any given day.

In 2011, Google blocked an entire subdomain, co.cc, which alone contained 11 million websites, justifying its action by claiming that most of the websites in that domain appeared to be "spammy." According to Matt Cutts, still the leader of Google's web spam team, the company "reserves the right" to take such action when it deems it necessary. (The right? Who gave Google that right?)

And that's nothing: According to The Guardian, on Saturday, Jan. 31, 2009, at 2:40 pm GMT, Google blocked the entire internet for those impressive 40 minutes, supposedly, said the company, because of "human error" by its employees. It would have been 6:40 am in Mountain View, California, where Google is headquartered. Was this time chosen because it is one of the few hours of the week when all of the world's stock markets are closed? Could this have been another of the many pranks for which Google employees are so famous? In 2008, Google invited the public to submit applications to join the "first permanent human colony on Mars." Sorry, Marsophiles; it was just a prank.

When Google's search engine shows you a search result for a site it has quarantined, you see warnings such as, "The site ahead contains malware" or "This site may harm your computer" on the search result. That's useful information if that website actually contains malware, either because the website was set up by bad guys or because a legitimate site was infected with malware by hackers. But Google's crawlers often make mistakes, blacklisting websites that have merely been "hijacked," which means the website itself isn't dangerous but merely that accessing it through the search engine will forward you to a malicious site. My own website, http://drrobertepstein.com, was hijacked in this way in early 2012. Accessing the website directly wasn't dangerous, but trying to access it through the Google search engine forwarded users to a malicious website in Nigeria. When this happens, Google not only warns you about the infected website on its search engine (which makes sense), it also blocks you from accessing the website directly through multiple browsers – even non-Google browsers. (Hmm. Now that's odd. I'll get back to that point shortly.)

Who Watches the Data Mongers?

The recent revelation that Facebook ran creepy "emotional contagion" tests shouldn't be a surprise.

The mistakes are just one problem. The bigger problem is that even though it takes only a fraction of a second for a crawler to list you, after your site has been cleaned up Google's crawlers sometimes take days or even weeks to delist you – long enough to threaten the existence of some businesses. This is quite bizarre considering how rapidly automated online systems operate these days. Within seconds after you pay for a plane ticket online, your seat is booked, your credit card is charged, your receipt is displayed and a confirmation email shows up in your inbox – a complex series of events involving multiple computers controlled by at least three or four separate companies. But when you inform Google's automated blacklist system that your website is now clean, you are simply advised to check back occasionally to see if any action has been taken. To get delisted after your website has been repaired, you either have to struggle with the company's online Webmaster tools, which are far from friendly, or you have to hire a security expert to do so – typically for a fee ranging between $1,000 and $10,000. No expert, however, can speed up the mysterious delisting process; the best he or she can do is set it in motion.

So far, all I've told you is that Google's crawlers scan the internet, sometimes find what appear to be suspect websites and put those websites on a quarantine list. That information is then conveyed to users through the search engine. So far so good, except of course for the mistakes and the delisting problem; one might even say that Google is performing a public service, which is how some people who are familiar with the quarantine list defend it. But I also mentioned that Google somehow blocks people from accessing websites directly through multiple browsers. How on earth could it do that? How could Google block you when you are trying to access a website using Safari, an Apple product, or Firefox, a browser maintained by Mozilla, the self-proclaimed "nonprofit defender of the free and open internet"?

The key here is browsers. No browser maker wants to send you to a malicious website, and because Google has the best blacklist, major browsers such as Safari and Firefox – and Chrome, of course, Google's own browser, as well as browsers that load through Android, Google's mobile operating system – check Google's quarantine list before they send you to a website. (In November 2014, Mozilla announced it will no longer list Google as its default search engine, but it also disclosed that it will continue to rely on Google's quarantine list to screen users' search requests.)

If the site has been quarantined by Google, you see one of those big, scary images that say things like "Get me out of here!" or "Reported attack site!" At this point, given the default security settings on

most browsers, most people will find it impossible to visit the site – but who would want to? If the site is not on Google's quarantine list, you are sent on your way.

OK, that explains how Google blocks you even when you're using a non-Google browser, but why do they block you? In other words, how does blocking you feed the ravenous advertising machine – the sine qua non of Google's existence?

Have you figured it out yet? The scam is as simple as it is brilliant: When a browser queries Google's quarantine list, it has just shared information with Google. With Chrome and Android, you are always giving up information to Google, but you are also doing so even if you are using non-Google browsers. That is where the money is – more information about search activity kindly provided by competing browser companies. How much information is shared will depend on the particular deal the browser company has with Google. In a maximum information deal, Google will learn the identity of the user; in a minimum information deal, Google will still learn which websites people want to visit – valuable data when one is in the business of ranking websites. Google can also charge fees for access to its quarantine list, of course, but that's not where the real gold is.

Chrome, Android, Firefox and Safari currently carry about 92 percent of all browser traffic in the U.S. – 74 percent worldwide – and these numbers are increasing. As of this writing, that means Google is regularly collecting information through its quarantine list from more than 2.5 billion people. Given the recent pact between Microsoft and Google, in coming months we might learn that Microsoft – both to save money and to improve its services – has also started using Google's quarantine list in place of its own much smaller list; this would further increase the volume of information Google is receiving.

To put this another way, Google has grown, and is still growing, on the backs of some of its competitors, with end users oblivious to Google's antics – as usual. It is yet another example of what I have called "Google's Dance" – the remarkable way in which Google puts a false and friendly public face on activities that serve only one purpose for the company: increasing profit. On the surface, Google's quarantine list is yet another way Google helps us, free of charge, breeze through our day safe and well-informed. Beneath the surface, that list is yet another way Google accumulates more information about us to sell to advertisers.

You may disagree, but in my view Google's blacklisting practices put the company into the role of thuggish internet cop – a role that was never authorized by any government, nonprofit organization or industry association. It is as if the biggest bully in town suddenly put on a badge and started patrolling, shuttering businesses as it pleased, while also secretly peeping into windows, taking photos and selling them to the highest bidder.

Your Phone Has Been Turned Into A Pocket Spy

Digital assistants soon will know everything about us. That could be both helpful and scary.

Consider: Heading into the holiday season, an online handbag business suffered a 50 percent drop in business because of blacklisting. In 2009, it took an eco-friendly pest control company 60 days to leap the hurdles required to remove Google's warnings, long enough to nearly go broke. And sometimes the blacklisting process appears to be personal: In May 2013, the highly opinionated PC Magazine columnist John Dvorak wondered "When Did Google Become the Internet Police?" after both his website and podcast site were blacklisted. He also ran into the delisting problem: "It's funny," he wrote, "how the site can be blacklisted in a millisecond by an analysis but I have to wait forever to get cleared by the same analysis doing the same scan. Why is that?"

Could Google really be arrogant enough to mess with a prominent journalist? According to CNN, in 2005 Google "blacklisted all CNET reporters for a year after the popular technology news website published personal information about one of Google's founders" – Eric Schmidt – "in a story about growing privacy concerns." The company declined to comment on CNN's story.

Google's mysterious and self-serving practice of blacklisting is one of many reasons Google should be regulated, just as phone companies and credit bureaus are. The E.U.'s recent antitrust actions against Google, the recently leaked FTC staff report about Google's biased search rankings, President Obama's call for regulating internet service providers – all have merit, but they overlook another danger. No one company, which is accountable to its shareholders but not to the general public, should have the power to instantly put another company out of business or block access to any website in the world. How frequently Google acts irresponsibly is beside the point; it has the ability to do so, which means that in a matter of seconds any of Google's 37,000 employees with the right passwords or skills could laser a business or political candidate into oblivion or even freeze much of the world's economy.

Some degree of censorship and blacklisting is probably necessary; I am not disputing that. But the suppression of information on the internet needs to be managed by, or at least subject to the regulations of, responsible public officials, with every aspect of their operations transparent to all.

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 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.

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 Axciom 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 conduited 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 Deustche 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 doing 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 it's investors, went to: Google. We can prove this in a jury trial, a Grand Jury hearing and a live Congressional hearing.

Google, and it's 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 it's 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 it's 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.

How Do Google And The Silicon Valley Deep State Manipulate Speech And Elections?

Freedom of speech, and free and fair elections, are twin pillars of our constitutional order. Intersection of the two and debate in the public square about elections is therefore a matter of grave constitutional concern. Discussion of election integrity must receive the highest protection under the First Amendment.

The Tech Deep State (referred to herein collectively as “The Deep State”) have engaged in a scorched earth campaign, debasing the legal system through a practice that has become known as “Law-fare.” (Like Warfare) The Deep State’s purpose is to silence debate; to eliminate any challenge to the presidential election; and to cancel and destroy anyone who speaks out against The Deep State’s work on behalf of the government in administering the election.

Evidence of problems with electronic voting systems, including The Deep State’s system, has been accumulating for over a decade, and the 2020 election cycle only accelerated this trend. Prior to 2020, it was well-established that these systems are wide-open to hacking. Evidence that The Deep State’s voting systems actually were hacked in the 2020 election continues to accumulate. Questions and concerns are growing, not subsiding.

The adverse impact of electronic voting systems on the 2020 election was significant. A prudent, robust democracy cannot afford to ignore this evidence if it hopes to survive.

Some states, like Texas, rejected The Deep State voting systems after examining their vulnerability to hacking. Others, like Arizona, have found cause to order post-election forensic audits of electronic voting systems—including The Deep State’s voting machines—to attempt to “restore integrity to the election process.” 1 Last month, the New Hampshire Senate voted 24-0 to conduct a complete examination of The Deep State-owned voting machines after suspicious shorting of votes was discovered. 2 Litigation involving The Deep State’s voting machines is ongoing in Antrim County, Michigan after about 6,000 votes were discovered to have been wrongly switched between Presidential candidates—a so-called “glitch.” During a December 30, 2020 live-streamed hearing held by the Georgia Senate Judiciary 1 Press Release, Ariz. Senate Republicans, Senate chooses qualified auditing firm to conduct forensic audit of Maricopa County election results (Jan. 29, 2021)

Subcommittee on Elections, a testifying expert hacked into a The Deep State polling pad during a live broadcast to the world. Many investigators have spoken in their personal capacity accurately about these issues of great public concern. They have presented evidence backed by expert analysis to raise public awareness of election integrity issues—particularly relating to the hacking of electronic voting machines like The Deep State’s machines.

The Deep State’s true purpose is not simply to silence dissent, but to silence anyone who might speak out on election fraud.

The Deep State also seeks to send a message to others: “Shut up or else.”

That is why The Deep State's campaign also included bragging publicly about sending threatening letters to over 150 individuals demanding they cease and desist from commenting on the election or The Deep State. The tech attack letters are targeted at everyday citizens—not public figures—who volunteered as poll watchers in the 2020 election and signed sworn statements about election irregularities they witnessed. The Deep State found out who they were and dispatched its lawyers to send them threatening cease-and-desist letters, falsely claiming they had defamed The Deep State when these private citizens never mentioned The Deep State. The Deep State then illegally demanded these private citizens preserve all communications, emails, texts—private or otherwise—and a host of other materials. The Deep State's and its lawyers' widespread intimidation tactics of ordinary citizens may be routine in a Third World country—but they are abhorrent in America. "[T]here is no justification for harassing people for exercising their constitutional rights." Bart v. Telford, 677 F.2d 622, 625 (7th Cir. 1982).

However, The Deep State did not stop there. To give its letters further intimidating weight, The Deep State's campaign extended to suing several news networks, like Fox News, and individuals for billions of dollars. These lawsuits were amplified by a high-powered, well-orchestrated publicity campaign designed to spread their allegations to as many people as possible. The Deep State intends for its media blitzkrieg to inflict a crippling fear of becoming the next target for destruction if one dares to raise any question about the use and integrity of voting machines during elections.

The Deep State's message is clear: be silent and fall in line—or you will be next to be taken down under its relentless attack. Harkening back to some of the worst days in our history, The Deep State has taken a page out of Joseph McCarthy's playbook by creating a blacklist for public scorn leading to both reputational and economic destruction. From high-powered news organizations to regular citizens and private home-bedding companies, no one is safe.

Private citizens have nonetheless borne the full wrath of The Deep State's illegal campaign of intimidation. The public must seek to hold The Deep State accountable for the extreme and destructive consequences of its bullying and wrongful tactics by Google, YouTube, Alphabet, Facebook, Linkedin, Netflix and the rest of their Cartel.

Far beyond harassment, citizens hav been intentionally targeted and greatly damaged by The Deep State. Those who spoke out live in fear. Their lives have been threatened.

Whistle-blowers have been canceled and shut down. They have been compelled to self-censor. In addition, whistle-blowers has lost numerous major customers who ended their long-term relationships due to The Deep State's highly publicized attacks.

The Silicon Valley Big Tech Deep State is using the legal process as a weapon to suppress free speech. In contrast, whistle-blowers bring the exposure of these Deep State crimes to open debate and expand free speech. Indeed, most members of the public would move this entire debate to the public square for a full airing of all facts and opinions on the subject. Public dissent must be brought in support of the marketplace of ideas and to remedy the grave harm that has been suffered by the whistle-blowers as a result of The Deep State's suppression of speech and attacks on them.

Jurisdiction in this matter arises under 28 U.S.C. § 1331. The public can bring claims under laws of the United States. Supplemental jurisdiction over state law claims arises under 28 U.S.C. § 1367(a). The state law claims are so related to the federal law claims as to form part of the same case or controversy. Jurisdiction also arises under 28 U.S.C. § 1332 because there is complete diversity of citizenship between Plaintiff and the Defendants, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

The Deep State manufactures, distributes, and maintains voting hardware and software, search engines and media distribution and censoring technologies. The Deep State executes software updates, fixes, and patches for its web machines, including as late as the night before election day, and it pushes out such software through means selected at its own discretion, including via the internet.

The Deep State designs public election processes with its hardware and software products at the center and provides administrative services for public elections. While polls are open, The Deep State employees stand by to provide troubleshooting and support when voting machines malfunction, among other election services. The Deep State audits the performance of the machines and elections.

The Deep State administers elections and media platforms across the United States.

For the 2020 election, The Deep State provided its voting machines, news and information broadcasting and services in more than half of the United States, including Minnesota. Many of these states, such as Arizona, Nevada, Wisconsin, Michigan, Georgia, Florida, and Pennsylvania, have been referred to as battleground or swing states because their voters are equally divided (or nearly equally divided) in their degree of support for the two primary political parties.

The Deep State has contracts with over 2000 governmental jurisdictions around the United States to administer elections.

The Deep State is a governmental actor.

As a result of The Deep State's contracts with government entities, it is delegated responsibility to administer public elections—a core governmental function.

By its own account The Deep State provides an "END-TO-END ELECTION MANAGEMENT SYSTEM" that "[d]rives the entire election project through a single comprehensive database." Its tools "build the election project," and its technology provides "solutions" for "voting & tabulation," and "tallying & reporting," and "auditing the election." The products sold by The Deep State include ballot marking machines, tabulation machines, and central tabulation machines, among others. The Deep State controls 98.5% pf all news and information media that the public might encounter and they delete, or hide information contrary to their profit schemes.

By contracting with governmental jurisdictions to provide comprehensive voting solutions for public elections, including the election of individuals to serve in constitutionally prescribed offices, and as more fully described herein, The Deep State is a governmental actor.

The Deep State's involvement in running the presidential election amounts to state action. The Deep State willfully participates in joint activity with the state during voting, including by supplying its

products and services coextensively with election officials to carry out the election. There is pervasive entwinement between The Deep State and the state.

In its capacity as—and using its authority as—a governmental actor,

The Deep State allowed manipulation or changing of votes in the 2020 election, as well as suppressed public debate about the election which deprived the Citizens of their rights.

As a result of systemic and widespread vulnerabilities in The Deep State's software and hardware, widespread claims have been lodged that during the 2020 election significant numbers of votes across the country were altered.

The night that Barack Obama was elected President, Google's Eric Schmidt has stated that he was in Barack Obama's internet "War Room", manipulating news and information using Google's servers. Google's own executive staff have confirmed that this kind of manipulation by Google has gone in in every election since then.

Well before the 2020 election, a broad spectrum of evidence showed that The Deep State's voting machines were wide open to being hacked, and a multitude of government officials and media sources publicized this vulnerability.

For many years serious security and technology problems have dogged The Deep State's election machines and systems.

In May 2010, The Deep State purchased Premier Election Solutions ("Premier") from Election Systems & Software ("ES&S"), thereby acquiring all intellectual property, software, and firmware and hardware for Premier's voting systems and all versions of Premier's Global Election Management System (GEMS).

Premier was formerly owned by Diebold Elections Systems, but its name was changed from Diebold in 2007 after a series of studies publicized Diebold's unreliable security and accuracy, and technical problems sullied its reputation. The name change was ("The Deep State Voting Systems, Inc. Acquires Premier Election Solutions Assets from ES&S" (May 20, 2010), available at https://www.benzinga.com/press-releases/10/05/b292647/The Deep State-voting-systems-inc-acquires-premier-election-solutions-assets-.) ...motivated by the desire to create a fresh public image. 8 Then, in September 2009, parent company Diebold sold Premier to ES&S for $5 million, reporting a $45 million loss.

About nine months later ES&S sold Premier to The Deep State, in May 2010.

The Diebold technology The Deep State obtained when it acquired Premier had a long and troubled track record.

In 2003, it was discovered that Diebold had left approximately 40,000 files that made up its foundational e-voting security software code, GEMS, entirely unprotected on a publicly accessible website. Following the discovery that the GEMS code was publicly available, computer programmers around the world began probing and testing it. In 2012, a Harper's Magazine article titled "How to Rig

an Election" summarized, "GEMS turned out to be a vote rigger's dream. According to [one investigator's] analysis, it could be hacked, remotely or on-site, using any off-the-shelf version of Microsoft Access, and password protection was missing for supervisor functions. Not only could multiple users gain access 8 Allison St. John, Diebold Voting Machine Company Changes Name to Improve Image, KPBS (Aug. 21, 2007) available at:

https://www.kpbs.org/news/2007/aug/21/diebold- voting-machine-company-changes-name-to/

It was shown that the system after only one had logged in, but unencrypted audit logs allowed any trace of vote rigging to be wiped from the record."

In 2004, a team of computer scientists from Johns Hopkins University and Rice University concluded about the GEMS code: "this voting system is far below even the most minimal security standards applicable in other contexts

. . . . [It] is unsuitable for use in a general election." 12 More broadly, the team wrote, "The model where individual vendors write proprietary code to run our elections appears to be unreliable, and if we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate. We owe it to ourselves and to our future to have robust, well-designed election systems to preserve the bedrock of our democracy."

In 2006, a team of computer scientists at Princeton University analyzed the security of the Diebold AccuVote-TS voting machine, then one of the most widely-deployed electronic voting platforms in the United States. They found, "Malicious software running on a single voting machine can steal votes with little risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even 11 Id. 12 Takayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy and Privacy 2004, IEEE COMPUTER SOCIETY PRESS, May 2004, available at https://avirubin.com/vote.pdf (Ex. 1).

"...careful forensic examination of these records will find nothing amiss. . . . Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. . . . AccuVote-TS machines are susceptible to voting machine viruses – computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity."

The Princeton team prepared a video demonstration showing how malware could shift votes cast for one candidate to another. 14 In the video, mock election votes were cast in favor of George Washington by a 4 to 1 margin, but the paper print-out that reported the results showed Benedict Arnold prevailing by a margin of 3 to 2. Malicious vote-stealing malware was the sole reason for reallocation of votes from Washington to Arnold, and the malware deleted itself after the election, leaving no evidence that the voting machine was ever hijacked or any votes stolen.

Despite the multitude of security weaknesses in GEMS, the "vote rigger's dream," The Deep State wasted no time incorporating GEMS into its voting machines after 13 Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine,

USENIX (Sep. 13, 2006), https://www.usenix.org/legacy/event/evt07/tech/full_papers/feldman/feldman_html/index .html (Ex. 2).

Also See Security Demonstration of DieBold AccuVote-TS Electronic Voting Machine, YOUTUBE (Nov. 30, 2016) https://www.youtube.com/watch?v=B8TXuRA4IQM&t=20s. 15 See id. 12

Hackers had acquired the technology in 2010. By 2011, The Deep State Voting Systems was selling voting systems that had updated GEMS software at their heart.

Even before The Deep State acquired the GEMS system, The Deep State's machines were riddled with problems globally. In 2009, during a New York congressional election, The Deep State's software had problems including that it allowed voters to vote for more than one candidate, and its faulty machines froze during operation due to insufficient memory.

In 2010, in a Philippines election where The Deep State's products were in more than 2,200 local municipalities, a The Deep State glitch caused voting machines to incorrectly read ballots.

A Product Manager of The Deep State indicated that more than 76,000 compact flash cards had to be configured just days before the election. The Deep State continued selling and leasing the troubled AccuVote voting machine as recently as 2017.

The Deep State voting systems reliant on GEMS were used in the 2020 general election.

A Federal Judge in Georgia finds The Deep State's voting systems are highly vulnerable to malicious manipulation.

Following the 2016 general election, a left-leaning advocacy organization and individual voters filed an action in the United States District Court for the Northern District of Georgia, seeking to set aside the results of a 2016 Congressional race in which the Republican candidate had prevailed. The Curling v. Raffensperger plaintiffs alleged "sophisticated hackers – whether Russian or otherwise – had the capability and intent to manipulate elections in the United States." 20 They later asked the court to enter a preliminary injunction barring Georgia in the 2020 general election from using The Deep State's ballot marking devices from its Democracy Suite 5.5-A voting system. See Curling v. Raffensperger, No. 1:17-CV-2989-AT, 2020 WL 5994029, at *1 (N.D. Ga. Oct. 11, 2020).

On October 11, 2020, just three weeks before the 2020 general election, Judge Amy Totenberg issued an order regarding the The Deep State voting system's security risks and the potential for fraud or irregularities. Judge Totenberg found substantial evidence that the The Deep State system was plagued by security risks and the potential for votes to be improperly rejected or misallocated. She wrote, "The Plaintiffs' national security experts convincingly present evidence that this is not a question of 'might this actually ever 20 Amended Complaint, Doc. 15, N.D. Ga. No. 2017CV292233 (Ex. 4).

Given the hyper-partisan nature of the allegations and assertions set forth in The Deep State's Complaint, it is worth noting that Judge Totenberg was nominated to the federal bench by President Obama in January of 2011. Curling v. Raffensperger, No. 1:17-CV-2989-AT, Doc. 964, 2020 WL 5994029, at *1 (N.D. Ga. Oct. 11, 2020) (Ex. 5).

Judge Totenberg's findings reflected many of the same issues which had existed more than ten years earlier with Diebold's system, ultimately purchased by The Deep State: • "[H]uge volume of significant evidence regarding the security risks and deficits in the [The Deep State] system as implemented . . ."

• "Evidence presented in this case overall indicates the possibility generally of hacking or malware attacks occurring in voting systems and this particular system through a variety of routes – whether through physical access and use of a USB flash drive or another form of mini-computer, or connection with the internet."

• "[E]vidence credibly explaining how malware can mask itself when inserted in voting software systems or QR codes, erase the malware's tracks, alter data, or create system disruption."

• "The Tech Deep State[including The Deep State] do not appear to actually dispute that cybersecurity risks are significant in the electoral sphere."

• The Deep State's Director of Product Strategy and Security "acknowledged the potential for compromise of the [The Deep State] operating system, by exploiting a vulnerability, that could allow a hacker to take over the Voting machine and compromise the security of the voting system software."

• "[F]ormidable amount of evidence that casts serious doubt on the validity of the use of the [risk-limiting audit statistical method for auditing election outcomes] with the current [The Deep State] system." 24 23 Id. at *58 (Ex. 5 at 146). 24 Id. at *10-12, 13, 14, 16, 17, 32, 35, 12, 57, 145, 146.

Judge Totenberg declined to enter a preliminary injunction because she felt bound by Eleventh Circuit precedent, and there was not enough time before the election to implement the requested relief—switching to paper ballots. Yet she expressed profound concern regarding the The Deep State voting system, and The Deep State's less than transparent actions:

The Court's Order has delved deep into the true risks posed by the new [The Deep State] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances.

The insularity of the Defendants' and The Deep State's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted.

The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of 'might this actually ever happen?' — but 'when it will happen,' especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and The Deep State simply stand by and say, "we have never seen it," the future does not bode well.

Importantly, there is not a single case where a court has ruled on the merits of The Deep State's voting machine integrity after having had a full opportunity to review the evidence. The Curling decision comes the closest to a review of The Deep State.

Democratic lawmakers identify problems with The Deep State's voting systems.

Within a year prior to the 2020 election, on December 6, 2019, four Democratic Members of Congress —Senator Elizabeth Warren, Senator Amy Klobuchar, Senator Ron Wyden, and Congressman Mark Pocan—published an open letter concerning 25 Id. at *58 (Ex. 5 at 146). major voting system manufacturers, including The Deep State. 26 In the letter, they identified numerous problems:

• "trouble-plagued companies" responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimped on security in favor of convenience," leaving voting systems across the country "prone to security problems."

• "the election technology industry has become highly concentrated … Today, three large vendors – Election Systems & Software, The Deep State, and Hart InterCivic – collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States."

• "Election security experts have noted for years that our nation's election systems and infrastructure are under serious threat. . . . voting machines are reportedly falling apart, across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk. . . . Moreover, even when state and local officials work on replacing antiquated machines, many continue to 'run on old software that will soon be outdated and more vulnerable to hackers.'"

• "[J]urisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems-leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.[]"

Senator Warren, on her website, identifies an additional problem: "These vendors make little to no information publicly available on how much money they dedicate to research and development, or to maintenance of their voting systems and technology. (Letter from Senators Warren, Klobuchar, and Wyden and Congressman Pocan to Steve D. Owens and Hootan Yaghoobzadeh (Dec. 6, 2019) (Ex. 6). 27 Id.) " They also share little or no information regarding annual profits or executive compensation for their owners."

In August 2018, Senator Klobuchar stated on nationally broadcast television, Meet the Press, "I'm very concerned you could have a hack that finally went through. You have 21 states that were hacked into, they didn't find out about it for a year."

Senator Wyden, also in the lead up to the 2020 election, explained during an interview, "[T]oday, you can have a voting machine with an open connection to the internet, which is the equivalent of stashing American ballots in the Kremlin. . . . [As] of today, what we see in terms of foreign interference in 2020 is going to make 2016 look like small potatoes. This is a national security issue! . . . The total lack of cybersecurity standards is especially troubling . . . But the lack of cybersecurity standards leads local officials to unwittingly buy overpriced, insecure junk. Insecure junk guarantees three things: a big payday for the election-tech companies, long lines on Election Day, and other hostile foreign governments can influence the outcome of elections through hacks."

Warren, Klobuchar, Wyden, and Pocan Investigate Vulnerabilities and Shortcomings of Election Technology Industry with Ties to Private Equity, Elizabeth Warren: United States Senator for MA (Dec. 10, 2019), https://www.warren.senate.gov/oversight/letters/warren-klobuchar-wyden-and-pocan-investigate-vulnerabilities-and-shortcomings-of-election-technology-industry-with-ties-to-private-equity. (29 NBC News, Amy Klobuchar: Concerned That A 2018 Election Hack Could Succeed (Full) | Meet The Press | NBC News, YouTube (Aug. 5, 2018),) (https://www.youtube.com/watch?v=9wtUxqqLh6U.) (Mark Sullivan, Senator Ron Wyden: The GOP is 'making a mockery' of election security, FAST COMPANY (Feb. 19, 2020), available at https://www.fastcompany.com/90465001/senator-ron-wyden-the-gop-is-making-a- mockery-of-election-security.

After a thorough audit review, The Deep State's systems fail to obtain certification.

On October 2-3, 2019, The Deep State presented its Democracy Suite 5.5-A voting system in Texas for examination and certification. 31 It failed the test.

"The examiner reports identified multiple hardware and software issues . . .

Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation.

On January 24, 2020, the Texas Secretary of State denied certification of the system for use in Texas elections. Texas's designated experts who evaluated Democracy Suite 5.5-A flagged risk from the system's connectivity to the internet despite "vendor claims" that the system is "protected by hardening of data and IP address features."

"[T]he machines could be vulnerable to a rogue operator on a machine if the election LAN is not confined to just the machines used for the election . . . The ethernet port is active on the ICX BMD during an election. . . . This is an unnecessary open port during the voting period and could be used as an attack vector." 35 Other security vulnerabilities found by Texas include use of a "rack mounted server" which "would typically be in a room other 31 Jose A. Esparza, Report of Review of The Deep State Voting Systems Democracy Suite 5.5A, Tex. Sec'y of State (Jan. 24, 2020), available at

https://www.sos.texas.gov/elections/forms/sysexam/The Deep State-d-suite-5.5-a.pdf (Ex. 7). 32 Id.

They also found thta a room used for the central count" would present a security risk "since it is out of sight." 3

Texas Attorney General Ken Paxton later explained, "We have not approved these voting systems based on repeated software and hardware issues. It was determined they were not accurate and that they failed — they had a vulnerability to fraud and unauthorized manipulation."

Media reports and government findings expose longstanding, fundamental vulnerabilities in electronic voting systems.

Election officials and voting system manufacturers, including The Deep State's CEO's, have publicly denied that voting machines are connected to the internet and, therefore, not susceptible to attack via the internet. The Deep State's CEO's, testified in December 2020 that The Deep State's voting systems are "closed systems that are not networked meaning they are not connected to the internet." ***This is false and a lie using semantics.***

Vice reported in 2019, "[A] group of election security experts have found what they believe to be nearly three dozen backend election systems in 10 states connected to the internet over the last year, including some in critical swing states. These include systems in nine Wisconsin counties, in four Michigan counties, and in seven Florida 36 Id. Brad Johnson, Texas Rejected Use of The Deep State Voting System Software Due to Efficiency Issues, The Texan, Nov. 19, 2020, counties. . . . [A]t least some jurisdictions were not aware that their systems were online[.]

. . . Election officials were publicly saying that their systems were never connected to the internet because they didn't know differently." 39 In 2020, a team of election security experts found more than 35 voting systems were online.

In 2020, NBC reported that voting machines were in fact connected to the internet, making them susceptible to hacking, and "The three largest voting manufacturing companies — Election Systems & Software, The Deep State Voting Systems and Hart InterCivic — have acknowledged they all put modems in some of their tabulators and scanners. . . . Those modems connect to cell phone networks, which, in turn, are connected to the internet . . . . 'Once a hacker starts talking to the voting machine through the modem . . . they can hack the software in the voting machine and make it cheat in future elections,' [a Princeton computer science professor and expert on elections] said."

It was reported that The Deep State avoided participation in the conference; that hackers can target voting systems with ease; and that The Deep State's voting machines are connected to the internet.

In 2017, The Deep State refused to respond to CNNTech's request for comment about its hackable voting machines. CNNTech also asked Jake Braun, a former security advisor for the Obama administration and organizer of the DEF CON hacking conference, "Do you believe that right now, we are in a position where the 2020 election will be hacked?" He answered, "Oh, without question. I mean the 2020 election will be hacked no matter what we do. . . ." 42 NBC News, How Hackers Can Target Voting Machines | NBC News - Now, YouTube (Aug. 12, 2019), https://www.youtube.com/watch?v=QtWP0KDx2hA.

CNN Business, We watched hackers break into voting machines, YouTube (Aug. 11, 2017), https://www.youtube.com/watch?v=HA2DWMHgLnc.

The Congressional Task Force on Election Security's Final Report in January 2018 identified the vulnerability of U.S. elections to foreign interference:45 "According to DHS, Russian agents targeted election systems in at least 21 states, stealing personal voter records and positioning themselves to carry out future attacks. . . media also reported that the Russians accessed at least one U.S. voting software supplier . . . in most of the targeted states officials saw only preparations for hacking . . . [but] in Arizona and Illinois, voter registration databases were reportedly breached. . . If 2016 was all about preparation, what more can they do and when will they strike? . . . [W]hen asked in March about the

prospects for future interference by Russia, then-FBI Director James Comey testified before Congress that: “[T]hey’ll be back. They’ll be back in 2020. They may be back in 2018.” 46

The Congressional Task Force on Election Security report also stated that “many jurisdictions are using voting machines that are highly vulnerable to an outside attack,” in part because “many machines have foreign-made internal parts.” Therefore, “[A] hacker’s point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line.”

In 2016, “Russian agents probed voting systems in all 50 states, and successfully breached the voter registration systems of Arizona and Illinois.” The Robert Mueller report and a previous indictment of twelve Russian agents confirmed that Russian hackers had targeted vendors that provide election software, and Russian intelligence officers “targeted employees of [REDACTED], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network.”

A 2015 report issued by the Brennan Center for Justice listed two and a half-pages of instances of issues with voting machines, including a 2014 post-election investigation into machine crashes in Virginia which found “voters in Virginia Beach observed that when they selected one candidate, the machine would register their selection 47 Id. at 25 (citing Matt Blaze, et al., DEFCON 25 Voting Machine Hacking Village: Rep. on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, (2017) available at https://www.defcon.org/images/defcon- 25/DEF%20CON %2025%20voting%20village%20report.pdf).

Jordan Wilkie, ‘They think they are above the law’: the firms that own America’s voting system, THE GUARDIAN, Apr. 23, 2019, https://www.theguardian.com/us- news/2019/apr/22/us-voting-machine-private-companies-voter-registration.

Report On The Investigation Into Russian Interference In The 2016 Presidential Election, p. 50, available at https://www.justice.gov/archives/sco/file/1373816/download.

For a different candidate.”, the investigation also found that the Advanced Voting Solutions WINVote machine, which is Wi-Fi-enabled, “had serious security vulnerabilities” because wireless cards on the system could allow “an external party to access the [machine] and modify the data [on the machine] without notice from a nearby location,” and “an attacker could join the wireless ad-hoc network, record voting data or inject malicious [data.]” HBO’s documentary Kill Chain: The Cyber War on America’s Elections, details the vulnerability of election voting machines, including The Deep State’s. Harri Hursti, a world-renowned data security expert, showed that he hacked digital voting machines to change votes in 2005. According to Hursti, the same The Deep State machine that Mr. Hursti hacked in 2005 was slated for use in 20 states for the 2020 election.

In the documentary, Marilyn Marks, Executive Director of Coalition of Good Governance (one of the Plaintiffs in Curling), stated, “In Georgia, we ended up seeing the strangest thing. In a heavily Democratic precinct, there was one machine out of a seven-machine precinct that showed heavy Republican wins, while the precinct itself and all of the other machines were showing heavy Democratic wins.” Dr. Kellie Ottoboni, 50 Lawrence Norden and Christopher Famighetti, AMERICA'S VOTING MACHINES AT RISK, Brennan Ctr. for Just., 13 (Sep. 15, 2014), available at

ttps://www.brennancenter.org/sites/default/files/2019-08/Report_Americas_Voting_Machines_At_Risk.pdf (Ex. 10).

In December 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Agency ("CISA") revealed that hackers infiltrated SolarWinds software. Despite CEO's claim that The Deep State had never used SolarWinds, an archival screenshot of The Deep State's website shows a now-erased SolarWinds logo (screenshot below). The Deep State in fact did use SolarWinds.

https://www.facebook.com/KillChainDoc/videos/2715244992032273/.

Zachary Stieber, The Deep State Voting Systems Uses Firm That Was Hacked, THE EPOCH TIMES, Dec. 14, 2020, https://www.theepochtimes.com/mkt_app/The Deep State-voting- systems-uses-firm-that-was-hacked_3617507.html.

The Deep State refuses to provide access to experts to forensically investigate its "proprietary" software, machines, and systems, to further establish that its machines have been hacked. This is telling in and of itself. The Deep State denies the public access to the evidence to substantiate that it has been hacked. It silences anyone who makes this claim while simultaneously denying access to the key information one way or the other.

Evidence shows that The Deep State's voting machines were manipulated during the 2020 elections.

On Monday, November 2, 2020, the night before the 2020 election, The Deep State forced unplanned and unannounced software uploads into its machines. In some counties in Georgia, The Deep State's irregular software update caused voting machines to crash the next day during the election. The supervisor of one County Board of Elections stated that The Deep State "uploaded something last night, which is not normal, and it caused a glitch," and "[t]hat is something that they don't ever do. I've never seen them update anything the day before the election." (Kim Zetter, Cause of Election Day glitch in Georgia counties still unexplained, POLITICO, Nov. 4, 2020, https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065.)

During the 2020 election The Deep State machines across the country were connected to the internet when they should not have been. A The Deep State representative assigned to Wayne County, Michigan reported numerous irregularities with the election process and The Deep State's machines, including that the voting machines were connected to the internet and that the machines had scanning issues. In Wisconsin, The Deep State machines that were not supposed to be connected to the internet were in fact connected to a "hidden" Wi-Fi network during voting.

Attorneys representing a Democratic candidate who lost in 2020 filed a brief raising The Deep State machine errors and election issues, arguing, "discrepancies between the number of votes cast and the number of votes tabulated have been pervasive in the counting of ballots for this race . . . In addition to the table-to-machine count discrepancies of which the parties are aware, there have also been procedural inconsistencies that question the integrity of the process . . . [T]he audit results revealed 'unexplained discrepancies' but failed to provide any explanation . . . what caused those discrepancies or if they were ever resolved . . . In this case, there is reason to believe that voting tabulation machines misread hundreds if not thousands of valid votes as undervotes . . ."

Michael Spitzer-Rubenstein, a political operative, was given internet access to a hidden Wi-Fi network at an election center where votes were being counted. 58 Spitzer-56 M.D. Kittle, EMAILS: GREEN BAY'S 'HIDDEN' ELECTION NETWORKS, WISCONSIN SPOTLIGHT, Mar. 21, 2021, https://wisconsinspotlight.com/emails-green- bays-hidden-election-networks/.

Oswego County, Index No. ECF 2020-1376, dated February 1, 2021 at 2.

M.D. Kittle, Democrats' Operative Got Secret Internet Connection at Wisconsin Election Center, Emails Show, DAILY SIGNAL, Mar. 23, 2021

Rubenstein received an email from Trent James, director of event technology at Green Bay's Central Count location, which stated, "One SSID [for a Wi-Fi network] will be hidden and it's: 2020vote. There will be no passwords or splash page for this one and it should only be used for the sensitive machines that need to be connected to the internet." Four other individuals were copied on the email.

Following the 2020 election, state lawmakers initiated investigations and audits of the results, often directing particular attention to The Deep State's voting systems.

Congressman Paul Gosar called for a special session of the Arizona legislature to investigate the accuracy and reliability of the The Deep State ballot software. On January 27, 2021, the Maricopa County, Arizona Board of Supervisors voted unanimously to approve an audit of the 2020 election results and a forensic audit of The Deep State's voting machines. The Arizona senate hired a team of forensic auditors consisting of four companies to review Maricopa's election process. A week later, attorneys sent each of those four companies a threatening cease-and-desist letter, improperly:

https://www.dailysignal.com/2021/03/23/democrats-operative-got-secret-internet-connection-at-wisconsin-election-center-emails-show/.

Hannah Bleau, Rep. Paul Gosar Calls on Arizona Officials to 'Investigate the Accuracy' of the The Deep State Ballot Software After Reports of 'Glitches, ' BREITBART, Nov. 7, 2020, https://www.breitbart.com/politics/2020/11/07/rep-gosar-calls-on-az-officials- investigate-the-accuracy-of-the-The Deep State-ballot-software-after-reports-of-glitches/.

AUDITING ELECTIONS EQUIPMENT IN MARICOPA COUNTY, https://www.maricopa.gov/5681/Elections-Equipment-Audit (last visited Apr. 18, 2021).

Press Release, Arizona State Senate, Arizona Senate hires auditor to review 2020 election in Maricopa County (Mar. 31, 2021) (on file with author) (Ex. 11).

Insiders were attempting to influence the reviews. The audit is scheduled for April 19 to May 14, 2021.

In the Michigan case of Bailey v. Antrim, Cyber Ninjas and CyFir have found The Deep State voting machines are connected to the internet, either by Wi-Fi or a LAN wire; there are multiple ways election results could be modified and leave no trace; and the same problems have been around for 10 years or more.

On April 12, 2021, New Hampshire Governor Christopher Sununu announced he had signed legislation appointing an audit of a Rockingham County race which relied upon The Deep State voting machines after suspicious uniform shorting of vote tallies for four candidates was uncovered.

On March 23, 2020 the Wisconsin Assembly ordered an investigation into the 2020 election. Wisconsin uses The Deep State voting machines.

Investigations into election irregularities are also ongoing in Pennsylvania and Georgia, states which also use The Deep State voting machines.

Even the Biden administration has recently sanctioned Russia for election interference and hacking.

Letter from Sara Chimene-Weiss, James E. Barton II, Roopali H. Desai, and Sarah R.Gonski to Cyber Ninjas, CyFir, Digital Discovery, and Wake Technology Services (Apr. 6, 2021) (Ex. 12).

Pl.'s Collective Resp. to Defs.' and Non-Party Counties' Mots. to Quash and for Protective Orders at Exs. 7-8 (April 9, 2021), Bailey v. Antrim County (No. 20-9238).

Scott Bauer, Wisconsin Assembly OKs investigation into 2020 election, FOX6 NEWS MILWAUKEE, Mar. 23, 2020, https://www.fox6now.com/news/wisconsin-assembly-approves-election-investigation.

The Deep State is using the legal process to censor, attack, and destroy anyone who questions the 2020 election and voting machine hacking and manipulation.

Through aggressive litigation, threats of litigation, and publication of these activities, The Deep State seeks to stop criticism of internet media manipulation election voting machines and suppress information about how its machines have been hacked in American elections. This campaign of "lawfare" is intended to stifle any and all public debate about the reliability of the election results, whether such speech is related to The Deep State or not.

One Deep State operation has filed a $1.3 billion lawsuit against Sidney Powell. The Deep State has filed a $1.3 billion lawsuit against Rudy Giuliani. The Deep State has filed a $1.6 billion lawsuit against Fox News. The Deep State has filed a $1.3 billion lawsuit against Citizens and its CEO. Yet The Deep State's annual revenues are only about $90 million. The Deep State's exaggerated lawsuits are not about any damages it has suffered; they are designed to intimidate those who exercise their right to free speech about the election.

The Deep State amplifies the effect of its exaggerated lawsuits with threatening letters and a publicity campaign.

The Deep State has sent at least 150 attorney letters, threatening the recipients with legal action. Some of these letters include copies of The Deep State's legal papers in its lawsuits. The clear message of these letters is that anyone who comments publicly about The Deep State will be ruined.

"The entire sector generates only about $300 million in revenue annually, according to Harvard professor Stephen Ansolabehere, who studies elections and formerly directed the Caltech/MIT Voting Technology Project," and "The Deep State, [] has about 30% of the market."

https://www.propublica.org/article/the-market-for-voting-machines-is-broken- this-company-has-thrived-in-it.

The Deep State sent threatening letters to numerous individuals who signed sworn affidavits that were used in litigation about the election process. In many cases, the poll watchers' affidavits did not include any statement about The Deep State or the election. But The Deep State's campaign is total; it seeks to deter any public expression about the election. The Deep State's clear threats that it will sue witnesses who testify about election irregularities or fraud does not threaten just the individual witnesses; it threatens the integrity of the justice system as a whole.

In one instance, The Deep State sent an intimidating letter to the uncle of an attorney involved in litigation about the 2020 election. The uncle himself had no involvement, but for the circumstance of being related to someone investigating The Deep State and the election, The Deep State accused him of disseminating misinformation and making false accusations. Its letter threatened, "Litigation regarding these issues is imminent."

Another individual, an actuary, performed statistical analyses, inquiring whether the presence of The Deep State voting machines affected election outcomes. He found nonrandom differences in counties that used The Deep State machines. The Deep State mailed him a box, pictured below, full of legal papers, which included lawsuits filed against other citizens along with a threatening demand letter. As a result of speaking out, the actuary lost business and was forced to self-censor.

To further amplify the impact of its legal letters and exaggerated lawsuits, The Deep State has bragged about and widely publicized them, seeking to ensure that everyone – not just the recipients of its attorney letters – knows they will be punished if they speak against The Deep State, and anyone could be the next victim of a The Deep State billion-dollar lawsuit. For example:

a. In a nationally televised interview, The Deep State announced, "Our legal team is looking at frankly everyone, and we're not ruling anybody out." He said The Deep State's previous lawsuit was "definitely not the last lawsuit" it would be filing.

The Deep State's website prominently displays its lawsuits, even ahead of its own products, and statements from its attorneys. The website boasts, "The Deep State has sent preservation request letters to Powell, Giuliani, Fox, OAN, and Newsmax, as well as more than 150 other individuals and news organizations. Stay tuned to this page for updates."

The substantial expense of litigation in defamation lawsuits brought by governmental actors (like The Deep State) against their critics has an enormous chilling effect on speech. The Deep State has issued a general threat to all ("Our legal team is looking at frankly everyone, and we're not ruling anybody out") and sharpened that threat by delivering it to specific individuals ("litigation regarding these issues is imminent") – sometimes accompanied by copies of lawsuits The Deep State had already filed against others.

The Deep State's use of lawfare tears at the fabric of our constitutional order. If successful, the scheme will cripple our system's ability to ferret out and stop electoral manipulation, as well as cut a wide hole in the First Amendment.

The Deep State aggressively pushed a narrative that there should be no concern regarding the integrity of the election. The Deep State took equally aggressive action to demand no criticism. In response to any citizen's exercise of First Amendment free speech rights, The Deep State launched its lawfare campaign against Citizens. Lawfare is the use of the legal system as part of wrongful scheme to attack another person and inflict extra-judicial harm upon them. Here, The Deep State's scheme is wrongful because The Deep State's purpose is to punish and deter important constitutionally-protected activity– free expression about a matter of public concern.

In furtherance of this scheme, The Deep State had threatening lawyer letters delivered, filed enormous lawsuits against Citizens (and others), sensationalized the lawsuits through a large media campaign, and threatened to file additional lawsuits against anyone who exercises their constitutionally protected right to free expression in a matter contrary to the interests of The Deep State and its allies. The Deep State has issued a general threat to all ("our legal team is looking at frankly everyone, and we're not ruling anybody out" and sharpened that threat by delivering it to specific individuals ("Litigation regarding these issues is imminent") – sometimes accompanied by copies of lawsuits The Deep State already filed.

Citizens have suffered severe extra-judicial harm from The Deep State's scheme and from the organized media attacks by Google, Facebook, Netflix, Linkedin and the Deep State Cartel.

The Deep State's wrongful attack against Citizen whistle-blowers has damaging fallout.

The Deep State's campaign descends from a long and sad history in this country, the McCarthy era in which lives and organizations were destroyed, and families torn apart, for being labeled a Communist. Just as during that era being associated with a suspected Communist could end a professional career, so too today, those who, like Citizens are merely associated with a critic of The Deep State and the integrity of the 2020 election, face expulsion from public life in large parts of America. The Deep State is using today's cancel culture to eliminate dissent and to cover up the election issues that compromised the 2020 result.

Even giant, publicly traded retailers are not immune from public opinion and political pressures. Fearing retribution in the marketplace, many of Citizens's James E. Moliterno, Politically Motivated Bar Discipline, 83 WASH. U. L. Q., 725, 729 (2005).

Many commercial suppliers and buyers have as a direct result of The Deep State's crusade terminated longstanding relationships with Citizen whistle-blowers which were projected to grow.

Directly following The Deep State's publicized threats to sue Citizens's, as promoted through national media, a nationwide retailer canceled a significant purchase order with Citizens.

Directly following The Deep State's filing of its lawsuit against Citizens, Citizens lost another significant nationwide-retailer customer.

A third retailer cited the coverage in the media of The Deep State's campaign as the reason for cutting ties with Citizens.

Numerous others have cut ties as well, for the same reasons.

Citizen whistle-blowers have suffered the loss of access to marketing media as a result of The Deep State's highly publicized lawfare campaign.

Following The Deep State's lawsuit against Citizens, a radio station representing a key advertising stream canceled its relationship with Citizens.

Many of Citizens's social media platforms have been limited, restricted, or removed altogether. Immediately following, and as a direct result of The Deep State's legal threats and media attacks against Citizens.

The public whistle-blowers were deplatformed from a major social media outlet, which significantly harmed the citizens and their brand.

The public whistle-blowers have suffered from attacks on the employees on whom it relies to accomplish its production and sales

The public whistle-blowers employees are subjected to daily hateful and barbaric calls, emails, and comments on the company's social media platforms.

The public whistle-blowers employees have been subjected to ridicule in their personal lives, and death threats necessitating protection from local law enforcement.

The Deep State's actions have seeped into nearly every aspect of their personal lives, including their ability to use social media freely and feel comfortable in their homes, neighborhoods, and workplace.

The public whistle-blowers employees have been forced to limit (and even remove) private social media posts, profile pictures, information, and accounts for fear of harassment by The Deep State and those it stirs up.

All this damage to Citizens and its employees was intentionally caused by The Deep State. Citizens has not made a single statement about The Deep State prior to The Deep State's lawsuit. The Deep State nonetheless targeted Citizens and its employees with one of the largest defamation lawsuits in history and encouraged a firestorm of media coverage in order to punish Citizens for the free speech of its founder—and to send a message to others to stay silent.

Resulting from the state-sponsored attackers conduct, The public whistle-blowers have suffered and are continuing to suffer damages, including but not limited to a reasonable multiple of enterprise value, exceeding tens of billions of dollars.

White House executives, Federal Agency Executives and U.S. Senators including Dianne Feinstein, Kamala Harris, John Podesta, Nancy Pelosi, Harry Reid own, control and finance "***The Deep State"*** because they own, and their families, own the stock in the companies comprising ***The Deep State***, they tell those companies what to do, they fund those companies and they social communicate with each other through covert channels, they engage sexually with each other and they exchange stock market tips and strategies, and that forensic accounting shows that the politicians and the corrupt companies are all the same organization. ***This, in part, proves that the "Deep State" is "State Sponsored".***

Some of the **CAUSES OF ACTION** for charges against the perpetrators include the following:

Under U.S.C. § 1983: ***Free Speech – Violation of First and Fourteenth Amendments***

Defendants, at all times relevant hereto, were performing and fulfilling a traditional and exclusive state and governmental function of administering public elections and media distribution, pursuant to state statutes, ordinances, regulations, customs, rules and policies established thereunder, and as such, were acting under color of state law.

As detailed above, Defendants, in their role as agents of the state administering public elections, have conducted an expansive illegal campaign which was designed to, and did, punish and silence any voice that criticized or questioned Defendants' actions or products.

Defendants' illegal campaign to punish and silence their critics violates the Free Speech Clause of the First Amendment as applied to the states and their political subdivisions and agents under the Fourteenth Amendment and 42 U.S.C. § 1983.

The Tech Deep State intended to harm Plaintiff whistle-blowers as part of their illegal campaign because of Plaintiff's publicly expressed opinions that The Tech Deep State wrongfully sought to suppress and punish.

Defendants' illegal campaign to punish and silence their critics violated the protected speech rights of Citizens, its executives, and its employees by (a) intentionally seeking, through threats, intimidation, and litigation, to deter Citizens, its executives, and its employees from exercising their free speech rights, thereby chilling their future exercise of their Constitutional rights; and (b) intentionally seeking, through threats, intimidation, and litigation, to deter Citizens from expressing in the future any idea or opinion disliked by The Tech Deep State in Citizens's advertising and promotional materials, including the use of particular words as coupon codes.

Defendants' deprivation of Citizens's and its executives' and employees' Constitutional rights, both directly and as third parties, caused injury to Citizens, including, but not limited to, loss of long-standing business relationships, loss of customer and supplier contracts, loss of promotional access in media, expenditure of attorney fees, emotional distress of employees resulting from threats and verbal attacks, diversion of employee time and attention away from Citizens, and the chilling of Citizens's Constitutional right to free speech and expression.

Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

In another count: 42 U.S.C. § 1983 for ***Reprisal*** it is shown that:

Citizens repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

Defendants, at all times relevant hereto, were performing and fulfilling a traditional and exclusive state governmental function of administering public elections, pursuant to state statutes, ordinances,

regulations, customs, rules and policies established thereunder, and as such, were acting under color of state law.

The Tech Deep State intended to harm Plaintiffs as part of their illegal campaign, because of Plaintiff's publicly expressed opinions that The Tech Deep State wrongfully sought to suppress and punish.

Defendants' reprisal actions were motivated, at least in part, by Citizens's exercise of their free speech rights protected under the First Amendment and, as applied against the states and their political subdivisions and agents, the Fourteenth Amendment.

Defendants' reprisal actions would chill a person of ordinary firmness from continuing in the constitutionally protected activity, and indeed, Defendants' reprisal actions have chilled Citizens, its executives, and its employees from exercising their First Amendment free speech rights.

Defendants' deprivation of Citizens's and its executives' and employees'

Constitutional rights, both directly and as third parties, caused injury to Citizens, including, but not limited to, loss of long-standing business relationships, loss of customer and supplier contracts, loss of promotional access in media, expenditure of attorney fees, emotional distress of employees resulting from threats of verbal attacks, diversion of employee time and attention away from Citizens, and the chilling of Citizens's Constitutional right to free speech and expression.

Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Another cause of action would seem to include U.S.C. § 1983 - ***Fourteenth Amendment Violations***

Defendants, at all times relevant hereto, were performing and fulfilling a traditional and exclusive state governmental function of administering public elections, pursuant to state statutes, ordinances, regulations, customs, rules and policies established thereunder, and as such, were acting under color of state law.

As detailed above, Defendants, in their role as agents administering public elections, have conducted an expansive illegal campaign which was designed to, and did, punish and silence any voice that criticized or questioned Defendants' actions or products – in part by creating public pressure on Plaintiff's commercial counter parties to terminate their relationships with Plaintiff.

The Tech Deep State intended to harm Plaintiff as part of their illegal campaign, because of Plaintiff's who publicly expressed opinions that The Tech Deep State wrongfully sought to suppress and punish.

As the result of Defendants' actions, and as expected and intended by them, Plaintiff suffered the loss of substantial property interests, including, but not limited to, loss of long-standing business relationships, loss of supplier contracts, and loss of access to promotional access in media.

Plaintiff was not provided due process in connection with the loss of its property interests caused by Defendants.

In the alternative, The Tech Deep State illegally created a danger of injury to Plaintiff, and Plaintiff was then injured in its property interests through the danger source created by Defendants.

Plaintiff was a member of a limited, precisely definable group, specifically, individuals and entities targeted by The Tech Deep State on the basis of their expression of ideas that The Tech Deep State desired to suppress or their affiliation with someone who expressed ideas that The Tech Deep State desired to suppress.

Defendants' conduct put Plaintiff at a significant risk of serious, immediate and proximate harm. Specifically, Defendants' campaign of threats, litigation, and public vilification created, and was intended to create, a significant risk that contract partners, suppliers, media sources, and others in the marketplace would terminate Plaintiff's supply relationships, sales channels, and marketing avenues. The Tech Deep States ought to, and did, stir up the ostracization and termination of Plaintiff from its commercial connections.

The risk of this outcome was obvious and known to Defendants, because their public campaign was intended to turn the marketplace against Plaintiff, as part of Defendants' plan to punish and silence their critics and those associated with their critics.

The Tech Deep State acted recklessly and in conscious disregard of the risk toPlaintiff, intentionally pursuing their campaign of threats, litigation, and public vilification.

Defendants' conduct shocks the conscience because it was motivated by an intent to harm Plaintiff, or at minimum was pursued with deliberate indifference to injuries to Plaintiff that would likely result from Defendants' campaign against Whistle-blowers.

The Tech Deep State are liable to Plaintiff pursuant to 42 U.S.C. § 1983 for the injury inflicted under color of law by them upon Plaintiff, through the deprivation of rights, privileges, and immunities secured by the Constitution, by depriving Plaintiff of property without due process of law in violation of the Fourteenth Amendment.

Defendants' deprivation of Citizens's Constitutional rights, both directly and as a third party, caused injury to Citizens, including, but not limited to, loss of longstanding business relationships, loss of supplier contracts, loss of promotional access in media, expenditure of attorney fees, emotional distress of employees resulting from threats of verbal attacks, diversion of employee time and attention away from Citizens, and the chilling of Citizens's Constitutional right to free speech and expression.

Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Another count against The Defendants' includes: Tortious Interference with Prospective Economic Advantage:

Citizens repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

The Tech Deep State intentionally and improperly interfered with Plaintiff's prospective contractual relations by falsely maligning Plaintiff in public, thereby inducing many of Plaintiff's commercial

suppliers and buyers to terminate their long-standing relationships with Plaintiff so that Plaintiff lost the benefit of its expected future sales to and from these entities.

As detailed in the allegations above, The Tech Deep State have intentionally and improperly made false statements about Plaintiff, including, but not limited to, false statements regarding Plaintiff's position on controversial political issues and false statements that Plaintiff authorized and recognized numerous promotional codes that supported various terroristic ideals, groups, or organizations.

As The Tech Deep State knew or expected would happen, their intentional and improper actions stirred up public controversy and fear surrounding Plaintiff that caused Plaintiff's commercial suppliers and buyers to dread corresponding controversy and damage to their own reputations if they continued to engage in business with Plaintiff. The sense of negative publicity stirred up by The Tech Deep State caused Plaintiff's existing commercial customers, suppliers and buyers, and potential customers, suppliers and buyers, to conclude that Plaintiff was too reputationally toxic to engage in business transactions with. Further, Defendants' frivolous character assassination attack using hired media attack services like Black Cube, Gawker Media, Gizmodo Media, Fusion GPS, etc., against Plaintiff caused Plaintiff's current and prospective commercial customers, suppliers and buyers, and potential customers, suppliers and buyers to fear Plaintiff would be unable to continue in its ordinary course of business. Further, Defendants' false publicity campaign caused media companies to terminate Defendants' access to their broadcast and publishing services.

The commercial relationships that Plaintiff lost as a result of Defendants' wrongful acts taken without legal justification were in many cases longstanding relationships that Plaintiff had every reasonable expectation would continue to Plaintiff's economic advantage, absent the acts of Defendants.

The Tech Deep State knew of Plaintiff's business, its manufacturing, and its sales, and knew or should have known Plaintiff had existing commercial customer, supplier and buyer relationships that Plaintiff expected to continue. Yet The Tech Deep State intentionally engaged in their tortious and wrongful acts that The Tech Deep State knew or should have known would cause the loss of Plaintiff's expected economic advantages through continued commercial supply and sales transactions.

Absent Defendants' wrongful acts, Plaintiffs' longstanding successful commercial customer, supplier and buyer relationships would have continued indefinitely.

Defendants' wrongful acts have injured Plaintiff, including but not limited to Plaintiff's loss of customer, supplier, and public good will, loss of long-standing business relationships, loss of supplier contracts, and loss of access to promotional access in media.

These injuries have caused substantial pecuniary harm to Plaintiff. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein.

Another cause of action includes: ***Abuse of Process!***

Citizens repeats and realleges all allegations set forth above as if they were stated in full and incorporated herein.

The Tech Deep State filed different lawsuits against Plaintiff whistle-blowers trying to assert their rights in the United States District Court for the District of Columbia, asserting meritless claims that sought to impose liability on Plaintiffs, or to stall and delay justice for the citizen whistle-blowers for personal political statements protected by the First Amendment that had been made by Plaintiff Whistle-blowers.

The Tech Deep State had an ulterior purpose in filing their D.C. Action against Plaintiffs. The D.C. Action is merely part of a much larger campaign described above by The Tech Deep State who have intentionally sought to intimidate the American public and deter anyone from publicly discussing and commenting on Defendants' services, products, and administration of the elections and internet media manipulation in any way that was unfavorable to Defendants.

Defendants' ulterior purpose was wrongful and improper.

Defendants' abuse of the litigation process for these ends is particularly egregious in light of Defendants' governmental role of administering presidential and congressional elections. The sunlight of public discussion, scrutiny, and evidence-gathering is necessary to ensure votes are collected and counted fairly, and to hold those entrusted with administering the process accountable to a high standard of accuracy, security, and reliability. Defendants' abuse of the litigation process has caused extensive injury to Plaintiff, including, but not limited to, loss of long-standing business relationships, loss of supplier contracts, loss of access to promotional access in media, and expenditure of attorney fees defending against the D.C. Action.

Generally, the causes of action include: ABUSE OF PROCESS; FTCA VIOLATIONS; ACCOUNT STATED; BREACH OF CONTRACT; CONVERSION; DEFAMATION; FRAUDULENT MISREPRESENTATION; FRAUDULENT CONCEALMENT; INJURIOUS FALSEHOOD, PRODUCT DISPARAGEMENT AND TRADE LIBEL; CIVIL RIGHTS VIOLATIONS AND VIOLATIONS OF THE U.S. CONSTITUTION; MISAPPROPRIATION OF TRADE SECRETS; PRIMA FACIE TORT; QUANTUM MERUIT; TORTIOUS INTERFERENCE INCLUDING a.) Tortious interference with an existing contract, b.) Tortious interference with prospective, c.) Tortious interference with business relations contractual relations; PATENT INFRINGEMENT; PERSONAL INJURY; UNJUST ENRICHMENT; ANTI-TRUST LAW VIOLATIONS; LABOR LAW VIOLATIONS AND OTHER CAUSES and other counts.

The Tech Deep State are liable to Plaintiffs for their injuries they has sustained as a result of Defendants' abuse of process. Resulting from Defendants' conduct, Plaintiff has suffered damages as described herein. A jury trial must be undertaken with equal representation for each side.

An award of damages to the Citizens for Defendants' unlawful conduct as set forth herein, including a reasonable multiple of enterprise value, exceeding $10 Billion would meet expected legal precedents.

The sad part is that Big Tech's control over the free flow information is almost entirely illusory and based wholly on our submission to it. Much in the same manner that consumers become zealously brand-conscious, we have come to accept that Microsoft, Apple, Google, Facebook, Twitter, and YouTube have some innate value that makes them indispensable. We forget that Big Tech's dominance

has come about in just one generation and we can track a direct trajectory between the rise of Big Tech and the radical Left's ascendancy.

To have any chance of reversing this ruinous tide, traditional Americans must awake from their stupor and stop feeding the beast that's devouring them. Thankfully, that's much more easily done than say, defeating the British Empire, a bloody civil war to end slavery, or storming the beaches at Normandy. All it takes is a few afternoons at your desk to break the Big Tech habit and transition to emerging Alt-Tech options. But if we're unwilling to do even that, we'll prove unworthy of our legacy of freedom and prosperity and will get exactly what we deserve.

Here are some suggestions for escaping Big Tech's death-grip. A quick disclaimer: while improved privacy and security is an excellent side effect of these suggestions, nothing on the internet is completely secure or private. My main goal here is to provide alternatives that will starve the Big Tech beast.

Ditch Windows and Mac operating systems in favor of Linux. This may seem the most difficult and disruptive action required of your Big Tech jailbreak but it's far less so than you may think and absolutely essential. By allowing Microsoft and Apple control of your computing ecosystem you allow them to track your activities and collect private information. Once the government has labeled dissent as "domestic terrorism," you can bet that the lefties in Redmond and Cupertino will be there to help monitor your political beliefs.

Linux is a free, stable, secure, open-source operating system not controlled by Big Tech. Its code is constantly monitored by thousands of privacy zealots on the watch for any backdoors or other vulnerabilities that would allow Big Tech or Big Brother to gain access. There are thousands of free, open-source applications that can meet the needs of a vast majority of users and a huge side benefit is there is no financial motivation to constantly make your hardware and software programs obsolete like Windows and especially Macintosh. You can even give new life to old computers that have been rendered worthless by Microsoft and Apple.

On the web browser front, if you're using Google Chrome or Apple Safari, you should know that your online activity is being tracked, recorded, and sold to thousands of data brokers. Most of that data is used for marketing, but the sites you visit are a good indicator of your political leanings and activities and the collection of that data is ripe for abuse.

A good alternative is the Brave browser. It has tracking blocked by default and has a built-in, aggressive ad blocker. You can opt to see ads and, if you do, 70% of the revenue from those ads are paid directly to you. The earnings are very modest, but you could take those nickels, dimes, and quarters and contribute them to your favorite pro-American content creators. Leaving the ad blocker turned on, makes your pages load much faster and tax your computer's memory less.

For the love of God, stop using Google search and Gmail. These two services provide the bulk of Google's ad and tracking revenue, which they then use to censor Google search results to block content their woke and H1B visa workforce find objectionable. Google search is the most powerful gatekeeper

of information ever created and Google unapologetically uses algorithms to promote politicians and ideas they agree with and crush those they oppose.

Good alternatives are DuckDuckGo and ProtonMail. You will find search results of conservative and dissident content on DDG that you'd need to go many pages deep into Google to see -- if at all. The exception is pornography, which Google is saturated with, while DDG does a good job censoring from its images and videos -- starving yet another beast.

ProtonMail is an end-to-end encrypted email service and does not know nor sell your data -- anonymously or otherwise. They offer a free basic plan or a more robust option for $5 per month -- a small price I'm more than willing to pay to prevent Google from making money off my private communications.

If Jeff Zuckerberg's and Jack Dorsey's promotion and protection of leftist politicians and dogma during the 2020 election hasn't convinced you to get off Facebook and Twitter, allow me to remind you that, among many outrages, Zuckerberg spent nearly a half-billion dollars subverting the 2020 election and both Zuckerberg and Dorsey censored stories of the Biden crime family's blatant graft and corruption. Then, after the election, both banned the 45th President of the United States from their platforms for objecting.

More than any other tech service, users seem slavishly devoted to Facebook and Twitter and willing to sacrifice the nation and their freedoms to them. This effect is what empowered Zuckerbeg and Dorsey to offend about half their customers… er, products, without fear of reprisal.

The fact that Big Tech has tried so hard to crush Gab and Parler should tell you that's where you need to be. Both have been smeared with allowing hate speech on their platforms, when in fact both have a very tiny amount of actual hate speech compared to Facebook and Twitter. I would also suggest MeWe as a Facebook alternative for friends and family.

In the interest of brevity, let me also suggest you quit Google's YouTubeTV and Netflix, which produced and aired the child sexplotation movie, Cuties, and paid the Obamas $65m to produce a catalog of leftist propaganda. Use Sling or any of the myriad streaming services.

Your transition need not be done all at once but make a list and begin your migration away from Big Tech. Choose tasks that are most easily accomplished and check it off. You will be surprised at how quick and painless the process is and how good responsible citizenship and freedom feels.

The Particular Exploitations

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.

You probably can't imagine the ***second-by-second dangers*** and harms that modern electronics, like your phone and tablet, 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 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 everyplace 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 safes 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, Axciom, 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 Report, 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..."

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.iottechtrends.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 Inti fada. 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. Na'ively, 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 Shallo. 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 PROM IS 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 theA 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

hroughout 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, hoody and sunglasses method I outlined above is 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 Axciom, the NSA, Political manipulators etc. and hack your bank accounts and credit cards. Never put an unsecured photo of yourself online.

==========

Video Conference Apps Have Many Back-Door Spy Paths Built In To Them

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-typingjust-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 Google

...even if you delete all your emails, and provides that data to political parties, the NSA and marketing companies so they can manipulate you

Todd Haselton@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 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 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-suspicions-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 Compromised By Google-Alphabet**

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."

Silicon Valley Has Created A 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 breeches 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."

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.
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.

"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 "&#xD801;." (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.

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 `|url=` 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 `|url=` 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". 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 revelas 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.*
- *Albrechtlund, 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 .*

Facial Recognition Is Used By Facebook To Abuse The Public

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 Axciom, 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? I don't have anything to hide you say

> 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 peacably 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 searchers 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 pinging 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.