2023

Nothing to Hide, Nothing to Share: A Call to Reform U.S. Surveillance Practices

Ryan M. Hodgett

Jacob Young

Nothing to Hide, Nothing to Share: A Call to Reform U.S. Surveillance Practices

Ryan M. Hodgett
Bradley University
rhodgett@mail.bradley.edu

Jacob A. Young
Bradley University
jayoung@bradley.edu

ABSTRACT

The United States' intelligence services have caused social, economic, and political strife, both domestically and internationally, through their surveillance practices. Mass wiretapping, secretive malware, and data collection has weakened the United States' international reputation and increased divisiveness domestically. Polling suggests that citizens want to protect themselves from mass data collection but feel hopeless when it comes to protecting themselves. Therefore, the information systems discipline must play an instrumental role in reforming the surveillance state and educating the public about privacy and security practices. To address these issues, this research-in-progress paper summarizes the United States' surveillance activity, discusses its impact on society, and offers solutions for practice and pedagogy.

Keywords

Privacy, security, surveillance, data brokers

INTRODUCTION

In June 2013, Edward Snowden blew the whistle by leaking National Security Agency (NSA) documents to journalists. Snowden's revelations showed that the NSA was tapping into almost every major Internet and telecommunications source. The United States government was caught red handed spying on international organizations, businesses, and governments, including many of their strongest allies. Americans felt a sense of disbelief, betrayal, and unease at their own government who they trusted to keep them safe (Gao, 2015). Instead, Americans were misled by their own government into a deal that lacked oversight to subvert criticism. Ultimately, Snowden reignited a debate that should have been settled long ago: should we exchange privacy for security? In this research-in-progress paper, we begin by summarizing U.S. surveillance activity before analyzing the societal impact of such programs. We then outline several possible solutions with respect to practice and pedagogy.

BACKGROUND

In this section, we discuss the domestic and foreign surveillance activity conducted by U.S. intelligence services. We also highlight the role of whistleblowers in exposing illegal, and sometimes unconstitutional, practices.

Domestic Activities

The U.S. government has a history of attempting to implement backdoors into civilian communication, such as through key escrow with the Clipper Chip (Froomkin, 1995). This desire was amplified after the terrorist attacks of September 11, 2001, which led to the passage of the Patriot Act. Bush-era spying operations were disclosed by James Risen (2018) and Siobhan Gorman (2006), detailing a mass warrantless spy operation that collected the data of American citizens. Just two years after Snowden, following the San Bernardino tragedy, the Federal Bureau of Investigation (FBI) requested a court order to force Apple into creating a backdoor into iOS encryption to get into the perpetrator's iPhone (Nielsen, 2018). Privacy advocates argued that siding with the FBI would diminish iPhone security as well as establish a precedent for the government to force any company to weaken the security of their products and services (Rotenberg et al., 2014).

Law enforcement agencies in the U.S. have also continued to utilize dragnet investigation techniques. For example, geofence warrants allow the government to obtain the data of every single device in a geographical area during a certain time period (Amster & Diehl, 2022). Reverse keyword warrants allow law enforcement to gather data on anyone who utilized certain keywords during a specified time period (Edano, 2022). In addition to surveillance, the U.S. government has taken an active role in shaping public discourse and quelling controversial stories. For example, in December 2022, Matt Taibi began unearthing the FBI's content moderation scheme that resulted in Americans being banned or silenced in various forms due to their opinions (Bhole, 2022).

Foreign Activities

U.S. surveillance and cyberactivity is not bulletproof and has been uncovered in the instances of Crypto AG and Stuxnet. Crypto AG was exposed in 1995 as a surrogate for the CIA to spy on any entities who used their encryption systems (Miller, 2020; Shane & Bowman, 1995). The malware program Stuxnet was discovered by a Belarusian cyber security company in Iranian computer systems (Zetter, 2014). Part of Snowden's releases contained documents on the bugging of former German Chancellor Angela Merkel. Cyberweapons, like Pegasus, only continue the escalation, creating vulnerabilities in companies and foreign entities (Mazzetti & Bergman, 2022). If intelligence agencies would operate under the assumption that all activity would eventually be public knowledge, it would help self-regulate their behavior.

Treatment of Whistleblowers

A lack of oversight has led to a culture without effective internal reporting mechanisms and that neglects to punish bad actors. Snowden himself cited the government's retaliation against Thomas Drake's whistleblowing as the primary motivation to go through the media rather than government channels (AJ+, 2015). Even if intelligence whistleblowers raise concerns through internal channels, arbiters often cannot access the classified documents that whistleblowers cite, making it extremely difficult to investigate their claims. As a result, intelligence whistleblowers may not be taken seriously and face severe repercussions in their career.

Compounded by a lack of oversight, intelligence agencies have free reign to punish dissenters. Oversight committees lack expertise and power due to various systematic flaws (Zegart, 2011). Intelligence committees are not attractive to politicians because voters generally see intelligence as foreign policy that does not affect them directly. Thus, intelligence committee work is not seen as effective at keeping politicians in office. Intelligence committees also lack the power of the purse due to a lack of Government Accountability Office (GAO) auditing, a lack of communication and information, and workload issues. Intelligence spending is wrapped into defense spending which sets appropriations dollars per legislator as the highest in government. In addition, because intelligence budgets are classified, legislators cannot stand against spending on the house or senate floor in a convincing fashion.

This environment allows intelligence agencies to circumvent oversight committees and go directly to the appropriations committee for budgeting. All of the above create an unethical culture leading to bad management practices and an inefficient use of resources. Examples include the NSA's Trailblazer project (Whittaker, 2015) and internal CIA reports of poor talent recruiting and retention for top level employees (Dilanian, 2013).

SOCIETAL IMPACT

While such spying might result in a positive short-term effect during international negotiations, the consequences can be devastating. International trust in the American government drastically fell, causing many countries, including Germany, to switch from American companies to foreign competitors. For example, a study of US cloud-based service providers found that the Snowden revelations decreased their revenue from 2013 to 2014 growth rate by 11% (Song & Wilkie, 2017).

Additionally, the U.S. has been increasingly losing the moral argument. Pushback against Chinese spying is viewed as hypocritical. For example, the U.S. criticizes China for spying on Americans with TikTok, yet fails to protect citizens from domestic data brokers. Data brokers provide the government with access to citizen data, push products with personalized ads, and steer people into supporting certain opinions, just like TikTok. Surveillance capitalism has led to mass consumerism, an increase in anxiety and depression, and political polarization (Landwehr et al., 2023). Furthermore, big tech algorithms, such as Facebook's, tend to emphasize extreme positions, thus increasing societal division.

Multiple government sources have repeatedly claimed that mass surveillance has been critical in catching terrorists. However, its effectiveness has been shown to be questionable at best. For example, White House officials have admitted that surveillance programs, such as those enacted under section 215 of the Patriot Act, have not been necessary in identifying or catching suspects (Isikoff, 2013). Additionally, top intelligence officials have been forced to retract exaggerated claims during Senate testimony (*Government Surveillance Programs and Privacy*, 2013; Office of Senator Patrick Leahy, 2013).

SOLUTIONS

Impactful solutions include reforming oversight committees, strengthening whistleblowing channels, passing data privacy legislation, and teaching the public how to protect their data. A simple reform is separating intelligence spending from the senatorial defense budget subcommittee to reduce the workload on the Senate intelligence committee. Additionally, intelligence whistleblowers should have a separate, specialized internal whistleblowing mechanism with anonymous submission. To protect consumer data, the federal government should pass enhanced privacy legislation similar to the European Union's General Data

Protection Regulation. U.S. laws could be modeled after the California Consumer Privacy Act and the Illinois Biometrics Privacy Act.

Technology companies can be vital in spearheading legal reforms with their immense legal teams. For example, Google and Microsoft have rallied against geofence and reverse keyword warrants (Whittaker, 2022). However, given that many U.S. companies have been silenced with National Security Letters (Weinstein 2015), we cannot trust the technology industry to resist government demands. Therefore, citizens must also advocate for change. Encouraging firms to curb their data addiction is equally important. For example, shifting from targeted advertising to contextual advertising would reduce the need for individualized consumer data. Eliminating advertising by adopting a subscription model would allow tech companies to remain profitable while simultaneously reducing data breach risk. Another step to limit data collection is the normalization of anonymity tools such as MySudo, SimpleLogin, virtual private networks (VPN), and the Tor network, among others.

Polls have shown that Americans want to "control who can get their information" (93%), yet only 9% believed that "they have a lot of control over how much information is collected about them" (Gao, 2015). Furthermore, a vast majority of Americans (81% companies, 66% government) think that the risks of mass data collection outweigh the benefits (Auxier et al., 2019). Providing students with basic privacy and security practices such as replacing Google with DuckDuckGo, utilizing secure messaging applications (e.g., Signal or Wire), and adopting password managers would give students the confidence to protect their data.

Offering a privacy and security course to all majors would improve their cyber hygiene and attract students to cybersecurity. Such a course can educate a wide range of majors about cybersecurity topics related to their desired professions. For example, marketing majors could learn about the dangers of surveillance capitalism, criminal justice students could realize how mass surveillance can result in the conviction of innocent citizens, and political science students can learn to protect themselves from the incendiary nature of social media in politics. An increased focus on technology ethics could also help malicious actors from arising, thus increasing cybersecurity on a societal level.

CONCLUSION

The system as it stands has allowed U.S. intelligence services to run amuck. The resulting unethical behavior caused leakers to blow the whistle, exposing dirty laundry. The effects of these leaks, and other exposures, have degraded the US's standing sociologically, economically, and internationally. Solutions need to start with oversight committee reform. Unattractive and overworked intelligence committee positions allow agencies to sidestep checks and balances and maintain the status quo.

Americans want their data kept private, but are intimidated by the scope of the issue. This has created a sense of nihilism that needs to be fixed. Thus, there is a need for more privacy and security training for all citizens, which could be partially addressed with an entry level cybersecurity course for undergraduates. Successful execution could lead to enhanced privacy, security, and ethics practices and more public pressure that challenges the security state and surveillance capitalism. The desire for security and privacy exists and we believe that the IS discipline is primed to address these issues.

REFERENCES

1. AJ+. (2015). *EXCLUSIVE: Edward Snowden Interview About Fellow NSA Whistleblower Thomas Drake*. https://www.youtube.com/watch?v=MKnnnufSYLo
2. Amster, H., & Diehl, B. (2022). Against Geofences. *Stanford Law Review, 74*(February), 385–445.
3. Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
4. Bhole, A. (2022). *Didn't they have anything better to do?! Latest Twitter Files show how FBI inundated social media network with so many requests to tackle obscure accounts posting "misinformation" that staffers had to triage Bureau's emails*. Daily Mail. https://www.dailymail.co.uk/news/article-11572377/Latest-Twitter-Files-FBI-inundated-social-media-site-requests-tackle-obscure-accounts.html
5. Dilanian, K. (2013). *Bad management drives talent from CIA, internal reports suggest*. Los Angeles Times. https://www.latimes.com/nation/la-xpm-2013-jul-29-la-na-cia-management-20130730-story.html
6. Edano, C. C. (2022). Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants. *Washington Law Review*, *97*(4), 977–1008.

7. Froomkin, A. M. (1995). The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. *University of Pennsylvania Law Review*, *143*(3), 709. https://doi.org/10.2307/3312529
8. Gao, G. (2015). *What Americans think about NSA surveillance, national security and privacy*. Pew Research Center. https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/
9. Gorman, S. (2006, May 18). NSA rejected system that sifted phone data legally. *The Baltimore Sun*. https://web.archive.org/web/20070927193047/http://www.baltimoresun.com/news/nationworld/bal-te.nsa18may18,1,5386811.story?ctrack=1&cset=true
10. *Government Surveillance Programs and Privacy*. (2013). C-SPAN. https://www.c-span.org/video/?314284-1/senate-judiciary-reviews-nsa-data-collection-program
11. Isikoff, M. (2013). *NSA program stopped no terror attacks, says White House panel member*. NBC News. https://www.nbcnews.com/news/world/nsa-program-stopped-no-terror-attacks-says-white-house-panel-flna2d11783588
12. Landwehr, M., Borning, A., & Wulf, V. (2023). Problems with surveillance capitalism and possible alternatives for IT infrastructure. *Information, Communication & Society*, *26*(1), 70–85. https://doi.org/10.1080/1369118X.2021.2014548
13. Mazzetti, M., & Bergman, R. (2022). *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*. The New York Times. https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html
14. Miller, G. (2020). *The intelligence coup of the century*. The Washington Post. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
15. Nielsen, R. P. (2018). "Ethical and Legal First Amendment Implications of FBI v. Apple: A Commentary on Etzioni's 'Apple: Good Business, Poor Citizen?'" *Journal of Business Ethics*, *151*(1), 17–28. https://doi.org/10.1007/s10551-017-3437-2
16. Office of Senator Patrick Leahy. (2013). *Leahy Questions NSA Director Keith Alexander On Cyber Security*. Leahy Questions NSA Director Keith Alexander On Cyber Security
17. Risen, J. (2018). *The Biggest Secret: My Life as a New York Times Reporter in the Shadow of the War on Terror*. The Intercept. https://theintercept.com/2018/01/03/my-life-as-a-new-york-times-reporter-in-the-shadow-of-the-war-on-terror/
18. Rotenberg, M., McCall, G., Butler, A., & Husband, D. (2014). *Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) and Twenty-Four Technical Experts and Legal Scholars in Support of Petitioner*. Electronic Privacy Information Center. https://epic.org/wp-content/uploads/amicus/cell-phone/riley/EPIC-Amicus-Brief.pdf
19. Shane, S., & Bowman, T. (1995). *RIGGING THE GAME Spy sting: Few at the Swiss factory knew the mysterious visitors were pulling off a stunning intelligence coup -- perhaps the most audacious in the National Security Agency's long war on foreign codes; NO SUCH AGENCY*. The Baltimore Sun. https://archive.is/ouJEt
20. Song, H., & Wilkie, S. (2017). *The Price of Privacy in the Cloud: The Economic Consequences of Mr. Snowden*. https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf
21. Whittaker, Z. (2015). *Drowned in data, whistleblowers speak of NSA's "largest failure."* ZDNET. https://www.zdnet.com/article/nsa-whistleblowers-security-thinthread-largest-failure-in-nsa-history/
22. Whittaker, Z. (2022). *Google, Microsoft and Yahoo back New York ban on controversial search warrants*. TechCrunch. https://techcrunch.com/2022/05/10/google-new-york-geofence-keyword-warrant/
23. Zegart, A. B. (2011). The domestic politics of irrational intelligence oversight. *Political Science Quarterly*, *126*(1), 1–25. https://www.jstor.org/stable/23056912
24. Zetter, K. (2014). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. WIRED. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/