

Domestic Surveillance in the United States Post-9/11: The Role of Legislation and Large Technology Corporations


A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Hamza Mir
Spring, 2021

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

Signature  _____ Date 5/10/2021
Hamza Mir

Approved  _____ Date 5/4/2021
Hannah Star Rogers, Department of Engineering and Society

Abstract

Domestic government surveillance has been a major topic in public discourse since the Snowden surveillance programs in 2013. These leaks revealed the extent of government surveillance on US citizens, as well as some of the methods used to conduct this surveillance. One notable takeaway was the large technology corporations were largely the target of domestic surveillance programs. This research paper will discuss and analyze the reasons for this phenomenon, making use of the policy analysis and actor-network theory methodologies. With regards to policy analysis, Executive Order 12333, the Patriot Act, and the FISA Amendments Act of 2008 will be discussed. This paper will attempt to understand the implications of these documents as well as the surveillance programs they were used as a legal basis for. An actor network theory analysis will identify government agencies, technology corporations, and US technology users as actors. The connections between these actors will be assessed in order to attain an understanding of why large technology corporations are so often targets of domestic surveillance programs.

Domestic Surveillance in the United States Post-9/11

Over the past several decades the US government has made substantial investments in surveillance technologies for the modern era, which have been used to collect intelligence on both foreign entities as well as millions of American citizens. Additionally, many surveillance policies were put into place in response to the terrorist attacks of September 11th. Among the most influential of these policies was the USA PATRIOT Act, which allowed the government greater leeway on being able to collect information on citizens' communications ("Domestic Surveillance Overview," 2015). Following shortly was the FISA Amendments Act of 2008, which gave the National Security Agency "almost unchecked power to monitor Americans' international phone calls, text messages, and emails" ("NSA Surveillance", n.d.). More information on the extent of government surveillance came to light when former NSA contractor Edward Snowden leaked a series of documents exposing NSA spying programs that he considered to be unethical (Rusbridger & MacAskill, 2014). Snowden gained notoriety as a result of these leaks, and sparked a debate regarding the ethics of data privacy in the nation. The information he leaked revealed the government accessed the servers of private technology companies to collect intelligence (Ray, n.d.).

Using policy analysis and Actor-Network theory, this paper aims to assert that the United States government has increasingly turned to large technology companies to conduct domestic surveillance in the past several decades due to the vast amount of data available and recent legislation and ordinances that have allowed for that manner of surveillance. This paper is divided into two main sections. In the first section, the programs and policies regarding surveillance that the United States has put into place will be assessed using policy analysis in order to gain a better understanding of why these programs were put into place and how they

function. The three primary documents which will be discussed are Executive Order 12333, the Patriot Act, and the FISA Amendments Act of 2008. In the second section, the US government, large technology companies, and American citizens this issue will be assessed with the lens of Actor-Network theory in order to understand the relationships between them.

Policy Analysis

Executive Order 12333

Executive Order 12333, titled *United States Intelligence Activities*, was issued by President Ronald Reagan in 1981 which extended the powers of the US intelligence agencies (“Executive Order 12333”, 1981). Of particular interest are two clauses regarding data collection. The order states that “information obtained in the course of lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation” is permitted to be collected and retained by intelligence agencies, in addition to “information that may indicate involvement in activities that may violate federal, state, local or foreign laws.” However, the collection and retention of the latter type of information are only permitted if it is “incidentally obtained”. Incidentally collected data refers to data that does pertain directly to the intended target of surveillance, but happened to be collected in pursuit of that target (Gellman et al., 2014). This caveat, on the surface, seems to make Executive Order 12333 serve primarily as a basis for collecting data through *foreign* surveillance activities, which is generally less protected than domestic data. However, John Napier Tye, a former State Department official, has stressed that this latter clause has been used by NSA as the basis for collecting vast amounts of (incidentally obtained) domestic data, and that the order can even be invoked if information between two US citizens leaves the country temporarily (Tye, 2014). As an example, Tye states, “U.S. communications increasingly travel across U.S. borders — or are stored beyond them. For

example, the Google and Yahoo email systems rely on networks of ‘mirror’ servers located throughout the world. An email from New York to New Jersey is likely to wind up on servers in Brazil, Japan and Britain. The same is true for most purely domestic communications.”

Executive Order 12333 was also amended by two subsequent executive orders under the Bush administration following the attacks on the World Trade Center. The first of these amendments was Executive Order 13355 signed in 2004, which restructured intelligence agencies such that they would report information to the president through the Director of National Intelligence, a position created by Bush (“Executive Order 13355”, 2004). The other amendment was Executive Order 13470, which broadened and strengthened the role of the Director of National Intelligence (“Executive Order 13470”, 2008).

The Patriot Act

The “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act”, also known as the “USA PATRIOT Act” or the “Patriot Act”, was a piece of legislation passed about a month after the September 11 terrorist attacks. The Patriot Act gave law enforcement greater authority to investigate terrorism, including powers given to federal agents to request permission from banks and businesses to provide records to aid in terror investigations (“Patriot Act”, 2017). The Patriot Act had several sunset provisions, but these were renewed by the *USA PATRIOT Improvement and Reauthorization Act of 2005* and the *USA PATRIOT Act Additional Reauthorizing Amendments Act* in 2005 (“Patriot Act Renewal”, 2005). Further reauthorizations took place over the next decade. These included renewals under the Obama administration, including the Sunsets Extension Act of 2011, USA FREEDOM (Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective

Discipline Over Monitoring) Act of 2015, which curtailed some of the powers in the original Patriot Act in response to the Snowden leaks (Duignan, n.d.).

Among the most controversial aspects of this law, and the most relevant one in this discussion, is Section 215, which states that the law “Authorizes the Director of the FBI (or designee) to apply for a court order requiring production of certain business records for foreign intelligence and international terrorism investigations. Requires the Attorney General to report to the House and Senate Intelligence and Judiciary Committees semi-annually” (“H.R.3162”, 2001). These court orders are processed through the FISA court, which was established by The Foreign Intelligence Surveillance Act of 1978 to (non-publicly) consider issuing federal warrants (“The Foreign Intelligence Surveillance Act of 1978”, n.d.). This section is particularly relevant because in 2013, Edward Snowden — an ex-NSA contractor — leaked a FISA court order which used Section 215 to justify the establishment of a bulk data collection program which collected millions of Americans’ phone records; the court order specifically allowed the collection of data from Verizon, one of the largest American telecom companies (Greenwald, 2013). Section 215 of the Patriot, in conjunction with the FISA court, allowed the federal government to implement broad domestic surveillance measures in a manner that was secret and opaque, shielding it from the dissent of informed citizens. This is a pattern which reveals itself subsequent times in the subsequent sections of this paper. Obama’s USA Freedom Act amended Section 215, disallowing the bulk data collection program, and it finally expired in March of 2020 (McKinney & Crocker, 2020).

The FISA Amendments Act of 2008

This act amended the aforementioned Foreign Intelligence Surveillance Act of 1978. A controversial section of this legislation, which gained attention in the wake of the Snowden

leaks, is Section 702. Section 702 states, “Notwithstanding any other provision of law, pursuant to an order issued in accordance with subsection (i)(3) or a determination under subsection (g)(1)(B), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information” (“H.R.3773”, 2007). Following his leaks regarding the FISA court order on Verizon, Ed Snowden revealed that this section was used as the legal basis for PRISM, a program which allows the NSA to order businesses to hand over data (Braun et al., 2013). The companies included in the surveillance conducted under PRISM include Microsoft, Google, Yahoo, Facebook, Apple and more, with data being collected over the course of five years (Johnson et al., 2013). Snowden leaked Powerpoint slides from the NSA explaining the details of the program, which showed that the types of data collected by PRISM included email, videos, photos, VOIP, file transfers and more.

Policy Analysis Conclusion

Despite the fact that the aforementioned federal documents seem to focus primarily on foreign surveillance, they were used (arguably in an overreach) to conduct massive domestic surveillance initiatives involving the data of millions of Americans with limited transparency. They were used to justify domestic data collection programs by the intelligence community in the name of fighting terrorism. The target of these programs seemed by and large to be large technology companies. Notable examples of this were the FISA court order allowing the bulk collection of Verizon phone records by the NSA, and also the use of PRISM to order the handing over of data by large corporations such as Apple and Google. The subsequent section will assess the actors involved in this world of surveillance and the networks that hold them together, in

order to try and develop an understanding of why the federal governments' focus is on these large corporations when it comes to domestic surveillance.

Actor-Network Theory Analysis

ANT is a methodology developed by Bruno Latour, Michel Callon, and John Law that assesses technological impacts on society (and vice-versa) as a set of interconnected, shifting networks, made up of decision-making agents called “actors” that react to one another (Cressman, 2009). ANT was chosen as the framework for assessing the issue of domestic surveillance due to the number and variety of participants and institutions involved in surveillance, as well as their complexity. The framework provides a convenient way to organize and break down these participants and institutions, and by using it, an understanding of how domestic surveillance functions within and acts on society can be attained. ANT will be used to assert that the federal government has turned primarily to large technology companies to conduct domestic surveillance largely because of the vast amounts of data available. The actors identified here are the federal government and government agencies (including the NSA, CIA, and other intelligence agencies), large technology corporations such as the ones who were targeted by PRISM, and US-based technology users whose personal data is ultimately collected by intelligence agencies.

Federal Government and Government Agencies

At the forefront of the federal surveillance apparatus of the United States is the National Security Agency (NSA). The agency evolved from intelligence organizations that existed during World War II, and was formally established by President Truman in 1952 “to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments, to provide for integrated operational

policies and procedures pertaining thereto” (“National Security Agency”, n.d.). The NSA identifies one of its primary goals to be the collection of signals intelligence, known as SIGINT. As of 2010 the NSA was intercepting and storing “1.7 billion e-mails, phone calls and other types of communications” (Priest & Arkin, 2010). According to the agency, SIGINT is “intelligence derived from electronic signals and systems used by foreign targets” (“Signals Intelligence”, n.d.). As with the aforementioned legislation and executive orders, the NSA defines its targets to be purely foreign in nature, which evidence suggests has not been entirely true.

Following the September 11th attacks, the NSA began initiating a multitude of domestic surveillance efforts. By 2002, they had started reaching out to telecom companies to gain assistance with their surveillance programs, and in 2005 it was revealed that they had been installing backdoors into these companies to capture purely domestic data (Lithblau & Risen, 2005). Later on in 2013, Snowden revealed that the NSA utilized its PRISM program to collect large amounts of data from large internet companies, as previously mentioned. The NSA also developed a program dubbed “MUSCULAR,” which tapped into Google and Yahoo’s overseas-based facilities which included domestic communications (Gellman & Soltani, 2013). This, like with the case of “incidentally obtained” data, is yet another example of how the federal agencies are able to circumvent restrictions around collecting data from domestic targets like US citizens. For years, the NSA has been installing backdoors in commercial software and attempting to break encryption protocols; there have even been concerns that the NSA has worked directly with the National Institute for Standards and Technology to place backdoors into encryption protocols themselves (Larson, 2013). A leaked budget document reveals that two hundred and fifty million dollars were appropriated for the NSA to insert backdoors into

commercial encryption systems (Ombres, 2015). These numerous instances of efforts made to implement domestic surveillance programs indicate that the NSA has been interested in conducting domestic surveillance, and they wish to have access to as much data as possible, evidenced by their attempts to install backdoors into encryption protocols.

This desire to be able to collect vast amounts of data is clearly explained by A. Denis Clift, the former President of the National Defense Intelligence College, who wrote a report in 2003 discussing the internet in relation to the collection of intelligence by the US government. He asserted that the role of the US intelligence community is to provide the President with an information advantage (Clift, 2003). Clift states, "...the Internet and its communications channels are at the forefront of the signals intelligence challenges of the 21st century. With new transnational adversaries — international terrorists foremost among them — the flood of new information technologies, the easing of export controls on encryption technology, and global access to the Web, the National Security Agency (NSA) is charting new directions in the ways it identifies, gains access to, and successfully exploits target communications." Clift makes it clear that at the turn of the century, the NSA saw value in the nature and quantity of data aggregated on the internet, and developed goals to incorporate this data into its intelligence collection programs.

Another facet of the federal government that is pertinent to this discussion is the United States Foreign Intelligence Surveillance Court (FISC). As mentioned previously, FISC was established under The Foreign Intelligence Surveillance Act of 1978 to oversee requests for surveillance warrants, with many of these requests being submitted and processed in secret. As reported by Snowden, this was the court which issued the order for Verizon to provide the intelligence community with a daily feed of both domestic and foreign telephone records. Given

the *ex-parte* nature of the court, it has drawn criticism given the lack of transparency in the process of acquiring sensitive data from technology users — often US citizens. Since the court was established in 1979 up to and including 2017, there have been over forty-one thousand requests submitted, with all but eighty-five fully processed and approved ("Foreign Intelligence Surveillance Act Court Orders", n.d.). With so many requests processed and so few denied, experts such as former National Security Agency analyst Russ Tice have referred to the court as a "rubber stamp" (Ackerman, 2013). New York Times reporter Eric Lichtblau has reported on disclosures alleging that the FISC has developed secret surveillance laws which create exceptions to the Fourth Amendment (Lichtblau, 2013). Lichtblau writes "the court has taken on a much more expansive role by regularly assessing broad constitutional questions and establishing important judicial precedents, with almost no public scrutiny, according to current and former officials familiar with the court's classified decisions. The 11-member Foreign Intelligence Surveillance Court, known as the FISA court, was once mostly focused on approving case-by-case wiretapping orders. But since major changes in legislation and greater judicial oversight of intelligence operations were instituted six years ago, it has quietly become almost a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues and delivering opinions that will most likely shape intelligence practices for years to come, the officials said." It is clear that the judicial branch has also made an effort to extend the powers of the federal government to be able to conduct domestic surveillance.

The executive branch and federal legislature should likewise not be dismissed in their role of ramping up the collection of domestic data. Executive orders issued by Presidents Ronald Reagan and George W. Bush have been used as legal justification for several forms of domestic surveillance, such as the collection and retention of incidentally obtained data. Congress is of

course responsible for expanding or restricting which forms of surveillance are legal. Since 2001, more efforts have gone towards expanding, perhaps most infamously with the passing (and continuous renewal) of the Patriot Act. The federal government, including government agencies like the NSA, have substantial power when it comes to extracting data and information on US citizens. They are able to use the power of the law, along with secretly supplied approval from the FISA court, to compel companies to fork over data. Given that citizens are in the dark as to how and when this occurs, they have limited power over how domestic surveillance is conducted.

Large Technology Corporations

As Clift mentioned, the quantity of signals intelligence available is rapidly rising in the wake of the Internet. Some of the largest banks of personal data are stored in the hard drives of Internet and social media corporations. The focus here will be on corporations based in the United States, since US-based internet companies make up the largest (in terms of data collection) and most influential actors in this category. Perhaps the quintessential social media company of today is Facebook. Facebook boasts a staggering 2.8 billion daily active users as of December 2020 (“Facebook Reports Fourth Quarter”, 2021). The company reported in 2014 that it stores three hundred thousand petabytes of data in its data warehouse and processes four petabytes of data per day (Wiener & Bronson, 2014). The company’s size makes it a compelling target for hackers, and when breaches occur, innumerable quantities of data can be leaked. In 2021, the personal data of over half a billion Facebook users was leaked, which included phone numbers, email addresses, and more (Peters, 2021). Yet another colossal corporation is Google, whose search engine processes around 7 billion queries per day and dominates the internet search market with nearly 93% control (Petrov, 2021). Facebook also dominates its respective market,

accounting for over 60% of all social media visits in the United States (Tankovska, 2021). These companies, along with other internet companies track and collect information from users that visit their sites by monitoring their activity, using tracking cookies, and more (Nield, 2020). Amazon, Apple, Microsoft and other large internet corporations have similarly huge user bases, and transfer and store vast amounts of personal data. These types of companies tend to be oligarchic in nature — that is, only one or two companies control a majority of their respective market (e.g. Facebook and social media, Google and online search, Amazon and online retail, etc). The large quantities of data which these companies can be framed in terms of “surveillance capitalism”. According to Shoshana Zuboff, surveillance capitalism is a system “invented at Google and elaborated at Facebook” wherein numerous and diverse data points are collected from product users in order to form predictive models about what will engage users to drive profit for the company (Zuboff, 2019).

The companies can be requested or even compelled to hand over data by way of digital search warrants, and also through programs like PRISM. According to the Harvard Law Review, “Facebook received 32,716 requests for information from U.S. law enforcement between January 2017 and June 2017. These requests covered 52,280 user accounts and included 19,393 search warrants and 7632 subpoenas. In the same time period, Google received 16,823 requests regarding 33,709 accounts, and Twitter received 2111 requests regarding 4594 accounts. Each company produced at least some information for about eighty percent of requests” (“Cooperation or Resistance”, 2018). Additionally, the PRISM program forced companies like Google, Facebook, Apple, Yahoo!, and more to hand over user data, which the NSA then stored for its own use. Leaked documents revealed that PRISM was the number one source of raw intelligence for the NSA (“NSA Slides”, 2013). These corporations arguably have some power when it

comes to how the government is able to conduct domestic surveillance. Perhaps one of the most effective ways to limit the amount of data collected would be to give users the option to have less of their data collected from or encrypt data in such a way that only users can access it (although, this would threaten a critical revenue source for many of these corporations). These corporations could also contest the government's requests for data, and use their wealth and influence to lobby for better privacy guarantees for their users.

US Technology Users

An actor-network analysis of this topic is not complete without a discussion of actual users (based in the US) of the products offered by large internet corporations as part of this analysis, since it is their data that is being collected by the internet companies and subsequently, by the intelligence community. Non-US users have been omitted from this discussion to focus more on purely domestic surveillance. One could argue that users have the power to decide whether or not they use the products offered by these companies. On, the other hand, the inseparable integration of the internet with society and the oligarchic nature of internet industries certainly makes it difficult to remove oneself entirely from these products. In many cases, they are required to maintain social connections and be productive, and therefore users cannot help but use these technologies. Over 60% of Americans believe that it is impossible to go through daily life without data being collected about them (Auxier et al., 2019). Perhaps a more realistic way in which users might have power over domestic surveillance is by influencing Congress through activism and voting.

Actor-Network Theory Analysis Conclusion

Sociologist C. Wright Mills asserted that the economy and industries are intertwined with the political elite, stating, "There is no longer, on the one hand, an economy, and, on the other

hand, a political order containing a military establishment unimportant to politics and to money-making. There is a political economy linked, in a thousand ways, with military institutions and decisions. On each side of the world-split running through central Europe and around the Asiatic rimlands, there is an ever-increasing interlocking of economic, military, and political structures” (Mills, 1956). Communications expert Christian Fuchs expands on this idea as it relates to surveillance. He remarks, “the military-industrial complex contains a surveillance-industrial complex in which social media are entangled: Facebook and Google each have more than 1 billion users and have likely amassed the largest collection of personal data in the world” and posits that surveillance capitalism and the surveillance state interact strongly with another (Fuchs, 2017). This interaction is clear through the NSA’s use of PRISM, FISC orders, and more to place data collected by large technology corporations such as Google and Facebook into the hands of the government. The NSA has prioritized collecting large amounts of data as the popularity of the Internet has risen, and internet companies have been able to produce it. Users seem to willingly submit their data to the Internet, possibly because society has become so dependent on the internet that they have no choice.

Conclusion

EO 12333, the Patriot Act, and the FISA Amendments Act laid out the foundation for government agencies to conduct surveillance on large technology companies. They took advantage of these documents and used them as legal bases for programs like PRISM and MUSCULAR, the collection of incidentally obtained data, access to feeds of data from US telecom companies, and more. Additionally, at the turn of the century, the NSA developed goals to gain access to new and bountiful forms of signals intelligence made available by the internet. It recognized that large technology corporations had access to large stores of personal data, and

focused many of their surveillance efforts on them in order to get access to as much data as possible. An ANT analysis of the actors and networks involved in domestic surveillance revealed strong coupling between “surveillance capitalism” — internet companies’ collection of data as a system for making profit — and the surveillance state. ANT is often criticized for being highly subjective when it comes to determining who and what the relevant actors of a social system are. This paper mitigates this issue by considering actors in broad terms/categories (i.e. the federal government, large internet companies, etc) and treating more specific entities (e.g. the NSA) as “sub-actors”, so that another author’s subjective selection of actors are likely to fall under the categories discussed here. The tightrope between security and privacy will always be a difficult one to walk. Greater transparency from the federal government and more data privacy choices provided by large technology companies to their users may be potential first steps to protecting the American people as well as their privacy.

References

- Ackerman, S. (2013, June 6). Fisa chief judge defends integrity of court over Verizon records collection. *The Guardian*.
<https://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance>
- Clift, A. D. (2003). Intelligence in the Internet Era. *Studies in Intelligence*, 47(3), 73–79.
- Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance. (2018). *Harvard Law Review*, 131(6), 1722–1741.
- Duignan, B. (n.d.). *Patriot Act*. <https://www.britannica.com/topic/USA-PATRIOT-Act>
- Esau, L. A. (2017). The Correlation between Wiretapping and Terrorism: A Comparative Analysis of American and European Societal Views on Government Surveillance. *ILSA Journal of International & Comparative Law*, 23(1), 55–76.
- Executive Order 12333—United States intelligence activities*. (1981). National Archives.
<https://www.archives.gov/federal-register/codification/executive-order/12333.html>
- Facebook Reports Fourth Quarter and Full Year 2020 Results. (2020, January 27). *Facebook Investor Relations*.
<https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx>
- Foreign Intelligence Surveillance Act Court Orders 1979-2017. (n.d.). *EPIC*.
<https://epic.org/privacy/surveillance/fisa/stats/default.html>
- Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page*. (n.d.).

<https://www.brennancenter.org/our-work/research-reports/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333>

Fuchs, C. (2017). *Social Media: A Critical Introduction* (2nd ed.). SAGE.

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*.

https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gellman, B., Tate, J., & Soltani, A. (2014, July 5). In NSA-intercepted data, those not targeted far outnumber the foreigners who are. *The Washington Post*.

https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*.

<https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

H.R. 3773—*FISA Amendments Act of 2008*. (n.d.).

<https://www.congress.gov/bill/110th-congress/house-bill/3773/text>

H.R.3162—*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. (n.d.).

<https://www.congress.gov/bill/107th-congress/house-bill/3162>

- Johnson, K., Martin, S., O'Donnell, J., & Winter, M. (2013, June 6). NSA taps data from 9 major Net firms. *USA Today*.
<https://www.usatoday.com/story/news/2013/06/06/nsa-surveillance-internet-companies/2398345/>
- Larson, J. (2013, September 5). Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security. *ProPublica*.
<https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption#:~:text=Series%3A%20Dragnets-,Revealed%3A%20The%20NSA's%20Secret%20Campaign%20to%20Crack%2C%20Undermine%20Internet%20Security,and%20others%20around%20the%20world.>
- Licthblau, E. (2013, July 6). In Secret, Court Vastly Broadens Powers of N.S.A. *The New York Times*.
<https://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html>
- Licthblau, E., & Risen, J. (2005, December 24). Spy Agency Mined Vast Data Trove, Officials Report. *The New York Times*.
- McKinney, I., & Crocker, A. (n.d.). *Yes, Section 215 Expired. Now What?*
- Mills, C. W. (1956). *The Power Elite*. Oxford Press.
- National Security Agency. (n.d.). In *Encyclopedia Britannica*.
<https://www.britannica.com/topic/National-Security-Agency>
- Nield, D. (2020, January 12). All the Ways Facebook Tracks You—And How to Limit It. *Wired*. <https://www.wired.com/story/ways-facebook-tracks-you-limit-it/>

NSA Slides Explain the PRISM Data-Collection Program. (2013, June 6). *The Washington Post*.

<https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>

Ombres, D. (2015). NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform. *Seton Hall Legislative Journal*, 39(1), 27–58.

Patriot Act. (2017, December 19). *History.Com*.

<https://www.history.com/topics/21st-century/patriot-act>

Patriot Act Renewal Resisted by Bipartisan Group. (2005, November 17). *The Washington Times*. <https://www.washingtontimes.com/news/2005/nov/17/20051117-111241-2085r/>

Peters, J. (2021, April 4). Personal data of 533 million Facebook users leaks online. *The Verge*.

<https://www.theverge.com/2021/4/4/22366822/facebook-personal-data-533-million-leaks-online-email-phone-numbers>

Petrov, C. (2021, February 17). The Stupendous World of Google Search Statistics.

TechJury. <https://techjury.net/blog/google-search-statistics/>

Priest, D., & Arkin, W. (n.d.). *A hidden world, growing beyond control*.

<https://www.washingtonpost.com/investigations/top-secret-america/2010/07/19/hidden-world-growing-beyond-control-2/>

Ray, M. (n.d.). Edward Snowden. In *Britannica*.

<https://www.britannica.com/biography/Edward-Snowden>

Signals Intelligence. (n.d.). NSA. <https://www.nsa.gov/what-we-do/signals-intelligence/>

Tankovska, H. (2021, February 10). Most famous social media sites in the U.S. 2021.

Statista.

<https://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us/>

The Foreign Intelligence Surveillance Act of 1978. (n.d.).

<https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286>

Tye, J. N. (2014, July 18). *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans.*

https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html

Wiener, J., & Bronson, N. (2014). Facebook's Top Open Data Problems. *Facebook*

Research. <https://research.fb.com/blog/2014/10/facebook-s-top-open-data-problems/>

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New*

Labor Forum. https://journals.sagepub.com/doi/10.1177/1095796018819461#_i2