WIKIPEDIA

Computer and network surveillance

Computer and network surveillance is the monitoring of computer activity and data stored on a hard drive, or data being transferred over computer networks such as the Internet. The monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent government agencies.

Computer and network surveillance programs are widespread today and almost all Internet traffic can be monitored.[1]

Surveillance allows governments and other agencies to maintain social control, recognize and monitor threats, and prevent and investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high-speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.[2]

However, many civil rights and privacy groups, such as Reporters Without Borders, the Electronic Frontier Foundation, and the American Civil Liberties Union, have expressed concern that with increasing surveillance of citizens we will end up in or are even already in a mass surveillance society, with limited political and/or personal freedoms. Such fear has led to numerous lawsuits such as *Hepting v. AT&T*.[2][3] The hacktivist group Anonymous has hacked into government websites in protest of what it considers "draconian surveillance".[4][5]

Contents

Network surveillance

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet.[6] For example, in the United States, the Communications Assistance For Law Enforcement Act, mandates that all phone calls and broadband internet traffic (emails, web traffic, instant messaging, etc.) be available for unimpeded, real-time monitoring by Federal law enforcement agencies.[7][8][9]

Packet capture (also known as "packet sniffing") is the monitoring of data traffic on a computer network.[10] Data sent between computers over the Internet or between any networks takes the form of small chunks called packets, which are routed to their destination and assembled back into a complete message. A Packet Capture Appliance intercepts these packets, so that they may be examined and analyzed. Computer technology is needed to perform traffic analysis and sift through intercepted data to look for important/useful information. Under the Communications Assistance For Law

Enforcement Act, all U.S. telecommunications providers are required to install such packet capture technology so that Federal law enforcement and intelligence agencies are able to intercept all of their customers' broadband Internet and voice over Internet protocol (VoIP) traffic.[11]

There is far too much data gathered by these packet sniffers for human investigators to manually search through. Thus, automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic, filtering out, and reporting to investigators those bits of information which are "interesting", for example, the use of certain words or phrases, visiting certain types of web sites, or communicating via email or chat with a certain individual or group.[12] Billions of dollars per year are spent by agencies such as the Information Awareness Office, NSA, and the FBI, for the development, purchase, implementation, and operation of systems which intercept and analyze this data, extracting only the information that is useful to law enforcement and intelligence agencies.[13]

Similar systems are now used by Iranian secret police to identify and suppress dissidents. All of the technology has been allegedly installed by German Siemens AG and Finnish Nokia.[14]

The Internet's rapid development has become a primary form of communication. More people are potentially subject to Internet surveillance. There are advantages and disadvantages to network monitoring. For instance, systems described as "Web 2.0"[15] have greatly impacted modern society. Tim O' Reilly, who first explained the concept of "Web 2.0",[15] stated that Web 2.0 provides communication platforms that are "user generated", with self-produced content, motivating more people to communicate with friends online.[16] However, Internet surveillance also has a disadvantage. One researcher from Uppsala University said "Web 2.0 surveillance is directed at large user groups who help to hegemonically produce and reproduce surveillance by providing user-generated (self-produced) content. We can characterize Web 2.0 surveillance as mass self-surveillance".[17] Surveillance companies monitor people while they are focused on work or entertainment. Yet, employers themselves also monitor their employees. They do so in order to protect the company's assets and to control public communications but most importantly, to make sure that their employees are actively working and being productive.[18] This can emotionally affect people; this is because it can cause emotions like jealousy. A research group states "...we set out to test the prediction that feelings of jealousy lead to 'creeping' on a partner through Facebook, and that women are particularly likely to engage in partner monitoring in response to jealousy".[19] The study shows that women can become jealous of other people when they are in an online group.

The virtual assistant has become a social integration into lives. Currently, virtual assistant such as Amazon's Alexa cannot call 911 or local services.[20] They are constantly listening for a command and recording parts of conversations that will help improve algorithms. If the law enforcement are able to be called using a virtual assistant, the law enforcement would then be able to have access to all the information saved for the device.[21] The device is connected to the home's internet, because of this law enforcement would be the exact location of the individual calling for law enforcement.[20] While the virtual assistance devices are popular, many debate the lack of privacy. The devices are listening to every conversation the owner is having. Even if the owner is not talking to a virtual assistant, the device is still listening to the conversation in hopes that the owner will need assistance, as well as to gather data.[22]

Corporate surveillance

Corporate surveillance of computer activity is very common. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. It can be used as a form of business intelligence, which enables the corporation to better tailor their products and/or services to be desirable by their customers. The data can be also sold to other corporations so that they can use it for the aforementioned purpose, or it can be used for direct marketing purposes, such as targeted advertisements, where ads are targeted to the user of the search engine by analyzing their search history and emails[23] (if they use free webmail services), which are kept in a database.[24]

One important component of prevention is establishing the business purposes of monitoring, which may include the following:

- Preventing misuse of resources. Companies can discourage unproductive personal activities such as online shopping or web surfing on company time. Monitoring employee performance is one way to reduce unnecessary network traffic and reduce the consumption of network bandwidth.
- Promoting adherence to policies. Online surveillance is one means of verifying employee observance of company networking policies.
- Preventing lawsuits. Firms can be held liable for discrimination or employee harassment in the workplace. Organizations can also be involved in infringement suits through employees that distribute copyrighted material over corporate networks.
- Safeguarding records. Federal legislation requires organizations to protect personal information. Monitoring can determine the extent of compliance with company policies and programs overseeing information security. Monitoring may also deter unlawful appropriation of personal information, and potential spam or viruses.
- Safeguarding company assets. The protection of intellectual property, trade secrets, and business strategies is a major concern. The ease of information transmission and storage makes it imperative to monitor employee actions as part of a broader policy.

A second component of prevention is determining the ownership of technology resources. The ownership of the firm's networks, servers, computers, files, and e-mail should be explicitly stated. There should be a distinction between an employee's personal electronic devices, which should be limited and proscribed, and those owned by the firm.

For instance, Google search stores identifying information for each web search. An IP address and the search phrase used are stored in a database for up to 18 months.[25] Google also scans the content of emails of users of its Gmail webmail service in order to create targeted advertising based on what people are talking about in their personal email correspondences.[26] Google is, by far, the largest Internet advertising agency—millions of sites place Google's advertising banners and links on their websites in order to earn money from visitors who click on the ads. Each page containing Google advertisements adds, reads, and modifies "cookies" on each visitor's computer.[27] These cookies track the user across all of these sites and gather information about their web surfing habits, keeping track of which sites they visit, and what they do when they are on these sites. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use to build a profile of the user to deliver better-targeted advertising.[26]

The United States government often gains access to these databases, either by producing a warrant for it, or by simply asking. The Department of Homeland Security has openly stated that it uses data collected from consumer credit and direct marketing agencies for augmenting the profiles of individuals that it is monitoring.[24]

Malicious software

In addition to monitoring information sent over a computer network, there is also a way to examine data stored on a computer's hard drive, and to monitor the activities of a person using the computer. A surveillance program installed on a computer can search the contents of the hard drive for suspicious data, can monitor computer use, collect passwords, and/or report back activities in real-time to its operator through the Internet connection.[28] Keylogger is an example of this type of program. Normal keylogging programs store their data on the local hard drive, but some are programmed to automatically transmit data over the network to a remote computer or Web server.

There are multiple ways of installing such software. The most common is remote installation, using a backdoor created by a computer virus or trojan. This tactic has the advantage of potentially subjecting multiple computers to surveillance. Viruses often spread to thousands or millions of computers, and leave "backdoors" which are accessible over a network connection, and enable an intruder to remotely install software and execute commands. These viruses and trojans are sometimes developed by government agencies, such as CIPAV and Magic Lantern. More often, however, viruses created by other people or spyware installed by marketing agencies can be used to gain access through the security breaches that they create.[29]

Another method is "cracking" into the computer to gain access over a network. An attacker can then install surveillance software remotely. Servers and computers with permanent broadband connections are most vulnerable to this type of attack.[30] Another source of security cracking is employees giving out information or users using brute force tactics to guess their password.[31]

One can also physically place surveillance software on a computer by gaining entry to the place where the computer is stored and install it from a compact disc, floppy disk, or thumbdrive. This method shares a disadvantage with hardware devices in that it requires physical access to the computer.[32] One well-known worm that uses this method of spreading itself is Stuxnet.[33]

Social network analysis

One common form of surveillance is to create maps of social networks based on data from social networking sites as well as from traffic analysis information from phone call records such as those in the NSA call database,[34] and internet traffic data gathered under CALEA. These social network "maps" are then data mined to extract useful information such as personal interests, friendships and affiliations, wants, beliefs, thoughts, and activities.[35][36][37]

Many U.S. government agencies such as the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), and the Department of Homeland Security (DHS) are currently investing heavily in research involving social network analysis.[38][39] The intelligence community believes that the biggest threat to the U.S. comes from decentralized, leaderless, geographically dispersed groups. These types of threats are most easily countered by finding important nodes in the network, and removing them. To do this requires a detailed map of the network.[37][40]

Jason Ethier of Northeastern University, in his study of modern social network analysis, said the following of the Scalable Social Network Analysis Program developed by the Information Awareness Office:

> *The purpose of the SSNA algorithms program is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people ... In order to be successful SSNA will require information on the social interactions of the majority of people around the globe. Since the Defense Department cannot easily distinguish between peaceful citizens and terrorists, it will be necessary for them to gather data on innocent civilians as well as on potential terrorists.*
>
> — Jason Ethier[37]

Monitoring from a distance

It has been shown that it is possible to monitor computers from a distance, with only commercially available equipment, by detecting the radiation emitted by the CRT monitor. This form of computer surveillance, known as TEMPEST, involves reading electromagnetic emanations from computing devices in order to extract data from them at distances of hundreds of meters.[41][42][43]

IBM researchers have also found that, for most computer keyboards, each key emits a slightly different noise when pressed. The differences are individually identifiable under some conditions, and so it's possible to log key strokes without actually requiring logging software to run on the associated computer.[44][45]

In 2015, lawmakers in California passed a law prohibiting any investigative personnel in the state to force businesses to hand over digital communication without a warrant, calling this Electronic Communications Privacy Act.[46] At the same time in California, state senator Jerry Hill introduced a bill making law enforcement agencies to disclose more information on their usage and information from the Stingray phone tracker device.[46] As the law took into effect in January 2016, it will now require cities to operate with new guidelines in relation to how and when law enforcement

use this device.[46] Some legislators and those holding a public office have disagreed with this technology because of the warrantless tracking, but now if a city wants to use this device, it must be heard by a public hearing.[46] Some cities have pulled out of using the StingRay such as Santa Clara County.

And it has also been shown, by Adi Shamir et al., that even the high frequency noise emitted by a CPU includes information about the instructions being executed.[47]

Policeware and govware

Policeware is software designed to police citizens by monitoring discussion and interaction of its citizens.[48] Within the U.S., Carnivore was a first incarnation of secretly installed e-mail monitoring software installed in Internet service providers' networks to log computer communication, including transmitted e-mails.[49] Magic Lantern is another such application, this time running in a targeted computer in a trojan style and performing keystroke logging. CIPAV, deployed by FBI, is a multi-purpose spyware/trojan.

The Clipper Chip, formerly known as MYK-78, is a small hardware chip that the government can install into phones, designed in the nineties. It is intended to secure private communication and data by reading voice messages that are encoded and decode them. The Clipper Chip was designed during the Clinton administration to, "...protect personal safety and national security against a developing information anarchy that fosters criminals, terrorists and foreign foes."[50] The government portrays it as solving the secret codes or cryptographic that the age of technology has created. Thus, this has raised controversy in the public, because the Clipper Chip is thought to have been the next "Big Brother" tool. This has led to the failure of the Clipper proposal, even though there have been many attempts.[51]

The "Consumer Broadband and Digital Television Promotion Act" (CBDTPA) was a bill proposed in the United States Congress. CBDTPA was known as the "Security Systems and Standards Certification Act" (SSSCA) while in draft form, and was killed in committee in 2002. Had CBDTPA become law, it would have prohibited technology that could be used to read digital content under copyright (such as music, video, and e-books) without Digital Rights Management (DRM) that prevented access to this material without the permission of the copyright holder.[52]

In German-speaking countries, spyware used or made by the government is sometimes called *govware*.[53] Some countries like Switzerland and Germany have a legal framework governing the use of such software.[54][55] Known examples include the Swiss MiniPanzer and MegaPanzer and the German R2D2 (trojan).

Surveillance as an aid to censorship

Surveillance and censorship are different. Surveillance can be performed without censorship, but it is harder to engage in censorship without some form of surveillance.[56] And even when surveillance does not lead directly to censorship, the widespread knowledge or belief that a person, their computer, or their use of the Internet is under surveillance can lead to self-censorship.[57]

In March 2013 Reporters Without Borders issued a *Special report on Internet surveillance* that examines the use of technology that monitors online activity and intercepts electronic communication in order to arrest journalists, citizen-journalists, and dissidents. The report includes a list of "State Enemies of the Internet", Bahrain, China, Iran, Syria, and Vietnam, countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. Computer and network surveillance is on the increase in these countries. The report also includes a second list of "Corporate Enemies of the Internet", Amesys (France), Blue Coat Systems (U.S.), Gamma (UK and Germany), Hacking Team (Italy), and Trovicor (Germany), companies that sell products that are liable to be used by governments to violate human rights and freedom of information. Neither list is exhaustive and they are likely to be expanded in the future.[58]

Protection of sources is no longer just a matter of journalistic ethics. Journalists should equip themselves with a "digital survival kit" if they are exchanging sensitive information online, storing it on a computer hard-drive or mobile phone.[58][59] Individuals associated with high-profile rights organizations, dissident groups, protest groups, or reform groups are urged to take extra precautions to protect their online identities.[60]

See also

- Anonymizer, a software system that attempts to make network activity untraceable
- Computer surveillance in the workplace
- Cyber spying
- Differential privacy, a method to maximize the accuracy of queries from statistical databases while minimizing the chances of violating the privacy of individuals.
- ECHELON, a signals intelligence (SIGINT) collection and analysis network operated on behalf of Australia, Canada, New Zealand, the United Kingdom, and the United States, also known as AUSCANNZUKUS and Five Eyes
- GhostNet, a large-scale cyber spying operation discovered in March 2009
- List of government surveillance projects
- Mass surveillance
  - China's Golden Shield Project
  - Mass surveillance in Australia
  - Mass surveillance in China
  - Mass surveillance in East Germany
  - Mass surveillance in India
  - Mass surveillance in North Korea
  - Mass surveillance in the United Kingdom
  - Mass surveillance in the United States
- Surveillance
  - Surveillance by the United States government:
    - 2013 mass surveillance disclosures, reports about NSA and its international partners' mass surveillance of foreign nationals and U.S. citizens
    - Bullrun (code name), a highly classified NSA program to preserve its ability to eavesdrop on encrypted communications by influencing and weakening encryption standards, by obtaining master encryption keys, and by gaining access to data before or after it is encrypted either by agreement, by force of law, or by computer network exploitation (hacking)
    - Carnivore, a U.S. Federal Bureau of Investigation system to monitor email and electronic communications
    - COINTELPRO, a series of covert, and at times illegal, projects conducted by the FBI aimed at U.S. domestic political organizations
    - Communications Assistance For Law Enforcement Act
    - Computer and Internet Protocol Address Verifier (CIPAV), a data gathering tool used by the U.S. Federal Bureau of Investigation (FBI)
    - Dropmire, a secret surveillance program by the NSA aimed at surveillance of foreign embassies and diplomatic staff, including those of NATO allies
    - Magic Lantern, keystroke logging software developed by the U.S. Federal Bureau of Investigation
    - Mass surveillance in the United States
    - NSA call database, a database containing metadata for hundreds of billions of telephone calls made in the U.S.
    - NSA warrantless surveillance (2001–07)
    - NSA whistleblowers: William Binney, Thomas Andrews Drake, Mark Klein, Edward Snowden, Thomas Tamm, Russ Tice
    - Spying on United Nations leaders by United States diplomats
    - Stellar Wind (code name), code name for information collected under the President's Surveillance Program
    - Tailored Access Operations, NSA's hacking program
    - Terrorist Surveillance Program, an NSA electronic surveillance program
    - Total Information Awareness, a project of the Defense Advanced Research Projects Agency (DARPA)

- TEMPEST, codename for studies of unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment

References

1. Anne Broache. "FBI wants widespread monitoring of 'illegal' Internet activity" (http://www.cnet.com/news/fbi-wants-widespread-monitoring-of-illegal-internet-activity/). *CNET*. Retrieved 25 March 2014.
2. "Is the U.S. Turning Into a Surveillance Society?" (https://www.aclu.org/privacy/gen/index.html). *American Civil Liberties Union*. Retrieved March 13, 2009.
3. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society" (https://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf) (PDF). *American Civil Liberties Union*. January 15, 2003. Retrieved March 13, 2009.
4. "Anonymous hacks UK government sites over 'draconian surveillance' " (http://www.zdnet.com/blog/security/anonymous-hacks-uk-government-sites-over-draconian-surveillance/11412), Emil Protalinski, ZDNet, 7 April 2012, retrieved 12 March 2013
5. Hacktivists in the frontline battle for the internet (https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet) retrieved 17 June 2012
6. Diffie, Whitfield; Susan Landau (August 2008). "Internet Eavesdropping: A Brave New World of Wiretapping" (http://www.sciam.com/article.cfm?id=internet-eavesdropping). *Scientific American*. Retrieved 2009-03-13.
7. "CALEA Archive -- Electronic Frontier Foundation" (http://w2.eff.org/Privacy/Surveillance/CALEA/?f=archive.html). *Electronic Frontier Foundation (website)*. Retrieved 2009-03-14.
8. "CALEA: The Perils of Wiretapping the Internet" (https://www.eff.org/issues/calea). *Electronic Frontier Foundation (website)*. Retrieved 2009-03-14.
9. "CALEA: Frequently Asked Questions" (https://www.eff.org/pages/calea-faq). *Electronic Frontier Foundation (website)*. Retrieved 2009-03-14.
10. Kevin J. Connolly (2003). *Law of Internet Security and Privacy*. Aspen Publishers. p. 131. ISBN 978-0-7355-4273-0.
11. American Council on Education vs. FCC (http://www.baller.com/pdfs/ACE.pdf) Archived (https://web.archive.org/web/20120907032500/http://www.baller.com/pdfs/ACE.pdf) 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.
12. Hill, Michael (October 11, 2004). "Government funds chat room surveillance research" (https://www.usatoday.com/tech/news/surveillance/2004-10-11-chatroom-surv_x.htm). USA Today. Associated Press. Retrieved 2009-03-19.
13. McCullagh, Declan (January 30, 2007). "FBI turns to broad new wiretap method" (http://www.zdnet.com/news/fbi-turns-to-broad-new-wiretap-method/151059). *ZDNet News*. Retrieved 2009-03-13.
14. "First round in Internet war goes to Iranian intelligence" (http://www.debka.com/article/3509/), Debkafile, 28 June 2009. (subscription required)
15. 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.
16. Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. Sociology Compass, 134-147.
17. Fuchs, C. (2011). Web 2.0, Presumption, and Surveillance. Surveillance & Society, 289-309.
18. Anthony Denise, Celeste Campos-Castillo, Christine Horne (2017). "Toward a Sociology of Privacy". *Annual Review of Sociology*. **43**: 249–269.
19. 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.
20. [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.
21. [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.
22. [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.
23. Story, Louise (November 1, 2007). "F.T.C. to Review Online Ads and Privacy" (https://www.nytimes.com/2007/11/01/technology/01Privacy.html?_r=1). *New York Times*. Retrieved 2009-03-17.

24. Butler, Don (January 31, 2009). "Are we addicted to being watched?" (http://www2.canada.com/ottawacitizen/news/observer/story.html?id=ade6d795-4e7a-4ede-9fc1-f7bf929849c8&p=1). *The Ottawa Citizen*. canada.com. Retrieved 26 May 2013.
25. Soghoian, Chris (September 11, 2008). "Debunking Google's log anonymization propaganda" (http://news.cnet.com/8301-13739_3-10038963-46.html). *CNET News*. Retrieved 2009-03-21.
26. Joshi, Priyanki (March 21, 2009). "Every move you make, Google will be watching you" (http://www.business-standard.com/india/news/every-move-you-make-google-will-be-watching-you/57071/on). *Business Standard*. Retrieved 2009-03-21.
27. "Advertising and Privacy" (http://www.google.com/privacy_ads.html). *Google (company page)*. 2009. Retrieved 2009-03-21.
28. "Spyware Workshop: Monitoring Software on Your OC: Spywae, Adware, and Other Software" (http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf), Staff Report, U.S. Federal Trade Commission, March 2005. Retrieved 7 September 2013.
29. Aycock, John (2006). *Computer Viruses and Malware* (https://www.springer.com/computer/security+and+cryptology/book/978-0-387-30236-2). Springer. ISBN 978-0-387-30236-2.
30. "Office workers give away passwords for a cheap pen" (https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/), John Leyden, *The Register*, 8 April 2003. Retrieved 7 September 2013.
31. "Passwords are passport to theft" (https://www.theregister.co.uk/2004/03/03/passwords_are_passport_to_theft/), *The Register*, 3 March 2004. Retrieved 7 September 2013.
32. "Social Engineering Fundamentals, Part I: Hacker Tactics" (http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics), Sarah Granger, 18 December 2001.
33. "Stuxnet: How does the Stuxnet worm spread?" (http://antivirus.about.com/od/virusdescriptions/f/How-Does-The-Stuxnet-Worm-Spread.htm). Antivirus.about.com. 2014-03-03. Retrieved 2014-05-17.
34. Keefe, Patrick (March 12, 2006). "Can Network Theory Thwart Terrorists?" (https://www.nytimes.com/2006/03/12/magazine/312wwln_essay.html?_r=0). *New York Times*. Retrieved 14 March 2009.
35. Albrechtslund, Anders (March 3, 2008). "Online Social Networking as Participatory Surveillance" (http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949). *First Monday*. **13** (3). Retrieved March 14, 2009.
36. 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* (http://fuchs.icts.sbg.ac.at/SNS_Surveillance_Fuchs.pdf) (PDF). Salzburg and Vienna: Forschungsgruppe Unified Theory of Information. ISBN 978-3-200-01428-2. Retrieved March 14, 2009.
37. Ethier, Jason (27 May 2006). "Current Research in Social Network Theory" (http://www.atkinson.yorku.ca/~sosc2410/Social%20Network%20Theory2.pdf) (PDF). Northeastern University College of Computer and Information Science. Retrieved 15 March 2009.
38. Marks, Paul (June 9, 2006). "Pentagon sets its sights on social networking websites" (https://www.newscientist.com/article/mg19025556.200?DCMP=NLC-nletter&nsref=mg19025556.200). *New Scientist*. Retrieved 2009-03-16.
39. Kawamoto, Dawn (June 9, 2006). "Is the NSA reading your MySpace profile?" (http://news.cnet.com/8301-10784_3-6082047-7.html). *CNET News*. Retrieved 2009-03-16.
40. Ressler, Steve (July 2006). "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research" (http://www.hsaj.org/?fullarticle=2.2.8). *Homeland Security Affairs*. **II** (2). Retrieved March 14, 2009.
41. McNamara, Joel (4 December 1999). "Complete, Unofficial Tempest Page" (http://www.jammed.com/~jwa/tempest.html). Retrieved 7 September 2013.
42. Van Eck, Wim (1985). "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" (http://jya.com/emr.pdf) (PDF). *Computers & Security*. **4**: 269–286. doi:10.1016/0167-4048(85)90046-X (https://doi.org/10.1016%2F0167-4048%2885%2990046-X).
43. Kuhn, M.G. (26–28 May 2004). "Electromagnetic Eavesdropping Risks of Flat-Panel Displays" (http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf) (PDF). *4th Workshop on Privacy Enhancing Technologies*. Toronto: 23–25.
44. Asonov, Dmitri; Agrawal, Rakesh (2004), *Keyboard Acoustic Emanations* (http://rakesh.agrawal-family.com/papers/ssp04kba.pdf) (PDF), IBM Almaden Research Center
45. Yang, Sarah (14 September 2005), "Researchers recover typed text using audio recording of keystrokes" (http://www.berkeley.edu/news/media/releases/2005/09/14_key.shtml), *UC Berkeley News*

46. "LA Times" (http://www.latimes.com/politics/la-pol-sac-cell-phone-surveillance-transparency-law-20170827-htmlstory.html). Retrieved November 10, 2017.
47. Adi Shamir & Eran Tromer. "Acoustic cryptanalysis" (http://tau.ac.il/~tromer/acoustic/). Blavatnik School of Computer Science, Tel Aviv University. Retrieved 1 November 2011.
48. Jeremy Reimer (20 July 2007). "The tricky issue of spyware with a badge: meet 'policeware'" (https://arstechnica.com/news.ars/post/20070719-will-security-firms-avoid-detecting-government-spyware.html). Ars Technica.
49. Hopper, D. Ian (4 May 2001). "FBI's Web Monitoring Exposed" (http://abcnews.go.com/Technology/story?id=98591&page=1). ABC News.
50. "New York Times" (https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all&mcubz=1). Retrieved November 10, 2017.
51. [cs.stanford.edu/people/eroberts/cs201/projects/1995-96/clipper-chip/history.html "Stanford University Clipper Chip"] Check |url= value (help). Retrieved November 10, 2017.
52. "Consumer Broadband and Digital Television Promotion Act" (http://w2.eff.org/IP/SSSCA_CBDTPA/20020321_s2048_cbdtpa_bill.pdf), U.S. Senate bill S.2048, 107th Congress, 2nd session, 21 March 2002. Retrieved 8 September 2013.
53. "Swiss coder publicises government spy Trojan" (http://news.techworld.com/security/3200593/swiss-coder-publicises-government-spy-trojan/). News.techworld.com. Retrieved 25 March 2014.
54. Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware) (http://www.zora.uzh.ch/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf), LISS 2013, pp. 419-428
55. "FAQ – Häufig gestellte Fragen" (https://web.archive.org/web/20130506102113/http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/faq_vuepf.faq_3.html). Ejpd.admin.ch. 2011-11-23. Archived from the original (http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/faq_vuepf.faq_3.html) on 2013-05-06. Retrieved 2014-05-17.
56. "Censorship is inseparable from surveillance" (https://www.theguardian.com/technology/2012/mar/02/censorship-inseperable-from-surveillance), Cory Doctorow, *The Guardian*, 2 March 2012
57. "Trends in transition from classical censorship to Internet censorship: selected country overviews" (http://www.ifla.org/files/assets/faife/publications/spotlights/1%20Bitso_Fourie_BothmaTrendsInTransiton.pdf)
58. *The Enemies of the Internet Special Edition : Surveillance* (http://surveillance.rsf.org/en/), Reporters Without Borders, 12 March 2013
59. "When Secrets Aren't Safe With Journalists" (https://www.nytimes.com/2011/10/27/opinion/without-computer-security-sources-secrets-arent-safe-with-journalists.html?_r=1&), Christopher Soghoian, *New York Times*, 26 October 2011
60. *Everyone's Guide to By-passing Internet Censorship* (http://www.nartv.org/mirror/circ_guide.pdf), The Citizen Lab, University of Toronto, September 2007

External links

- "Selected Papers in Anonymity" (http://freehaven.net/anonbib/topic.html), Free Haven Project, accessed 16 September 2011.
- Best and Cheaper of Spy Software (https://www.hackingfy.com/cheaper-whatsapp-spy-software-mspy-review/)