YOUR INTERNET SAFETY: HOW TO SURVIVE AND KEEP YOUR FAMILY, FRIENDS AND YOURSELF SAFE ON THE WEB

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, 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.

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?

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.

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.

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 notice, the following data applies to you:

1. EVERY network is known to contain Intel, Cisco, Juniper Networks, AMD, QualComm and other hardware which has been proven to contain back-door hard-coded access to outside

parties. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

2. Chinese, Russian FSB, Iranian and other state-sponsored hacking services as well as 14 year old domestic boys are able to easily enter your networks, emails and digital files because of this. They can enter your network at any time, with less than 4 mouse clicks, using software available to anyone. This is a proven, inarguable fact based on court records, FISA data, IT evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

3. Your financial office is aware of these facts and has chosen not to replace all of the at-risk equipment, nor sue the manufacturers who sold your organization this at risk equipment. They believe that the hassle and cost of replacement and litigation is more effort than the finance department is willing to undertake. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

4. In addition to the existing tools that were on the internet, in recent years, foreign hackers have released all of the key hacking software that the CIA, DIA and NSA built to hack into any device. These software tools have already been used hundreds of times. Now the entire world has access to these tools which are freely and openly posted across the web. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national

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

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

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

7. The thinking: "Well, nobody would want to hack us", or "We are not important enough to get hacked" is the most erroneous and negligent thinking one could have in the world today. Chinese, Russian and Iranian spy agencies have a global "Facebook for blackmail" and have been sucking up the data of every entity on

Earth for over a decade. If the network was open, they have the data and are always looking for more. The same applies to Google and Facebook who have based their entire business around domestic spying and data re-sale. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

8. You are a "Stepping Stone" doorway to other networks and data for targeted individuals and other entities. Your networks provide routes into other people's networks. The largest political industry today is called "Doxing" and "Character Assassination". Billions of dollars are expended by companies such as IN-Q-Tel - (DNC); Gawker Media - (DNC); Jalopnik - (DNC); Gizmodo Media - (DNC); K2 Intelligence - (DNC); WikiStrat - (DNC); Podesta Group - (DNC); Fusion GPS - (DNC/GOP); Google - (DNC); YouTube - (DNC); Alphabet - (DNC); Facebook - (DNC); Twitter - (DNC); Think Progress - (DNC); Media Matters - (DNC); Black Cube - (DNC); Mossad - (DNC); Correct The Record - (DNC); Sand Line - (DNC/GOP); Blackwater - (DNC/GOP); Stratfor - (DNC/GOP); ShareBlue - (DNC); Wikileaks (DNC/GOP); Cambridge Analytica - (DNC/GOP); Sid Blumenthal- (DNC); David Brock - (DNC); PR Firm Sunshine Sachs (DNC); Covington and Burling - (DNC), Buzzfeed - (DNC) Perkins Coie - (DNC); Wilson Sonsini - (DNC) and hundreds of others to harm others that they perceive as political, personal or competitive threats. Do not under-estimate your unintended role in helping to harm others. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

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

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

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

12. Never post your real photograph online, or on a dating site social media or on any network. There are thousands of groups who scan every photo on the web and cross check those photos in their massive databases to reveal your personal information

via every other location your photo is posted. These "image harvesters" can find out where you, who your friends and enemies are and where your kids are in minutes using comparative image data that they have automated and operating around the clock. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

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

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

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

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

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

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

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

Palantir is a private intelligence data management company mapping relationships between individuals and organizations alike founded by Peter Thiel and CEO Alex Karp and accused rapist Joe Lonsdale. You may remember Palantir from journalist Barrett Brown, Anonymous' hack of HBGary, or [accusations](#) that the company provided the technology that enables NSA's mass surveillance PRISM. Founded with early investment from the CIA and heavily used by the military, Palantir is a subcontracting

company in its own right. The company has even been featured in the Senate's grilling of Facebook, when Washington State Senator Maria Cantwell [asked](#) CEO Mark Zuckerberg, "Do you know who Palantir is?" due to Peter Thiel sitting on Facebook's board.

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

> Bank of America/Palintir/HBGary combined WikiLeaks attack plan. You can find more here: https://t.co/85yECxFmZu [pic.twitter.com/huNtfJp8gl](#)
>
> — WikiLeaks (@wikileaks) [November 29, 2016](#)

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

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

> Palantir Law Enforcement supports existing case management systems, evidence management systems, arrest records, warrant data, subpoenaed data, RMS or other crime-reporting data, Computer Aided Dispatch (CAD) data, federal repositories, gang intelligence, suspicious

activity reports, Automated License Plate Reader (ALPR) data, and unstructured data such as document repositories and emails.

Palantir's software, *Bloomberg* [reports](#),

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

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

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

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

about millions of Americans in event of an emergency like Martial Law.

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

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

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

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

YOU HAVE BEEN WARNED:

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

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

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

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

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

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

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

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

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

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

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

https://youtu.be/lwoyesA-vlM

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

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

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

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

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

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

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

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

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

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

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

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

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

https://www.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. Throughout three administrations, the mainstream Mockingbird media obediently covered up the Inslaw affair, enhanced PROMIS being a master tool of inference extraction able to track and eavesdrop like nothing else. Once enhanced PROMIS was being sold domestically and abroad so as to steal data from individuals, government agencies, banks, and corporations everywhere, intelligence-connected Barry Kumnick~ turned PROMIS into an artificial intelligence (AI) tool called SMART (Special Management Artificial Reasoning Tool) that revolutionized surveillance. The DOJ promised Kumnick $25 million, then forced him into bankruptcy as it had Hamilton. (Unlike Hamilton, Kumnick settled for a high security clearance and work at military contractors Systematics and Northrop.) Five Eyes / Echelon and the FBI's Carnivore / Data Collection System 1000 were promptly armed with SMART, as was closed circuit satellite highdefinition (HD) television. With SMART, Five Eyes /

Echelon intercepts for UKUSA agencies became breathtaking.

The next modification to Hamilton's PROMIS was Brainstorm, a behavioral recognition software, followed by the facial recognition soAware Flexible Research System (FRS); then Semantic Web, which looks not just for link words and embedded code but for what it means that this particular person is following this particular thread. Then came quantum modification. The Department of Defense paid Simulex, Inc. to develop Sentient World Simulation (SWS), a synthetic mirror of the real world with automated continuous calibration with respect to current real-world information. The SEAS (Synthetic Environment for Analysis and Simulations) soAware platform drives SWS to devour as many as five million nodes of breaking news census data, shiAing economic indicators, real world weather patterns, and social media data, then feeds it proprietary military intelligence and fictitious events to gauge their destabilizing impact. Research into how to maintain public cognitive dissonance and learned helplessness (psychologist Martin Seligman) help SEAS deduce human behavior.

YOUR CONSTITUTIONAL RIGHTS!

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?

First, let me start out by giving you the bad news, there is no such thing as perfect online privacy. We'll assume for the purposes of this article that online privacy and anonymity mean roughly the same thing. No matter what anyone tells you, online privacy (and anonymity) just doesn't exist. The fight for online privacy is like warfare. Every time one side gets an advantage, the other side figures out how to get around it. That means your level of online privacy is dependent on how much effort you are willing to continually put into making yourself invisible. Let's face it, if the NSA wants to spy on you and is willing to put more time and money into singling you out than you are willing to spend being anonymous, then you will be spied on.

The good news is that there are things you can do to be less surveillable--and they won't cost you anything. Remember the old story about the two friends in the woods who came across a bear. One says to the other, "We'll never outrun this bear." The other smiles and says, "That's OK. I only have to outrun you." That isn't exactly a perfect analogy, because any trace that you leave behind on the internet could be used against you at some later date. But it's still better to leave less behind than the next guy. Make it too expensive for "Them" to surveil everyone to the level that they would need to get much on you--at least for the time being.

The most anyone can possibly do to avoid online surveillance is

to use a different computer every time he goes on line--one that has never been on the internet before and cannot be traced to him. Then, after a single use, he will dispose of it where it can never be found by anyone. Further, he will wear gloves, a ski mask, and dark glasses and go to some public wifi hot spot with hundreds of people using it in a town far away from where he lives (a different town each time). Then he will avoid sites he has frequented in the past and never log on to any site with a password. And he will leave no finger prints or DNS evidence behind... So, obviously, no one is going to actually do this--unless he is in some really, really deep trouble. But, barring that, no sane person is going to put out this level of effort to be anonymous every time he goes on the internet.

So, what level of effort is reasonable? Well, it depends on what you are trying to accomplish. But let's assume you are not doing anything illegal. You just want to access your email and surf the internet, maybe buy something on Amazon. In other words, you are the average consumer. Well, there's some more bad news. Given a reasonable level of effort, you can't be anonymous on any website where you enter a password. Once you type your password, you have identified yourself. That's the point of a password. So, some level of anonymity can only be achieved when you don't enter a password during the period of time that you're logged on to the internet. I know that's probably not what you were hoping to hear. But unless you are someone like Edward Snowden fleeing from the NSA, or on the FBI's ten-most-wanted list, you'll probably not be willing to expend the amount of effort I spelled out above to get the level of online privacy that it would take to keep yourself really, really anonymous.

Assessing Threats

Given that you are willing to make an effort to achieve a reasonable level of anonymity, how do you go about it? The first thing you need to do is to understand who "They" are and how they are watching you. The first group that is watching you is the companies who are hoping to make a buck off of you or off of information about what you are doing on line. These are companies like your internet service provider, Google, Google Analytics, Microsoft, Facebook, WordPress, Squarespace, their competitors, and every website that uses web development software written by these companies or their competitors. The problem is that their software is used on just about every website these days. So, chances are extremely good that if you visit a website that sponsors advertisements, tracks the number of hits it receives, or allows you to make comments or fill out any kind of a form, you are being identified and tracked online. (By the way, this website, The Cheapskate's Guide to Computers and the Internet, only uses open-source software and does not attempt to identify or track you in any way.) If you are using an internet browser or operating system written by Google, like Chrome or Android, you are also being identified and tracked. If you are using Windows 10, you are being identified and tracked online. That covers just about everyone who accesses the internet.

The next group that is watching you works for a government. These are the NSA and possibly the CIA and FBI and other US government agencies (there are 17 government intelligence agencies in the US) and their foreign equivalents. For the time being, all the US government agencies want is to make sure that you are not a criminal or a terrorist--and to make sure they know where you are at all times, in case you ever decide to commit a

crime or become a terrorist. In the future, who knows? Governments of some countries make it a crime to speak out against them, so you can probably figure out why they may want to watch their citizens. And the British government seems to want to spy on its people ... well apparently it just likes spying on its people. I don't know how else to account for the level of surveillance in Britain.

The next group that is watching you is composed of thieves. These are people who want your passwords, so they can empty out your bank accounts. Or they may want to use your online accounts, so they can hide while they steal from others. They may also want to convince you that they are actually a nigerian prince (https://www.bbb.org/new-york-city/get-consumer-help/articles/the-nigerian-prince-old-scam-new-twist/) who has no other place to keep his money safe except in your trustworthy hands.

The next group that is watching you is the hackers who are not thieves. Mostly, they just want to snoop and to practice snooping so as to improve their ability to snoop. They want to know everything about everyone, especially governments and large corporations. And sometimes they want to get notoriety for revealing that information. Maybe some want to fix the broken systems that we all live under to make the world a better place.

Reasonable questions for you, the average consumer, to ask are, which groups, if any, can you protect yourself from, and how hard should you be trying? In order to be able to answer these questions, let's look at a few things. In the three lists which follow, I've assumed that the governments to which I am referring are Western "democratic" governments. The first list is

a probable ranking of the above groups from most to least difficult to protect yourself from:

	Governments
	Hackers
	Corporations
	Thieves

Next, the ranking from most to least likely to be spying on you probably looks like this:

	Corporations
	Governments
	Thieves
	Hackers

Lastly, the amount of damage from most to least that these groups could do to you while spying on you probably looks like this:

	Thieves
	Governments
	Corporations
	Hackers

Taken together, the three lists above suggest the following. First, you shouldn't be worried about hackers, because they probably aren't spying on you. But even if they are, you can't do anything about it. And you really don't have much to fear from them, even if they are spying on you. Second, you should definitely be trying to protect yourself from thieves, because you have the most to fear from them, there is a reasonable likelihood that they are

trying to spy on you, and they are the easiest group to protect yourself from. Next, Corporations probably aren't going to do you much damage by spying on you, even though they are certainly spying on you, although you have a chance, with vigilance on you part, of protecting yourself from them. So, whether you want to try to protect yourself from corporations is a judgment call that you'll have to make. And, lastly, governments are spying on you. And you have nearly as much reason to fear them as to fear thieves. However, governments are the hardest to protect yourself from. So, though you may be tempted to give up on trying to protect yourself from governments, due to the difficulty of doing so, you should probably be looking for ways to protect yourself from them. By the way, it makes sense that you have nearly as much to fear from governments spying on you as from thieves, since according to Paul Kennedy, who wrote The Rise and Fall of the Great Powers, (https://www.amazon.com/Rise-Fall-Great-Powers/dp/0679720197) governments are nothing more than institutionalized thievery. One more thing to note about government spying is that the numbers of people they are spying on is at least in the millions--if not a very significant portion of everyone on the planet, judging by what we know about the NSA (https://www.eff.org/nsa-spying). Also, see this (https://en.wikipedia.org/wiki/PRISM_(surveillance_program) and this: https://www.youtube.com/watch?v=wB4Gn0u4DSE

Threat-Tailoring Approaches

So, now that we have established that we need to fear thieves, governments, and corporations, in that order, let's talk about what we can do about each. Thieves' main methods of attack are

through social engineering attacks (https://www.incapsula.com/web-application-security/social-engineering-attack.html). Social engineering works mainly through phone calls, offers on web sites, and email. A thief may call you on the phone or send you an email to try to scam you by saying they are someone else who has a legitimate need for your information. For example, they may pretend to be the IRS and ask for your tax information, including your banking information and social security number. A thief may have a website with a message that pops up saying that your computer is infected with a virus and telling you to call a phone number. This is never legitimate. To avoid being scammed through email, many people advise you not to open emails from people you don't know. That's like never answering your phone unless you recognize the person calling. You may miss legitimate calls. But it is safer than talking to every caller. Avoid clicking on links in emails or opening attachments, because they may execute malware programs or take you to fake websites. Also 2-factor authentication is another layer of protection against thieves. By the way, you cannot protect yourself from thieves who steal your information out of companies' computers; however, the one exception is that you can encrypt your data before giving it to online services like Dropbox or sending it in emails. Often thieves will hide malware in software that looks legitimate. Don't load software onto your phone or computer from any sources that you don't trust, which is just about every source on the internet except for official Microsoft and Google websites and Linux distribution repositories. With any other software, including web browser add-ons, you are risking your privacy and security. If you have to load software from another source, some of the less risky sources can be found here (https://www.makeuseof.com/tag/9-cleanest-safest-websites-

download-free-software-windows/). One way of telling if you may have malware on your computer that is transmitting information to a thief is to see what ports you have open. You can do this using the Shieldsup test (https://www.grc.com/x/ne.dll?rh1dkyd2). You should not see any ports open while you are online. If you want even more online security, my personal recommendations are to not bank online and to consider using my three-USB stick method. Also, since threats, threat prevention software, and threat prevention techniques change continuously, it is important to keep yourself aware of the latest information.

Protecting yourself from corporate spying requires even more effort. It also requires even more knowledge. No gadget out there will do the work for you. Every time I've seen someone offer consumers a gadget, I've seen someone else explain why it's not very effective--at least, not so far. That leaves software. First, your Internet Service Provider (ISP) can see everything you do online. You probably can't do anything to completely change that; however, you can make it a little harder for them. First, use another DNS server, not your ISP's. This will make it slightly harder for them to see which websites you visit. It is also possible to encrypt your DNS traffic (https://www.opendns.com/about/innovations/dnscrypt/). This prevents your ISP from from seeing which websites you're visiting by examining the DNS headers in individual packets coming across its servers. Then, take full advantage of the built-in encryption on the internet by only using HTTPS websites, where possible. Many people suggest using a VPN service. However, studies have shown that most VPN services don't actually work when it comes to hiding your activities from your ISP. Note that HTTPS and VPN's can no longer protect you from

government surveillance.
https://cheapskatesguide.org/articles/no-online-bank-account.html

To protect yourself from being tracked online by corporations other than your ISP, like Google and Facebook, many people recommend that you use anti-tracking software--like, for example, Privacy Badger. The bad news is that anti-tracking software, including anti-tracking settings in your browser and deletion of tracking cookies are far from 100% effective. There is a technique called fingerprinting that takes all the information that your browser puts out to websites and uses it to uniquely identify you, no matter what anonymizing or anti-tracking measures you have taken. It is extremely difficult to circumvent fingerprinting, because all browsers transmit information to websites. I have never tried using an ancient web browser like Lynx to see if it may transmit significantly less data than the average modern web browser, but it's worth a shot. However, since a lot of corporate tracking techniques rely on your own web browser to do their work for them, one thing you can do to thwart them to some extent is to turn off javascript in your browser. https://helpeverybody.wpengine.com/websocial-media/1409-you-have-no-idea-how-many-visitors-your-website-gets

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.

Some people recommend using ProtonMail to send private emails (and then, only to other ProtonMail users). In order for this to work, ProtonMail would have to provide both the sender and the receiver with software that runs on their computers to encrypt and decrypt the contents of their emails before they are sent over the government-monitored internet lines. Or you could encrypt the contents yourself with a prearranged password (from that face-to-face meeting you had). Be sure to use an extremely secure password! The real benefit of ProtonMail is not its encryption (because it's more secure to do that yourself), but the fact that the emails are stored in Switzerland, where the US government can't get them. But, if the government has a backdoor into either the encryption software that you used or that ProtonMail used to encrypt your email, then encryption does you no good if the US government ever manages to get their hands on your emails. (See this, this, and this.) All we know is that Snowden provided evidence in 2014 that the NSA had not cracked Truecrypt. Whether that is still the case today is unknown.

Be aware that simply the use of methods of avoiding government spying techniques may make you a target. This includes the use of encryption and TAILS. However, if millions and millions of law-abiding people begin to actively use these methods, then the NSA cannot put them under significantly more scrutiny than that to which it is already subjecting the rest of the world. This alone is an argument for their use.

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.
thumbnail for post ID 9772825Two guardsmen faint amid sweltering heat during Trooping the Colour rehearsals

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.
Car crash collision accident with scooter, motor bike; Shutterstock ID 1041606415; Purchase Order: -Man has erection for nine days after moped injury

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.
Smiling pug walking in summer parkSunscreen and shade: How to protect your pet from the summer heat

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.

===========================

Who's Watching Your WebEx? Webex has many back-door spy paths built in

KrebsOnSecurity spent a good part of the past week working with **Cisco** to alert more than four dozen companies — many of them household names — about regular corporate **WebEx** conference meetings that lack passwords and are thus open to anyone who wants to listen in.

[Department of Energy's WebEx meetings.](#)

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

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.

CNBC Tech: Sundar Pichai Google IO 2019

Google CEO Sundar Pichai
Google

Google and other tech companies have been under fire recently for a variety of issues, including failing to protect [user data](#), [failing to disclose](#) how data is collected and used and [failing to police the content](#) posted to their services.

Companies such as Google have embedded themselves in our lives with useful services including Gmail, Google Maps and Google Search, as well as smart products such as the Google Assistant which can answer our questions on a whim. The benefits of these tools come at the cost of our privacy, however, because while Google says that privacy should not be a "[luxury good](#)," it's still going to great lengths to collect as much detail as possible about its users and making it more difficult than necessary for users to track what's collected about them and delete it.

Here's the latest case in point.

In May, I wrote up something weird I spotted on [Google](#)'s account management page. I noticed that Google uses Gmail to store a list of [everything you've purchased](#), if you used Gmail or your Gmail address in any part of the transaction.

If you have a confirmation for a prescription you picked up at a pharmacy that went into your Gmail account, Google logs it. If you have a receipt from Macy's, Google keeps it. If you bought food for delivery and the receipt went to your Gmail, Google stores that, too.

You get the idea, and you can see your own purchase history by going to [Google's Purchases page](#).

Google says it does this so you can use Google Assistant to track packages or reorder things, even if that's not an option for some purchases that aren't mailed or wouldn't be reordered, like something you bought 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.

CNBC Tech: Google Purchases

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 HACKED OR SOON WILL BE:

In a country of just 7 million people, the [scale of the hack](#) means that just about every working adult has been affected.
"We should all be angry. ... The information is now freely available to anyone. Many, many people in Bulgaria already have this file, and I believe that it's not only in Bulgaria," said Genov, a blogger and political analyst. He knows his data was compromised because, though he's not an IT expert, he managed to find the stolen files online.

[Microsoft says foreign hackers still actively targeting US political targets](#)
[Microsoft says foreign hackers still actively targeting US political targets](#)

The attack is extraordinary, but it is [not unique](#).
Government databases are gold mines for hackers. They contain a huge wealth of information that can be "useful" for years to come, experts say. "You can make (your password) longer and more sophisticated, but the information the government holds are things that are not going to change," said Guy Bunker, an information security expert and the chief technology officer at Clearswift, a cybersecurity company. "Your date of birth is not

going to change, you're not going to move house tomorrow," he said. "A lot of the information that was taken was valid yesterday, is valid today, and will probably be valid for a large number of people in five, 10, 20 years' time."

Hackers' paradise

Data breaches used to be spearheaded by highly skilled hackers. But it increasingly doesn't take a sophisticated and carefully planned operation to break into IT systems. Hacking tools and malware that are available on the dark web make it possible for amateur hackers to cause enormous damage.A [strict data protection law](#) that came into effect last year across the European Union has placed new burdens on anyone who collects and stores personal data. It also introduced hefty fines for anyone who mismanages data, potentially opening the door for the Bulgarian government to fine itself for the breach.
[Slack is resetting thousands of passwords after 2015 hack](#)
[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."

[Chinese spies stole NSA hacking tools, report finds](#)
[Chinese spies stole NSA hacking tools, report finds](#)

If the "old data" hasn't changed, it's still valuable to hackers.

The Bulgaria incident is concerning, said Desislava Krusteva, a Bulgarian privacy and data protection lawyer who advises some of the world's biggest tech companies on how to keep their clients' information safe.

"These kinds of incidents should not happen in a state institution. It seems like it didn't require huge efforts, and it's probably the personal data of almost all Bulgarian citizens," said Krusteva, a partner at Dimitrov, Petrov & Co., a law firm in Sofia. The Bulgarian Commission for Personal Data Protection has said it would launch an investigation into the hack.

A National Revenue Agency spokesman would not comment on whether the data was properly protected.

"As there is undergoing investigation, we couldn't provide more details about reasons behind the hack," Communications

Director Rossen Bachvarov said.

'Very embarrassing for the government'

A 20-year-old cybersecurity worker has been arrested by the Bulgarian police in connection with the hack. The computer and software used in the attack led police to the suspect, according to the Sofia prosecutor's office.

The man has been detained, and the police seized his equipment, including mobile phones, computers and drives, the prosecutor's office said in a statement. If convicted, he could spend as long as eight years in prison.

[US indicts two people in China over hacks](#)
[US indicts two people in China over hacks](#)

"It's still too early to say what exactly happened, but from political perspective, it is, of course, very embarrassing for the government," Krusteva said.

The embarrassment is made worse by the fact that this was not the first time the Bulgarian government was targeted. The country's Commercial Registry was brought down less than a year ago by an attack. "So, at least for a year, the Bulgarian society, politicians, those who are in charge of the country, they knew quite well about the serious cybersecurity problems in the government infrastructures," Genov said, "and they didn't do anything about it."

Hackers posted screenshots of the company's servers on Twitter and later shared the stolen data with Digital Revolution, another

hacking group [who last year breached Quantum, another FSB contractor](#).

This second hacker group shared the stolen files in greater detail on their Twitter account, on Thursday, July 18, and with Russian journalists afterward.

SyTech Digital Revolution

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.