Resisting the Surveillance State:
How Americans Are Fighting to Stop Mass Data Collection

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Gabriel Silliman

May 10, 2023

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Gabriel Silliman

STS Advisor: Peter Norton

Resisting the Surveillance State: How Americans Are Fighting to Stop Mass Data Collection

Following the attacks of September 11, 2001, US federal intelligence agencies expanded surveillance operations for national security. The government launched programs to ensure it would not happen again, including the expansion of its surveillance power. The Patriot Act and amendments to the Foreign Intelligence Surveillance Act (FISA) authorized federal agencies to conduct blanket surveillance on both Americans and foreigners, including warrantless surveillance of phone and internet records (Sensenbrenner, 2001; Reyes, 2008). These expansions were justified as necessary to defend democracy, while surveillance abuses were concealed (Toomey & Gorski, 2021).

As the surveillance operation grew, it became clear that tech companies were essential to its success. Often compelled by classified court orders, telecommunications companies and internet service providers cooperated. Technology companies also profit massively by selling data to advertisers and data brokers. Over the past 20 years, both government surveillance and commercial data collection have become increasingly flagrant, prompting public outrage. Data privacy advocates resist the continued growth of the surveillance state through whistleblowing, stricter data protection laws, and the use of consumer privacy tools.

Review of Research

Swanlund and Schuurman suggest tactics for resisting geosurveillance by companies and the government (2019). However, their recommendations focus on the "minimization, obfuscation, and manipulation" of personal data, as opposed to systematic change. Additionally, their strategies specifically address location data, which is unique because as metadata, "spatial data often slips through the cracks of legal protection." (Swanland & Schuurman, 2019)

Denick and Cable (2017) argue the Snowden leak normalized data-driven surveillance and dampened privacy advocacy as resistance was seen as hopeless. However, Deibert (2015) argues that it validated and energized data privacy advocates and placed technology companies in “a public relations nightmare,” forcing the private sector to react strongly by providing increased transparency to compensate. Both agree that the leak had a negligible effect on government agencies, who stubbornly doubled down on their surveillance tactics.

IEEE outlines a set of specific recommendations for providing consumers with algorithmic tools that assist with data privacy and protection by automatically submitting do not track or data deletion requests under the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (2019). Their recommended tools would specifically help protect the data of nontechnical consumers under existing data privacy legislation.

Whistleblowers

In the past decade, the public has become more aware of mass data collection by government agencies and private companies due to highly publicized data leaks by whistleblowers. These leaks garner significant short-term media attention, leading to changes in legislation restricting federal law enforcement agencies and governing private companies’ data practices. Though in the long-term, whistleblowers' revelations have led to a sense of resignation to mass digital surveillance due to the normalization of data collection.

The most prominent whistleblower leak was released in 2013 by Edward Snowden, a contractor for the National Security Agency. Snowden leaked documents showing that the NSA collected telephone records from telecommunications companies on millions of Americans (Greenwald, 2013). Documents also showed how the NSA extracted “audio and video chats,

photographs, e-mails, documents, and connection logs" from major US internet companies (Gellman & Poitras, 2013). The program, known as PRISM, collected data indiscriminately on individuals around the world, regardless of reason or suspicion. Widespread media coverage and public outrage over the NSA's actions spurred national awareness and discussion of government surveillance.

Intense scrutiny led Congress to amend the Patriot Act, which authorized the controversial mass surveillance. In 2015, Congress passed the USA Freedom Act, which then-president Barack Obama said would "strengthen civil liberty safeguards and provide greater public confidence…by prohibiting bulk collection" of phone records (2015). Thereafter, telecommunications companies continued to collect and store all phone records, but, "the government can only obtain calling records associated with particular targeted numbers that have been approved." (Franklin, 2019) While the Snowden leak led to greater oversight of the NSA and attempts to restrict surveillance of Americans without a court order, the NSA still engages in extensive domestic surveillance (Kosseff, 2023).

Snowden's revelations also spurred protests around the globe against the NSA's surveillance tactics. In the United States, many protests were organized on social media under the slogan "Restore the Fourth," referring to the Fourth Amendment of the US Constitution which prohibits unreasonable searches and seizures (Kelly, 2013). Following a series of protests, Restore the Fourth was founded as a nonprofit advocacy "opposing unconstitutional mass government surveillance." (Restore the Fourth, 2023) Yet for most Americans, digital surveillance remained a peripheral issue. According to Rainie and Madden (2015), two years after Snowden's leak, 87 percent of Americans had heard of domestic surveillance, but only 22 percent changed device usage in response. Of those who did change their behavior, many merely

used more complex passwords – not enough to thwart the kind of surveillance Snowden disclosed. According to Preibusch (2015): "While media coverage ... was elevated for the 30 weeks" after Snowden's leak, the disclosures "brought few new users to privacy-enhancing technologies." Denick and Cable argue that instead of mass resistance, the Snowden leaks led to a condition they call "surveillance realism," where the lack of control over mass data collection caused widespread resignation (2017).

In 2018, another whistleblower revealed that Cambridge Analytica, a British consulting firm, gained access to up to 87 million Facebook users' data, including names, birthdays, locations, and likes (Schroepfer, 2018). Christopher Wylie, a former employee of Cambridge Analytica, detailed how the firm matched millions of users with other public records to build psychographic voter profiles, which were used by the political campaigns of Ted Cruz and Donald Trump in 2016 to micro-target political advertisements to individuals' views (Rosenberg et al., 2018).

In response, an investigation by the Federal Trade Commission found that "Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences" and was fined $5 billion for the mishandling of users' data (FTC, 2019). Fines, even as large as this one, have little effect on big tech companies like Facebook which can afford to pay them. However, FTC also imposed new regulations on Facebook to prioritize privacy and establish "strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy." (FTC, 2019)

The revelations about Cambridge Analytica's access to Facebook user data also led to widespread public outrage. After the information was made public, the hashtag #DeleteFacebook went viral and was posted more than 400,000 times the following month (Kemp 2018). Many

celebrities and figures in the tech world also joined the call to delete their Facebook accounts. However, results from the social media campaign were mixed. According to a study by the Pew Research Center in 2018, around a quarter of Facebook users polled in the US deleted the app from their phone, and over half changed their Facebook privacy settings in response to the Cambridge Analytica scandal (Perrin). However, this action did not last, as a more recent poll showed that while Facebook use among Americans has plateaued, usage has not decreased (Gramlich, 2021).

While the public response did not last long enough to make a significant difference in Facebook use, it did make many Americans more aware of their privacy on Facebook and other social media platforms. Due to increased scrutiny and new regulations by the FTC, Facebook introduced stronger privacy settings to make it easier to protect their personal information. By exposing this abuse of user data, Wylie forced Facebook to change its approach to privacy (Zuckerberg, 2019) and put Cambridge Analytica into bankruptcy (Lapowsky, 2019). Such consequences may deter similar abuses of user data.

In both cases, Snowden and Wylie's revelations exposed the extent to which the government and private companies collect, store, and use personal data, sparking public and media outrage. Despite public outcry and some legal and policy reforms, data collection and surveillance practices remain largely unchanged. Consumers still interact with technology through which their data is being collected, and the government and private companies still collect vast amounts of personal data. Most people do not have the technical knowledge to obfuscate their data from companies or the government (Rainie & Madden, 2015), and instead resign to accept a lower level of privacy (Denick & Cable, 2017). Even so, whistleblower

disclosures have brought public attention to the risks and potential abuses of data surveillance practices (Lapowsky, 2019).

Current and Proposed Legislation

The data privacy laws in the US applying to companies and government organizations are fragmented and deficient in protecting Americans' rights. Though several states have now passed consumer data protection laws, federal legislation is needed to extend these rights to all Americans. Despite greater public awareness of government surveillance, law enforcement agencies are still largely unrestricted in carrying out mass surveillance and frequently evade the existing laws.

Europe made the largest single change to data protection practices when the EU passed the GDPR in 2016, which requires companies to inform users what data they collect and how it will be used, get consent before collecting data, and access or erase all user data on request (Wolford, 2018). Following this regulation, any company that operated in the EU was required to comply with data protection and privacy standards or else face substantial fines.

California followed Europe's lead and became the first state to implement a data privacy law when the CCPA was passed in 2018. The CCPA gives residents the right to know what data is collected and how it is used, the right to delete their data, and the right to opt out of the sale of their data (CDOJ, 2023).

Four other states—Virginia, Colorado, Utah, and Connecticut—have followed California and passed their own data privacy laws (Millar & Marshall, 2022). While each grants similar rights to residents of their state, each has slight differences. Due to the nature of the internet, the laws apply to state residents' data regardless of where it was collected (Jaglom et al., 2019).

Therefore, many companies—including Microsoft, Netflix, Starbucks, and UPS—guarantee all users the rights granted by the CCPA, as it is easier than verifying the residency of consumers (Fowler, 2020). However, with several more data protection laws either already in effect or coming into effect in 2023, companies will need to pay close attention to the specific rights granted by each one to ensure that they comply with all states' legislation. There are also currently 19 states considering versions of data privacy legislation (Desai, 2023). Although many will fail to pass, each additional state law that passes adds to the patchwork of data rights granted to different Americans.

Currently, there is no comprehensive federal consumer privacy law that grants Americans the right to their data. There have been several dozen bills that have been introduced in Congress in recent years that have attempted to address consumer privacy, business needs, and data protection—but one is yet to pass (Fazlioglu). The most recent bill introduced, American Data Privacy and Protection Act (ADPPA), defines "how companies … handle personal data" and "establishes consumer data protections, including the right to access, correct, and delete personal data." (Palone, 2022) A sweeping federal law granting certain rights to all Americans would allow both consumers and businesses to better understand their rights and obligations regarding personal data. However, legislation on a federal level would require compromise and would likely not go as far as some states, such as California, would like (Zhao, 2022). Even so, any federal legislation granting data rights to all Americans would be a big improvement for Americans, especially in the 45 states that currently are not granted these rights.

Much stricter laws need to be passed to stop the continued mass surveillance of Americans by federal law enforcement agencies. Despite reforms after the Snowden leak, the NSA still gathers extensive data on Americans without warrants through the PRISM program.

This program is enabled by Section 702 of FISA, which was most recently renewed by Congress in 2018 (Kaplan, 2023). While this law only applies to the communications and internet traffic of noncitizens, it also sweeps up Americans' interactions with foreign nationals (Savage, 2023). Access to the collected records is granted to government agencies, including the FBI, CIA, and NSA. According to a report from the Office of the Director of National Intelligence (ODNI), the FBI queried Section 702 data for information on Americans 3.4 million times in 2021 alone (2022). The FBI claims to have policies to "prohibit the use of the data for personal or other improper reasons," (Kosseff, 2023) however, in an audit of the FBI, the ODNI found that over 36% of data queries violated their own targeting or minimization procedures (2021).

In the reauthorization of Section 702, a provision was added to require the FBI "to obtain a probable cause order ... from queries in a small fraction of late-stage criminal investigations that are unrelated to national security." (Kosseff, 2023) However, Goitein shows that in the four years following this rule—despite over 100 situations in which this requirement applied—the FBI did not obtain a single probable cause order (2022). The Foreign Intelligence Surveillance Court (FISC) repeatedly found that the FBI failed to maintain data privacy practices (Boasberg, 2018, 2019, 2020). In his 2020 opinion, Judge Boasberg stated that even despite some reforms, he "continues to be concerned about FBI querying practices involving U.S.-person query terms."

Not only do government agencies continue to collect mass communication records on a large, unknown number of Americans without warrants, but they also frequently abuse the data and disregard the data protection policies in place. Kosseff argues that as Section 702 is set to expire at the end of 2023, Congress has an opportunity to revise the law to restrict the mass collection of and use of Americans' internet communications (2023). There is rare bipartisan support for

reform—something the intelligence community is aware of—allowing privacy advocates to bargain for greater civil liberties protections (Lucas, 2023).

New laws are also necessary to stop private companies from selling user data to the government to circumvent restrictions placed on data law enforcement agencies, especially regarding location data. In 2018, the Supreme Court ruled in *Carpenter v. United States* that accessing cell phone location data without a warrant is a violation of the Fourth Amendment. However, the court previously ruled that "the purchase of information already collected by a third party is constitutionally distinct from asking a court for permission to collect it." (Joh, 2021) So, law enforcement agencies turned to private companies—known as data brokers—to collect user location data for them.

Users frequently give their location data to countless services, including seemingly harmless weather or navigation apps. Many developers then sell access to their users' live location data by installing software development kits (SDK) in their apps, automatically sending the device's location alongside other data, such as IP address and email address, to data brokers—often even if the app is not open (Cyphers, 2022). Data brokers collect device data from a multitude of apps and in turn resell it to other brokers who aggregate from many sources, making it difficult to determine where the data originated (Keegan & Ng, 2021). Gravy Analytics, which does not interact with any apps directly and collects all data from other data brokers, claims to have location data from over 150 million devices (Cyphers, 2022). Access to the location data is sold to countless private companies, making up a $16 billion industry in 2022 (Grand View Research, 2022). Some data brokers, like Venntel—a subsidiary of Gravy Analytics—and Babel Street, sell access to the location data to US government agencies (Cyphers, 2022).

According to public contracts available from the Federal Procurement Data System, Venntel and Babel Street sell hundreds of thousands of dollars of location data per year to government agencies including the Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), FBI, Drug Enforcement Administration (DEA), Secret Service, and others (GSA, 2023). According to an anonymous source who works with Venntel, the location data is device-specific, meaning that it could be associated with an individual if their location were known at a specific time (Cox, 2020). By purchasing location data from data brokers, government agencies can evade restrictions on what data they can collect without warrants and how they can use that data. In 2020, it was reported that CBP used location data purchased from Venntel to identify border crossings and ICE used it to find, arrest, and deport immigrants, all without obtaining a single warrant (Tau & Hackman).

In 2021, Apple and Google banned the SDKs made by data brokers X-Mode and Predicio from their app stores, after it was revealed that they collected user data sold to federal law enforcement agencies (Cyphers). While this is a good first step, Cyphers argues that it does little to limit unwanted data collection unless all data broker SDKs are banned as well. Google and Apple should moderate the apps they provide access to and should not allow data brokers to collect location data without user knowledge or consent. A bill, The Fourth Amendment Is Not for Sale Act, was introduced in the Senate, but was not passed (Wyden, 2020). This law would ban the purchase of data by government agencies that they would normally need a court order to obtain. According to research by the Center for Democracy & Technology, this legal loophole allows federal law enforcement to "evad[e] Fourth Amendment safeguards as recognized by the Supreme Court." (Franklin et al., 2021) Franklin et al. recommend Wyden's law and ending the

legally and ethically dubious location data collection practices by government agencies through private companies.

While there are several disjoint laws currently in effect in the United States regarding data protection, privacy, and collection, there are huge deficiencies from consumer, business, and government standpoints. By passing laws such as the ADPPA (Palone, 2022) and the Fourth Amendment is Not For Sale Act (Wyden, 2021), Americans can take control of their data back from companies and reinstate their fourth amendment rights.

Consumer Privacy Tools

With greater awareness and concern over mass data collection and surveillance, Americans are increasingly turning towards a variety of tools to hide their digital identity and avoid being constantly tracked. However, for non-technical users, this can be challenging. Over half of Americans have not taken steps to make their actions more private because they feel that it would be too difficult (Rainie & Madden, 2015). While educating people on the use of privacy tools is important, it is unrealistic to expect a non-expert to outsmart a multibillion-dollar industry. Instead, by providing people with out-of-the-box privacy tools and built-in tools, individuals with no knowledge or interest in privacy tools can protect their identity online. There exist several common tools that are effective at enhancing a user's privacy. The first of these is a virtual private network (VPN), which creates secure encrypted connections to websites a user visits and masks their IP address (Symanovich, 2022). In 2020, around 25% of Americans used a VPN at least once a month to improve their privacy online (Migliano). One problem with VPNs is that most require a monthly subscription to use, and free VPN options perform poorly and often collect and sell user data to make money, defeating the purpose of masking your

identity (Savickaitė, 2023). Another common tool is Signal, a free end-to-end encrypted messaging and phone app that is impossible to intercept (Hoffman, 2021). For those concerned about government agencies accessing their text messages or logs of their phone calls, Signal is an easy-to-use and helpful tool.

The tool with the most potential to limit the tracking of an individual's data is the browser that they use, along with its privacy features. Not all browsers are created equal, as some make deliberate choices to prioritize the privacy of users. A 2020 study of five major browsers—Chrome, Edge, Firefox, Safari, and Brave—found that Edge performed the worst, consistently sending unique device identifiers to backend servers, allowing websites to track users over time and across websites, and leaking web history (Leith). By contrast, Leith found that Brave outperformed all other browsers substantially, with built-in default privacy settings that block all cross-site trackers, ad blocking, and HTTPS connections for encrypted browsing. The other browsers tested had mixed results, however, since 2020, with an increase in consumer desire for browser privacy, the developers of Edge, Chrome, and Safari have tried to follow Brave's lead and implement similar privacy features (Shankland, 2022; Wilander, 2020; Colby 2020;). Despite adding privacy features, some browsers like Chrome and Edge still default to insecure privacy settings, forcing users to sift through complicated settings to protect their data when browsing.

Unlike other tech companies, Apple has made privacy one of its top priorities in recent years, especially focusing on default, built-in features that don't require technical expertise (Whittaker, 2021). One such new feature is called App Tracking Transparency, which requires "every single company that wants to track users and their data across different apps and websites … to ask permission first." (Gartenberg, 2021) While it was already possible to opt out of

tracking, by prompting users to make an active choice to be tracked, users are much more likely to ask apps not to track them (O'Flaherty, 2021). By adding built-in privacy features to popular consumer products, it becomes easier for nontechnical users to protect their data and digital identity.

Conclusion

While those in power continue to argue that these surveillance programs are necessary for national security, most Americans understand that government agencies have overstepped their bounds, aided by private companies. If Americans are to regain the right to our data and privacy, many different approaches are necessary. Americans have been resisting the expansion of the surveillance state for many years, but in the past few years with the spike in internet use because of the pandemic, it has been at the forefront of national attention. This will continue to be a prominent issue for the foreseeable future, and Americans must remain focused on fighting for improved data privacy rights.

References

Boasberg, J. (2018, Oct. 18). Section 702 Certification Memorandum Opinion and Order. United States Foreign Intelligence Surveillance Court. https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf

Boasberg, J. (2019, Dec. 6). Section 702 Certification Memorandum Opinion and Order. United States Foreign Intelligence Surveillance Court. https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf

Boasberg, J. (2020, Nov. 18). Section 702 Certification Memorandum Opinion and Order. United States Foreign Intelligence Surveillance Court. https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf

Cahn, A. F. (2021, Sep. 9). 20 Years After 9/11, Surveillance Has Become a Way of Life. Wired. www.wired.com/story/20-years-after-911-surveillance-has-become-a-way-of-life/

Cameron, D. (2023, March 8). The FBI Just Admitted It Bought US Location Data. Wired. https://www.wired.com/story/fbi-purchase-location-data-wray-senate/

Carpenter v. United States, 138 S.Ct. 2206 (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

CDOJ (2023, Feb. 15). Department of Justice, State of California. California Consumer Privacy Act (CCPA). Office of the Attorney General. www.oag.ca.gov/privacy/ccpa

Colby, C. (2020, March 4). Microsoft Edge privacy settings to change right away. CNET. www.cnet.com/tech/computing/microsoft-edge-privacy-settings-to-change-right-away/

Cox, J. (2020, Aug. 25). Customs and Border Protection Paid $476,000 to a Location Data Firm in New Deal. Vice. www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs

Cyphers, B. (2021, March 10). App Stores Have Kicked Out Some Location Data Brokers. Good, Now Kick Them All Out. Electronic Frontier Foundation. www.eff.org/deeplinks/2021/03/apple-and-google-kicked-two-location-data-brokers-out-their-app-stores-good-now

Cyphers, B. (2022, June 13). How the Federal Government Buys Our Cell Phone Location Data. Electronic Frontier Foundation. www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data

Deibert, R. (2015). The Geopolitics of Cyberspace after Snowden. *Current History (New York, N.Y.: 1941) 114*, 9–15. https://doi.org/10.1525/curh.2015.114.768.9

Denick, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication 11*, 763–781.

Desai, A. (2023, March 17). US State Privacy Legislation Tracker. International Association of Privacy Professionals. www.iapp.org/resources/article/us-state-privacy-legislation-tracker/

EFF (2017, May 9). Tools from EFF's Tech Team. Electronic Frontier Foundation. www.eff.org/pages/tools

Fazlioglu, M. (2022, Dec.). US Federal Privacy Legislation Tracker. International Association of Privacy Professionals. www.iapp.org/resources/article/us-federal-privacy-legislation-tracker/

Fowler, G. (2020, Feb. 19). Don't sell my data! We finally have a law for that. Washington Post. www.washingtonpost.com/technology/2020/02/06/ccpa-faq/

FTC. (2019, July 24). Federal Trade Commission. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (Press Release). www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Franklin, S. B. (2019, March 28). Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records. Just Security. www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/

Franklin, S. B., Nojeim, G., Thakur, D., & Shenkman, C. (2021, Dec.). Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers. In Center for Democracy & Technology (Report). cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf

Gartenberg, C. (2021, April 27). Why Apple's new privacy feature is such a big deal. The Verge. https://www.theverge.com/2021/4/27/22405474/apple-app-tracking-transparency-ios-14-5-privacy-update-facebook-data

Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Goitein, Elizabeth. (2022, 4 Nov.). Comments to the Privacy and Civil Liberties Oversight Board re: Section 702 of the Foreign Intelligence Surveillance Act. Brennan Center for Justice. www.brennancenter.org/our-work/research-reports/brennan-center-submits-comments-pclobs-oversight-project-section-702

Gramlich, J. (2021, June 1). 10 facts about Americans and Facebook. Pew Research Center. www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

Greenwald, G. (2013, June 6). NSA Collecting Phone Records of Millions of Verizon Customers Daily. The Guardian. www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

GSA (2023). United States General Services Administration. FPDS-NG ezSearch. Federal Procurement Data System. www.fpds.gov/ezsearch/fpdsportal?q=venntel&s=FPDS.GOV&templateName=1.5.2&indexName=awardfull&x=0&y=0

Hoffman, C. (2021, Jan. 12). What Is Signal, and Why Is Everyone Using It? How-to Geek. www.howtogeek.com/708916/what-is-signal-and-why-is-everyone-using-it/

IEEE (2019). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (1st Edition). IEEE.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, *51*(8), 56–59. www.doi.org/10.1109/MC.2018.3191268

Jaglom, Smigel, Stallone, & Syracuse. (2019, March 20). What Businesses Outside California Should Know About the California Consumer Privacy Act. Tannenbaum Helpern Syracuse & Hirschtritt. www.thsh.com/publications/what-businesses-outside-california-should-know-about-the-california-consumer-privacy-act

Joh, Elizabeth E. (2021, July 19). A Gig Surveillance Economy. *SSRN Electronic Journal*. dx.doi.org/10.2139/ssrn.3889795

Kaplan, F. (2023, March 1). Why Biden Wants to Keep the Law That Allows NSA Mass Surveillance, and Republicans Want to Kill It. Slate. www.slate.com/news-and-politics/2023/03/why-biden-wants-to-keep-section-702-nsa-mass-surveillance.html

Keegan, J., & Ng, A. (2021, Sep. 30). There's a Multibillion-Dollar Market for Your Phone's Location Data. The Markup. www.themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data

Kelly, H. (2013, July 4). Report: NSA mined U.S. e-mail data. CNN. www.edition.cnn.com/2013/07/04/tech/web/restore-nsa-protests

Kemp, S. (2018, March 28). Data shows you didn't #DeleteFacebook, so make sure to change these settings. The Next Web. www.thenextweb.com/news/data-shows-didnt-deletefacebook-make-sure-change-settings

Kosseff, J. (2023, Feb. 9). If Congress Wants to Protect Section 702, It Needs to Rein in the FBI. Lawfare. www.lawfareblog.com/if-congress-wants-protect-section-702-it-needs-rein-fbi

Lapowsky, I. (2019, March 17). How Cambridge Analytica Sparked the Great Privacy Awakening. Wired. www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

Leith, D. J. (2021). Web browser privacy: What do browsers say when they phone home? *IEEE Access, 9*, 41615–41627. doi.org/10.1109/ACCESS.2021.3065243

Lucas, R. (2023, March 23). In fight over key surveillance law, officials look to sway congressional skeptics. NPR. www.npr.org/2023/03/23/1164724089/in-fight-over-key-surveillance-law-officials-look-to-sway-congressional-skeptics

Meta (2023, Feb. 1). Meta Reports Fourth Quarter and Full Year 2022 Results (Press Release). investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx

Migliano, S. (2020, March 17). Global VPN Usage Statistics in 2020. Top10VPN. www.top10vpn.com/research/global-vpn-usage-statistics/

Millar, S., & Marshall, T. (2022, May 24). The State of U.S. State Privacy Laws: A Comparison. Keller & Heckman. www.khlaw.com/insights/state-us-state-privacy-laws-comparison?language_content_entity=en

Obama, B. (2015, June 2). Statement by the President on the USA FREEDOM Act. www.obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act

ODNI. (2021, Sep.). Office of the Director of National Intelligence. 23rd Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence (Audit). www.intel.gov/assets/documents/702%20Documents/declassified/23rd_Joint_Assessment_of_FISA_for_Public_Release.pdf

ODNI. (2022, April). Office of the Director of National Intelligence. Annual Statistical Transparency Report: Regarding the Intelligence Community's Use of National Security Surveillance Authorities (Report). www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf

O'Flaherty, K. (2021, April 7). iOS 14.5: How To Use Apple's Stunning New iPhone Privacy Feature. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2021/04/07/ios-145-how-to-use-apples-stunning-new-iphone-privacy-feature/

Pallone, F. (2022, June 21). H.R.8152 — 117th Congress (2021-2022): American Data Privacy and Protection Act (Legislation). www.congress.gov/bill/117th-congress/house-bill/8152

Perrin, A. (2018, Sep. 5). Americans are changing their relationship with Facebook. Pew Research Center; Pew Research Center. www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Preibusch, S. (2015). Privacy behaviors after Snowden. Communications of the ACM, 58(5), 48–55. www.doi.org/10.1145/2663341

Rainie, L., & Madden, M. (2015, March 16). Americans' Privacy Strategies Post-Snowden. Pew Research Center. www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/

Restore the Fourth (2023). Restore the Fourth. www.restorethe4th.com/

Reyes, Silvestre. (2008, July 10). H.R.6304 - 110th Congress (2007-2008): FISA Amendments Act of 2008 (Legislation). https://www.congress.gov/bill/110th-congress/house-bill/6304

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Savage, C. (2023, Feb. 27). Security Agencies and Congress Brace for Fight Over Expiring Surveillance Law. The New York Times. www.nytimes.com/article/warrantless-surveillance-section-702.html

Savickaitė, M. (2023, March 22). Are free VPNs safe? All you need to know before getting one. Surfshark. surfshark.com/blog/are-free-vpns-safe

Schroepfer, M. (2018, April 4). An Update on Our Plans to Restrict Data Access on Facebook. Facebook. www.about.fb.com/news/2018/04/restricting-data-access/

Sensenbrenner, F. J. (2001, Oct. 26). H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Legislation). https://www.congress.gov/bill/107th-congress/house-bill/3162

Shankland, S. (2022, Jan. 26). Chrome tries new ad-targeting technology after privacy backlash. CNET. www.cnet.com/tech/mobile/chrome-tries-new-ad-targeting-technology-after-privacy-backlash/

Swanlund, D., & Schuurman, N. (2019). Resisting geosurveillance: A survey of tactics and strategies for spatial privacy. *Progress in Human Geography*, *43*(4), 596–610. www.doi.org/10.1177/0309132518772661

Symanovich, S. (2022, Feb. 24). What is a VPN? Norton. us.norton.com/blog/privacy/what-is-a-vpn

Tau, B., & Hackman, M. (2020, Feb. 7). Federal Agencies Use Cellphone Location Data for Immigration Enforcement. Wall Street Journal. www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

Toomey, P., & Gorski, A. (2021, Sep. 7). The Privacy Lesson of 9/11: Mass Surveillance is Not the Way Forward | News & Commentary. American Civil Liberties Union. https://www.aclu.org/news/national-security/the-privacy-lesson-of-9-11-mass-surveillance-is-not-the-way-forward

Wahl-Jorgensen, K.; Bennett, L.; and Taylor, G. (2017). The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations. *International Journal of Communication 11*, 740–762.

Whittaker, Z. (2021, June 7). Apple unveils new iOS 15 privacy features at WWDC. TechCrunch. https://techcrunch.com/2021/06/07/apple-wwdc-2021-privacy-security/

Wilander, J. (2020, March 24). Full Third-Party Cookie Blocking and More. WebKit. www.webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

Wolford, B. (2018, Nov. 7). What Is GDPR, the EU's New Data Protection law? GDPR.eu; European Union. www.gdpr.eu/what-is-gdpr/

Wyden, R. (2021, April 21). S.1265 - 117th Congress (2021-2022): Fourth Amendment Is Not For Sale Act (Legislation). www.congress.gov/bill/117th-congress/senate-bill/1265

Zhao, Q. (2022, Oct. 19). American Data Privacy and Protection Act: Latest, Closest, yet Still Fragile Attempt Toward Comprehensive Federal Privacy Legislation. Harvard Journal of Law & Technology. jolt.law.harvard.edu/digest/american-data-privacy-and-protection-act-latest-closest-yet-still-fragile-attempt-toward-comprehensive-federal-privacy-legislation

Zuckerberg, M. (2019, March 6). A Privacy-Focused Vision for Social Networking (Blog Post). www.facebook.com/notes/2420600258234172/