WEB SAFETY - Part Two

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 "<break time="1"/>."

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.