T-MOBILE SECURITY ISSUES

CONGRESSIONAL STUDY FOR GAO AND FTC INVESTIGATORS

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

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

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

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

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

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

The Take-Aways:

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

- Every dating site, comments section and social media site sends your private data, covertly, to government, political campaigns and corporate analysis groups and can also be hacked by anyone.
- Any hacker can hack ANY network with even a single Intel, Cisco, Juniper Networks or AMD motherboard on it and nobody can stop them unless they destroy the motherboard because the back-doors are built into the hardware. Many of the companies you think are providing security are secretly owned by the Chinese government spy agencies or the CIA (***https://boingboing.net/2020/02/11/cia-secretly-owned-worlds-to.html*** ***)***
- Warehouses in Nigeria, Russia, Ukraine, Sao Paolo, China and hundreds of other regions, house tens of thousands of hackers who work around the clock to try to hack you and manipulate your data.
- Every red light camera, Walmart/Target/Big Box camera and every restaurant camera goes off to networks that send your activities to credit companies, collection companies, political parties and government agencies (***'Homeland Security' using location data from apps to track millions of people...***
- Match.com, OKCupid and Plenty of Fish are also DNC voter analysis services that read your texts and keep your profiles forever
- If you don't put fake ages, addresses, phone numbers and disposable email addresses on ANY form you fill out electronically, it will haunt you forever (***https://www.the-sun.com/news/284784/pornstar-data-breach-massive-leak-bank-details/***)
- Every train, plane and cruise line records you constantly and checks the covert pictures they take of you against global databases. Corporations grab your collateral private data that those Princess Cruises and United Airlines companies take and use them to build files on you (***https://www.silive.com/news/2020/01/report-new-app-can-id-strangers-with-a-single-photo.html***)
- The people who say "nobody would be interested in me" are the most at risk because their naiveté puts them at the top-of-the-list for targeting and harvesting (***https://www.cnet.com/news/clearview-app-lets-strangers-find-your-name-info-with-snap-of-a-photo-report-says/***)
- Silicon Valley tech companies don't care about your rights, they care about enough cash for their executives to buy hookers and private islands with. Your worst enemy is the social media CEO. They have a hundred thousand programmers trying to figure out more and more extreme ways to use your data every day and nobody to stop them
- The government can see 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 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. 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.

==========

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

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

Department of Energy’s WebEx meetings.

At issue are recurring video- and audio conference-based meetings that companies make available to their employees via WebEx, a set of online conferencing tools run by Cisco. These services allow customers to password-protect meetings, but it was trivial to find dozens of major companies that do not follow this basic best practice and allow virtually anyone to join daily meetings about apparently internal discussions and planning sessions.

Many of the meetings that can be found by a cursory search within an organization’s “Events Center” listing on Webex.com seem to be intended for public viewing, such as product demonstrations and presentations for prospective customers and clients. However, from there it is often easy to discover a host of other, more proprietary WebEx meetings simply by clicking through the daily and weekly meetings listed in each organization’s “Meeting Center” section on the Webex.com site.

Some of the more interesting, non-password-protected recurring meetings I found include those from **Charles Schwab**, **CSC**, **CBS**, **CVS**, **The U.S. Department of Energy**, **Fannie Mae**, **Jones Day**, **Orbitz**, **Paychex Services**, and **Union Pacific**. Some entities even also allowed access to archived event recordings.

Cisco began reaching out to each of these companies about a week ago, and today released an all-customer alert (PDF) pointing customers to a consolidated best-practices document written for Cisco WebEx site administrators and users.

“In the first week of October, we were contacted by a leading security researcher,” Cisco wrote. “He showed us that some WebEx customer sites were publicly displaying meeting information online, including meeting Time, Topic, Host, and Duration. Some sites also included a ‘join meeting’ link.”

==========

Quest Diagnostics Says All 12 Million Patients May Have Had Financial, Medical, Personal Information Breached. It includes credit card numbers and bank account information, according to a filing... HOW MANY TIMES DO YOU NEED TO BE TOLD: "NEVER, EVER, GIVE TRUE INFORMATION TO ANY COMPANY THAT USES A NETWORK OR MAKES YOU SIGN-IN TO ANYTHING ONLINE!"

https://khn.org/news/a-wake-up-call-on-data-collecting-smart-beds-and-sleep-apps/

==========

https://www.wsj.com/articles/hackers-may-soon-be-able-to-tell-what-youre-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.

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.

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

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

tomorrow," he said. "A lot of the information that was taken was valid yesterday, is valid today, and will probably be valid for a large number of people in five, 10, 20 years' time."

Hackers' paradise

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

Slack is resetting thousands of passwords after 2015 hack

Still, attacks against government systems are on the rise, said Adam Levin, the founder of CyberScout, another cybersecurity firm. "It's a war right now -- one we will win if we make cybersecurity a front-burner issue," he said. The notion that governments urgently need to step up their cybersecurity game is not new. Experts have been ringing alarm bells for years.
The US Department of Veterans Affairs suffered one of the first major data breaches in 2006, when personal data of more than 26 million veterans and military personnel were compromised. "And it was all, 'Oh, this is dreadful. We must do things to stop it.' ... And here we are, 13 years later, and an entire country's data has been compromised, and in between, there's been incidents of large swathes of citizen data being compromised in different countries," Bunker said. Out-of-date systems are often the problem. Some governments may have used private companies to manage the data they collected before the array of hacks and 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

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

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

"These kinds of incidents should not happen in a state institution. It seems like it didn't require huge efforts, and it's probably the personal data of almost all Bulgarian citizens," said Krusteva, a partner at Dimitrov, Petrov & Co., a law firm in Sofia.

The Bulgarian Commission for Personal Data Protection has said it would launch an investigation into the hack.

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

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

'Very embarrassing for the government'

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

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

US indicts two people in China over hacks

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

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

Hackers posted screenshots of the company's servers on Twitter and later shared the stolen data with Digital Revolution, another hacking group who last year breached Quantum, another FSB contractor.

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

Alexa and Google Home eavesdrop and phish passwords

Amazon- and Google-approved apps turned both voice-controlled devices into "smart spies."

Dan Goodin -

Enlarge
Aurich Lawson / Amazon

By now, the privacy threats posed by Amazon Alexa and Google Home are common knowledge. Workers for both companies routinely listen to audio of users—recordings of which can be kept forever—and the sounds the devices capture can be used in criminal trials.

Now, there's a new concern: malicious apps developed by third parties and hosted by Amazon or Google. The threat isn't just theoretical. Whitehat hackers at Germany's Security Research Labs developed eight apps—four Alexa "skills" and four Google Home "actions"—that all passed Amazon or Google security-vetting processes. The skills or actions posed as simple apps for checking horoscopes, with the exception of one, which masqueraded as a random-number generator. Behind the scenes, these "smart spies," as the researchers call them, surreptitiously eavesdropped on users and phished for their passwords.

"It was always clear that those voice assistants have privacy implications—with Google and Amazon receiving your speech, and this possibly being triggered on accident sometimes," Fabian Bräunlein, senior security consultant at SRLabs, told me. "We now show that, not only the manufacturers, but... also hackers can abuse those voice assistants to intrude on someone's privacy."

The malicious apps had different names and slightly different ways of working, but they all followed similar flows. A user would say a phrase such as: "Hey Alexa, ask My Lucky Horoscope to give me the horoscope for Taurus" or "OK Google, ask My Lucky Horoscope to give me the horoscope for Taurus." The eavesdropping apps responded with the requested information while the phishing apps gave a fake error message. Then the apps gave the impression they were no longer running when they, in fact, silently waited for the next phase of the attack.

As the following two videos show, the eavesdropping apps gave the expected responses and then went silent. In one case, an app went silent because the task was completed, and, in another instance, an app went silent because the user gave the command "stop," which Alexa uses to terminate apps. But the apps quietly logged all conversations within earshot of the device and sent a copy to a developer-designated server.

The phishing apps follow a slightly different path by responding with an error message that claims the skill or action isn't available in that user's country. They then go silent to give the impression the app is no longer running. After about a minute, the apps use a voice that mimics the ones used by Alexa and Google home to falsely claim a device update is available and prompts the user for a password for it to be installed.

SRLabs eventually took down all four apps demoed. More recently, the researchers developed four German-language apps that worked similarly. All eight of them passed inspection by Amazon and Google. The four newer ones were taken down only after the researchers privately reported their results to Amazon and Google. As with most skills and actions, users didn't need to download anything. Simply saying the proper phrases into a device was enough for the apps to run.

All of the malicious apps used common building blocks to mask their malicious behaviors. The first was exploiting a flaw in both Alexa and Google Home when their text-to-speech engines received instructions to speak the character "&#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 .*

How Artists And Fans Stopped Facial Recognition From Invading Music Festivals

The surveillance dystopia of our nightmares is not inevitable — and the way we kept it out of concerts and festivals is a lesson for the future.

Imagine showing up at a music festival or concert and being required to stand in front of a device that scans and analyzes your face.
Once your facial features are mapped and stored in a database, a computer algorithm could then decide that you are drunk and should be denied entry, or that you look “suspicious” and should be flagged for additional screening. If you make it through security, facial recognition technology could then be used to track the minute details of your movements once inside.

Face scanning software could be used to police behavior — constantly scanning the crowd for drug use or rule-breaking — or for strictly commercial purposes, like showing you targeted ads, monitoring which artists you came to see, or tracking how many times you go to the bar or the bathroom. Festival organizers could be forced to hand this trove of sensitive biometric data over to law enforcement or immigration authorities, and armed officers could pull people out of the crowd because they have an outstanding warrant or a deportation order. If you’re a person of color, or your gender presentation doesn’t conform to the computer’s stereotypes, you’d be more likely to be falsely flagged by the system.

This surveillance nightmare almost became a reality at US music events. Industry giants like Ticketmaster invested money in companies like Blink Identity, a startup run by ex–defense contractors

who helped build the US military's facial recognition system in Afghanistan. These vendors, and the venture capitalists who backed them, saw the live music industry as a huge potential market for biometric surveillance tech, marketed as a convenient ticketing option to concertgoers.

But now, it seems they'll be sorely disappointed — and there's a lesson in the story of how we dashed their dystopian profit dreams. A future where we are constantly subjected to corporate and government surveillance is not inevitable, but it's coming fast unless we act now.

Over the last month, artists and fans waged a grassroots war to stop Orwellian surveillance technology from invading live music events. Today we declare victory. Our campaign pushed more than 40 of the world's largest music festivals — like Coachella, Bonnaroo, and SXSW — to go on the record and state clearly that they have no plans to use facial recognition technology at their events. Facing backlash, Ticketmaster all but threw Blink Identity under the bus, distancing itself from the surveillance startup it boasted about partnering with just a year ago. This victory is the first major blow to the spread of commercial facial recognition in the United States, and its significance cannot be overstated.

In a few short weeks, using basic grassroots activism tactics like online petitions, social media pressure, and an economic boycott targeting festival sponsors, artists and fans killed the idea of facial recognition at US music festivals. Now we need to do the same for sporting events, transportation, public housing, schools, law enforcement agencies, and all public places. And there's no time to lose.

Facial recognition is spreading like an epidemic. It's being deployed by police departments in cities like Detroit, disproportionately targeting low-income people of color. Immigration and Customs Enforcement (ICE) are using it to systematically comb through millions of driver's license photos and target undocumented people for apprehension and deportation. Cameras equipped with facial recognition software are scanning thousands of people's faces right now in shopping malls, casinos, big box stores, and hotels. Schools are using it to police our children's attendance and behavior, with black and Latinx students most likely to end up on watch lists. Major airlines are rapidly adopting it as part of the boarding process. France is about to institute a national facial recognition database. Police and corporate developers in the UK are defending their use of the tech. In China, where authorities have already used facial recognition to arrest people out of crowds at music festivals, the government is making a face scan mandatory to access the Internet.

But in almost all of these cases, facial recognition is still in its early stages. It's an experiment. And we're the test subjects. If we accept ubiquitous biometric monitoring and normalize the idea of getting our faces scanned to get on a plane or pick up our kids from school, the experiment works and our fate is sealed. But if we organize — if we refuse to be lab rats in a digital panopticon — we can avert a future where all human movements and associations are tracked by artificial intelligence algorithms trained to look for and punish deviations from authoritarian norms.

Opposition to facial recognition is spreading almost as quickly as the tech itself. More than 30 organizations, ranging from the Council on American Islamic Relations to Greenpeace, have endorsed Fight for the Future's BanFacialRecognition.com campaign, pushing lawmakers at the local, state, and federal level to halt face surveillance. Four cities have already banned government use of biometric spy

tech. California banned its use in police body cameras. States like Michigan, Massachusetts and New York are considering legislation. Sweden recently banned facial recognition in schools after getting slapped with a fine under the GDPR data privacy regime. Leading 2020 candidates like Bernie Sanders and Beto O'Rourke have echoed grassroots calls for a ban, and there's rare bipartisan agreement in Congress, where lawmakers as diametrically opposed as Alexandria Ocasio-Cortez and Jim Jordan agree that facial recognition poses a unique threat to privacy and civil liberties.

When it comes to automated and insidious invasions of our personal lives and most basic rights, tech lobbyists and politicians sell a calculated brand of cynicism. They want us to believe that the widespread use of deeply creepy technology like facial recognition is a forgone conclusion, that we should get used to it, and that the only questions to address are how, where, and how quickly to roll it out. We can prove them wrong, by channeling our ambient anxiety and online outrage into meaningful action and political power.

Surveillance profiteers who hope to make a lot of money selling facial recognition software to governments and private interests are now on high alert. They're watching closely for public reactions, running tests to see just how much intrusive monitoring we're willing to put up with. They're manipulatively calling for regulation — a trap intended to assuage public fears while hastening adoption. They're promising that facial recognition can be done in an "opt-in," manner, ignoring the inherent dangers in corporate harvesting and storing of biometric data. But we can draw a line in the sand now, and shut down this unethical human experiment by pushing for legislation to ban facial recognition, and refusing to support corporations who use it.

We have a chance to stop the proliferation of surveillance technology that rivals nuclear weapons in the threat that it poses to the future of humanity. The clock is ticking.

THE LATEST DANGERS OF FACE-TRACKING

Face-tracking harvesters grab one picture of you and then use AI to find every other digital picture of you on the web. They open every social media post, resume, news clipping, dating account etc. and sell the full dossier on you to 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 Tools

Prefer the classic site? View a single-page layout.

Providers

Discover privacy-centric online services, including email providers, VPN operators, DNS administrators, and more!

Web Browsers

Find a web browser that respects your privacy, and discover how to harden your browser against tracking and leaks.

Software

Discover a variety of open source software built to protect your privacy and keep your digital data secure.

Operating Systems

Find out how your operating system is compromising your privacy, and what simple alternatives exist.

PrivacyTools Services

The PrivacyTools team is proud to launch a variety of privacy-centric online services, including a Mastodon instance, search engine, and more!

Privacy? I don't have anything to hide.

> Over the last 16 months, as I've debated this issue around the world, every single time somebody has said to me, "I don't really worry about invasions of privacy because I don't have anything to hide." I always say the same thing to them. I get out a pen, I write down my email address. I say, "Here's my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting.

After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." **Not a single person has taken me up on that offer.**

Why privacy matters - TED Talk

The primary reason for window curtains in our house, is to stop people from being able to see in. The reason we don't want them to see in is because we consider much of what we do inside our homes to be private. Whether that be having dinner at the table, watching a movie with your kids, or even engaging in intimate or sexual acts with your partner. None of these things are illegal by any means but even knowing this, we still keep the curtains and blinds on our windows. We clearly have this strong desire for privacy when it comes to our personal life and the public.

The Crypto Paper

[...] But saying that you don't need or want privacy because you have nothing to hide is to assume that no one should have, or could have, to hide anything -- including their immigration status, unemployment history, financial history, and health records. You're assuming that no one, including yourself, might object to revealing to anyone information about their religious beliefs, political affiliations, and sexual activities, as casually as some choose to reveal their movie and music tastes and reading preferences.

Permanent Record

Read also:

- Nothing to hide argument (Wikipedia)
- How do you counter the "I have nothing to hide?" argument? (reddit.com)
- 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy (Daniel J. Solove - San Diego Law Review)

Quotes

Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say. Or that you don't care about freedom of the press because you don't like to read. Or that you don't care about freedom of religion because you don't believe in God. Or that you don't care about the freedom to 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.