Glenn Findlay 11/2021

Edward Snowden: Hero or Traitor?

On May 20, 2013, NSA contractor Edward Snowden fled to Hong Kong with a vast quantity of highly classified documents he had downloaded from his workplace at an NSA facility in Hawaii. Over the coming weeks he would share thousands of these documents with journalists. They contained many revelations about the extent of the NSA's surveillance capabilities, which included secret programs that enabled them to defeat trusted security measures and collect data on a scale that few would have imagined.

The programs revealed by these documents ignited a debate about whistleblowing and government surveillance. Are such programs necessary to ensure the safety of Americans, or were they a dangerous and even illegal overreach by government intelligence? Should Snowden be applauded for having cast light on dubious government programs, or should he be arrested and prosecuted as a traitor who revealed some of his country's most closely guarded secrets?

In this essay I will work to address each of these issues in turn. First I will provide more detail into the nature of the programs revealed. Then I will cover important points in the relevant debates surrounding whistleblowing and government surveillance, and explore the ethics and laws involved.

Who is Edward Snowden?

Snowden was born into a family with a tradition of public service. His father and maternal father were both officers with the coast guard, and his mother was a chief deputy clerk at the U.S. District Court for the District of Maryland[1]. In 2003 he enlisted in the army because, in his words, "I felt like I had an obligation to help free people from oppression" [2] but he was discharged after breaking both legs in a training accident. Shortly after he began to work in IT security at CIA facilities, where he was quickly successful due to his understanding of the internet and his talent for programming.

According to *Ars Technica*, Snowden had been active on the site's online forums for many years under the pseudonym "TheTrueHOOHA" and had posted as recently as 2012. On many occasions TheTrueHOOHA showed strong support for U.S. security agencies, and in January 2009 criticised the

New York Times for publishing previously-secret details of U.S. attempts to sabotage Iranian nuclear infrastructure. Their anonymous sources should, he said, “be shot in the balls.” [3]

As his career progressed, Snowden became disillusioned with U.S. security agencies and their impact on the world. In his words, “I realised I was a part of something that was doing far more harm than good.”[1] At some point he became interested in internet freedom organizations such as the Electronic Frontier Foundation and the Tor project.

Investigators believe that Snowden began amassing documents describing government surveillance programs in April of 2012, [4] when he was at that time working as a contractor for the NSA. He continued to do so until May 2013, when he fled to Hong Kong and began to share his trove of top-secret documents with journalists. Just over a month later he boarded a flight to Moscow, and he has remained in Russia since. According to Snowden, he had destroyed or shared with journalists all the classified documents in his possession before leaving Hong Kong.[4] He also claims that he never intended to remain in Russia, but that he was left stranded there when the U.S. cancelled his passport.[4]

Snowden chose not to opt for anonymity because, in his words, “I have no intention of hiding who I am because I know I have done nothing wrong.” [1] In public statements, intelligence officials have sought to minimize his work for the NSA by describing him as a low-level systems administrator. He pushed back vehemently against this characterization of his work, saying “I was trained as a spy in the traditional sense of the word in that I lived and worked undercover overseas – pretending to work in a job that I’m not – and even being assigned a name that was not mine… I developed sources and methods for keeping our information secure in the most hostile and dangerous environments in the world.” [5]

What was revealed?

The documents that Snowden shared with journalists revealed a number of secret information-gathering programs of unprecedented ambition and scope. Some estimates have placed the number of documents he shared with journalists in the hundreds of thousands,[4] but here I will try to highlight some of the most outstanding revelations.

The NSA divides online surveillance into a couple of broad categories; ‘upstream’ and ‘downstream.’ Upstream surveillance generally involves the direct collection of internet traffic as it passes

through infrastructure such as fiber optic cables. ‘Downstream’ surveillance, on the other hand, describes the collection of data stored by companies such as Google, Facebook, Microsoft, and others.

Documents leaked by Snowden describe PRISM, a downstream surveillance program that allowed the NSA to directly reach into data housed by Google, Apple, and other cloud storage companies to extract emails, photos, contact lists and many other kinds of data. It also allowed for the agency to collect ‘huge quantities of raw internet traffic at major network exchange points’ by scanning in-transit internet packets for particular keywords. [6] The NSA had broad powers to obtain this data on communications between foreigners so long as they were deemed to be relevant to the broadly defined category of ‘foreign intelligence information.’ [7] Communications between foreigners and U.S. citizens could also be collected, meaning that potentially huge amounts of American communications and other sensitive data could also be swept up, without the need for a warrant.[7]

The documents revealed by Snowden also included a top secret court order issued by an intelligence court that required Verizon to provide the NSA with information on all the calls in their systems, updated on an ‘ongoing, daily basis’ over a 3-month period.[8] This data did not include the content of the calls themselves, but it did include certain ‘metadata’ including phone numbers, call time and duration, and location data. Members of congress later confirmed that similar orders had been issued every 3 months for years.[9]

The leaked documents also describe the ‘MUSCULAR’ program wherein the NSA would collect data by tapping directly into fiber optic cables owned by companies such as Google, Yahoo, and others. The PRISM program had some limitations in that much of the raw traffic collected was encrypted, and ‘PRISM requests are relatively limited in scope.’ [6] By tapping into data connections between data storage centers and within company security perimeters, the NSA could collect vast amounts of unencrypted traffic. The NSA took care to place these taps overseas, where the agency is subject to less restriction and oversight.[10] Legally, they are allowed to assume that all data collected outside the U.S. belongs to foreigners and collect data in a way that would be illegal in the U.S. itself. Happily for the NSA, many companies will backup their data across various data centers, replicating data for the purposes of backup and universal access. This means that the data of many Americans would be collected on these taps, even if they had never travelled overseas.[10]

The documents leaked by Snowden also detail ongoing efforts by the NSA to defeat or circumvent standards of encryption. Even with powerful supercomputers at their disposal, government intelligence agencies often struggle to circumvent modern encryption standards.[11] Their best option is often to go over, under, or around encryption - but rarely through it. In the words of cryptographer Adi Shamir, “Cryptography is typically bypassed, not penetrated.” [11] One approach used by the NSA was to collaborate with technology companies to intentionally insert weaknesses or ‘backdoors’ into commercial encryption software.[12] This program, which appears in leaked slides as “SIGINT [signals intelligence] enabling”, received $254.9 million in funding in 2013 alone.[24] In another case, the NSA succeeded in stealing encryption keys used by a SIM card manufacturer named “Gemalto” and based in the Netherlands, allowing them to decrypt communications on vast numbers of mobile phones around the world.[11]

It is difficult to know what happens internally at the NSA, but there are some signs that growing pains set in as the agency began to absorb previously unfathomable quantities of data. Databases became clogged with vast amounts of spam emails,[6] analysts complained of ‘drowning’ in data, and some NSA officials grumbled about the ballooning costs of ‘collect-it-all’ style programs.[13] In response, the NSA began to develop sophisticated tools to efficiently trawl through data collected. One such tool, ‘XKEYSCORE’, was described by *The Intercept* as a kind of ‘google for the world’s private communications.’ [14] Using this tool, an analyst could easily filter and study online activity. One leaked slide displays a search in which an analyst queries the system for “all individuals in Pakistan visiting specific German language message boards.” [14] XKEYSCORE also provides powerful tools for studying the online activity of individuals – an analyst can conduct sweeping searches simply entering a person’s email address, name, or telephone number ‘with just a few clicks.’ Apparently, this tool was used in hacking Gemalto’s network, by enabling spies to stalk the online activity of employees and uncover their usernames, passwords, and email. [14]

One recurrent issue in NSA offices was a tendency of analysts and officers to use their surveillance tools to spy on love interests, a practice referred to as "LOVEINT" by NSA employees. Documents leaked by Snowden reveal that internal audits found the NSA breaks its own privacy rules thousands of times a year. [25]

Were these programs legal?

In United States law the cornerstone of privacy is 4th amendment, which says that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." This is to say, a person's privacy can only be violated after a warrant is issued, and the warrant must specifically detail the 'persons or things to be seized'. In 1986, the Electronic Communications Privacy Act (or ECPA) clarified that electronic communications and data are protected, and law enforcement will need a warrant to acquire them.[15] Certain kinds of metadata such as records about phone use have a lower level of protection, however, and can be obtained by law enforcement with a court order. In general court orders require a lower standard than a warrant and are easier to obtain.

Legally, the Fourth Amendment is understood to protect U.S. citizens and residents only. From a legal standpoint, it is very easy for the NSA to read the emails (for example) of foreigners provided they can in some way be obtained. In the case of the overseas tapping of fiber optic cables, the NSA is allowed to collect such data en masse by assuming that the targets will be foreigners.[10]

In 1978, the Foreign Intelligence Surveillance Act (FISA) was passed into law, with the intention of curtailing the NSA's capacity to spy on Americans. At that time, surveillance by the NSA of activists, civil rights leaders and others had caused a widespread backlash, and this law specified for the first time that the NSA was for the purpose of foreign surveillance.[16] If they believed that a foreign agent or spy was operating in the U.S. they would need to obtain a warrant from a Foriegn Intelligence Surveillance Court, or FISC, a secretive court where cases are presented behind closed doors and decisions are made away from the public view. As of 2008, the Fisa Amendments Act allowed for the warrantless collection of communications, in the case where at least one end of the exchange is outside of the U.S. It also clarifies that no warrant is needed for surveillance targeting a U.S. person overseas.[16] This further broadened the possibilities for the data of Americans to be swept up in foreign surveillance, and provided the legal basis for programs such as PRISM where vast amounts of communications between Americans and foreigners was collected.

According to the NSA, court orders such as the once compelling Verizon to share call metadata with the NSA were authorized under section 215 of the Patriot Act, which allows the government to order companies to collect “tangible things” that aid in a terrorism or espionage investigation. This interpretation of the law was accepted for years by FISC judges.[16] In 2015, however, a federal appeals court ruled in favor of the A.C.L.U and declared that these requests were illegal and used an interpretation of that language that was overly broad and beyond the scope of the law’s original purpose.[17]

A great deal of the NSA’s overseas surveillance activities are authorized by Executive Order 12333, signed in 1981 by President Raegan, which authorized the collection of any intelligence relevant to ‘national defense’ as long as it is not specifically prohibited by any other law.[16] In general, these activities are outside the scope of the FISC and receive very little congressional oversight. The NSA may be required to justify that the collection of data is relevant to defense, but the agency will only need to make this case to itself and individuals in the executive branch.[10]

By and large, the NSA did operate within the confines of existing laws. Loopholes were exploited creatively and aggressively, however. In particular, lax rules regarding the surveillance of foreign communications and the overseas collections of data allowed them tremendous leeway in collecting data on Americans in ways that would otherwise require a warrant. Some of the programs revealed required very little oversight from courts or from Congress. Many of their surveillance activities were approved by FISC judges. As to whether the laws under which the NSA operated were consistent with the 4th amendment is a broader question that I will return to later.

In 2015, the USA Freedom Act was passed. It banned the bulk collection of metadata via court orders and constrained requests for such data to be more specific.[18] It also allowed companies to disclose more information about FISA orders they receive, and moderately increased the amount of information about FISC court rulings that would be accessible to the public. [18]

Were these programs ethical?

In my opinion, the rules that spies must follow do not conform to what I see as a consistent ethical framework. While U.S. citizens and residents are protected by the Fourth Amendment, the rights of foreigners do not appear to be well defined. This raises an obvious ethical issue - foreign people

obviously have rights - and also opens up enormous loopholes that have allowed the NSA to scoop up huge amounts of data about Americans. In foreign and overseas intelligence gathering, the NSA is able to operate with minimal oversight and collect huge amounts of sensitive data on Americans that they would otherwise require a warrant to obtain. While court decisions and the USA Freedom Act have introduced more limits on the bulk collection of Americans' phone and internet metadata, this basic loophole remains intact.

These leaks also suggest the question of how exactly 'metadata' is defined. It is easy to imagine many contexts in which the information contained in metadata could be equally as sensitive as the content of the message itself. At the time when the Verizon court order was signed, the company had around 121 million customers.[9] Potentially, a single secret court order could have furnished the NSA with the data they would need to map the relationships, habits and even movements of a huge fraction of the U.S. population. While subsequent reforms have placed some limits on metadata collection, I feel that we still need an approach that is more sensitive to the highly contextual value of such data.

In an interview, one former intelligence official justified wide-reaching surveillance by referring to the analogy of a needle in a haystack.[16] In order to find the needle, he argued, it is necessary to have the whole haystack. Intelligence services will need to cast a wide net if they are to catch criminals or terrorists who are careful to cover their tracks. Their analysts are trained and disciplined, and can be trusted to use the information they have access to in a responsible way.

On the other hand, civil rights advocates criticized the secretive proliferation of government surveillance techniques. How can democracy function if the American people don't know what their government is doing or capable of?

The Snowden leaks revived long-running debates around the tradeoffs between privacy and security. One the one hand, privacy skeptics will cite the adage of "if you have nothing to hide, then you have nothing to fear" essentially displacing concerns about government surveillance as based on irrational fear. On the other hand, many privacy advocates see new surveillance technologies as potential steps towards a 1984-style scenario of mass-surveillance and totalitarianism.

In my research, I've come to feel that the privacy vs. security debate is at once too simplistic and too abstract to resonate with many people. Reading through accounts of the NSA's secret programs, it

becomes evident that many kinds of surveillance entail a very real human cost and present unique dangers that threaten to wipe out both privacy and security in one fell swoop. Once created, surveillance tools can be abused by individual employees, or can be co-opted for political ends. XKEYSCORE was once used to obtain the talking points of Secretary General Ban Ki-moon before a meeting with President Obama.[14] In spending 250 million a year to insert weaknesses into security products, the NSA directly undermines the work done by the NIST (National Institute for Standards and Technology), another government agency responsible for recommending cybersecurity standards, and creates dangerous security flaws that could potentially do tremendous harm if they were discovered by criminal groups. This is not idle speculation; over the years, a number of hacking tools developed by the NSA have fallen into the hands of criminal groups,[26] a phenomenon that has both puzzled and infuriated NSA officials.

Is whistleblowing illegal?

Government employees with a security clearance will sign agreements of secrecy that are broken when they leak information to the public. The consequences for breaking these agreements include the removal of the leaker from their job and the revocation of their security clearance.[19] These are modest civil penalties and generally will be merely the first step when the government decides to opt for the litigation of a whistleblower.

In some cases, the leaker can be charged with theft or unlawful possession of government property.[19] These offenses can be prosecuted as felonies and entail a penalty of up to 10 years in prison per charge.

When it comes to the litigation of whistleblowers, the sharpest tool in the government's arsenal is the Espionage Act of 1917. The espionage act was originally intended for use against spies and traitors working for foreign rivals. In the 1950s, The Act was famously (and successfully) used against Ethel and Julius Rosenberg and Morton Sobell, military engineers found guilty of handing nuclear secrets to the Soviets.

More recently, the act has been used for the purpose of litigating whistleblowers, on the basis that their revealing of state secrets constitutes a form of espionage. In 1976 the Act was used against Daniel Ellsberg, a military analyst who leaked an internal Pentagon study detailing how the scope of the Vietnam

war had been expanded beyond the public's knowledge. The judge dismissed the case against him when it was revealed that the government had recorded his conversations without a court order and performed other kinds of illegal evidence gathering.

In 1998, the Intelligence Community Whistleblower Protection Act established certain protections for intelligence whistleblowers against retaliation or reprisal. In order to be protected under the Act, however, a whistleblower must file a complaint through official channels where there is no guarantee that their complaint will be considered valid.[20] According to Snowden, "You have to report wrongdoing to those most responsible for it." [21] According to him he made various efforts to report through official channels before he began leaking documents to journalists, although this claim is disputed by the NSA.

In 2010, military analyst Chelsea (then Bradley) Manning leaked a vast quantity of classified videos and documents. The videos included footage of U.S. soldiers shooting innocents, and nearly 700,000 military and diplomatic documents.[15] Manning was found guilty of violating the Espionage Act, as well as theft, and sentenced to 35 years. In 2017 her sentence was commuted by President Obama, and she is now free. Prior to Snowden, this was the most significant leak in the history of U.S. intelligence.

In June of 2013, federal prosecutors filed charges against Snowden consisting of one count of theft of government property and two counts of violating the Espionage Act. If he were found to be guilty of all these charges, he would face a maximum of 30 years imprisonment.

In 2019 a judge ruled that Snowden's new book, Permanent Record, violated non-disclosure agreements he signed while working for the NSA. U.S. authorities did not try to stop publication of the book but merely to seize the proceeds. The court ruled that royalties from the book would be paid into a trust held by the U.S. government, which has accrued at least $5.2 million USD.[22]

Is whistleblowing ethical?

According to the Electronic Frontier Foundation, "whistleblowers often serve as a last-resort failsafe when there are no other methods of bringing accountability to secretive processes." [23] By this view, when government programs overrun the laws and moral codes that should guide them and oversight mechanisms fail to correct, there is no other remedy than for a whistleblower to bring knowledge of their doings directly to the American public.

Of course, intelligence agencies treasure any program or technique that gives them an edge, in a world where foreign powers are developing their own surveillance strategies and proliferating use of encryption threatens to compromise their ability to perform basic surveillance. From the NSA's perspective, a leaker of classified information and a spy may have some things in common. In either case, a valuable source or method is lost and the agency is potentially set back in their ability to collect valuable information.

In many ways, however, the use of the Espionage Act against whistleblowers seems inappropriate. As defined by the Act itself, the crime of espionage involves the intention for the information "to be used to the injury of the United States or to the advantage of a foreign nation." But many leakers of classified information such as Snowden or Manning genuinely see themselves as acting in service of the constitution and the American public.

In my opinion, the current legal framework for dealing with whistleblowers is insufficient. Trying to cast them traitors or spies is inaccurate and unfair. Having studied the case of Edward Snowden, I now believe that the determination of whether whistleblowing is an ethical act comes down to three main factors. Firstly, what are the motivations of the whistleblower - did they release information out of greed, carelessness, or loyalty to a foreign adversary, or because they were genuinely troubled by a crisis of conscience that compelled them to reveal certain information? Secondly, was the information revealed genuinely in the public interest and did it lead to significant reforms or other positive outcomes? Finally, did the whistleblower handle sensitive and classified materials in a way that demonstrated responsibility, or did they indiscriminately release documents in a way that unnecessarily put others at risk? Obviously, we want our laws to conform to our sense of ethics as closely as possible, and for that reason I would prefer to see a legal code that more closely reflects these core principles.

From my research, it appears that Snowden believed his actions were in service of the public. They have led to intense public discussion and real reforms like the USA Freedom Act. He claims that he did not indiscriminately hand documents over to journalists although, given that some estimates place the total number of documents released in the hundreds of thousands,[4] I do have my doubts about just how selective he was or could have been. While he does not perfectly fit the mold of a hero, he is certainly not a traitor.

References

1. Marbella, J. (2013, June 10). *Details about Edward Snowden's life in Maryland emerge*. *The Baltimore Sun*. Retrieved from https://www.baltimoresun.com/maryland/bs-xpm-2013-06-10-bs-md-snowden-profile-20130610-story.html

2. Greenwald, G. (2013, June 11). Edward Snowden: the whistleblower behind the Nsa surveillance revelations. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

3. Mullin, J. (2013, June 26). In 2009, Ed Snowden said leakers “should be shot.” Then he became one. *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2013/06/exclusive-in-2009-ed-snowden-said-leakers-should-be-shot-then-he-became-one/.

4. McCabe, S. (2014, April 23). The Snowden Saga: A Shadowland Of Secrets And Light. *Vanity Fair*. Retrieved from https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.

5. Windrem, R. (2014, May 28). Edward Snowden's Motive Revealed: He Can 'Sleep at Night'. *NBC News*. Retrieved from https://www.nbcnews.com/feature/edward-snowden-interview/edward-snowdens-motive-revealed-he-can-sleep-night-n116851.

6. Gallagher, S. (2013, October 31). How the Nsa's Muscular tapped Google's and Yahoo's private networks. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/.

7. Greenwald, G. (2013, June 7). Nsa Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

8. Greenwald, G. (2013, June 6). Nsa collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

9. Court order to spy on Verizon users is a 3-month renewal of ongoing practice: Feinstein. (2013, June 6). *The New York Post*. Retrieved from https://nypost.com/2013/06/06/court-order-to-spy-on-verizon-users-is-a-3-month-renewal-of-ongoing-practice-feinstein/.

10. Gellman, B. (2013, October 14). Nsa collects millions of e-mail address books globally. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

11. Scahill, J., & Begley, J. (2015, February 19). How Spies Stole The Keys To The Encryption Castle. *The Intercept*. Retrieved from https://theintercept.com/2015/02/19/great-sim-heist/.

12. Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*. Retrieved from https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.

13. Maass, P. (2015, May 28). Inside Nsa, Officials Privately Criticize “Collect It All” Surveillance. *The Intercept*. Retrieved from https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/.

14. Marquis-Boire, M., Greenwald, G., & Lee, M. (2015, July 1). Xkeyscore: Nsa’s Google for the World’s Private Communications. *The Intercept*. Retrieved from https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.

15. Baase, S., & Henry, T. (2019). Ch. 2-3. In *A gift of fire: Social, legal, and ethical issues for Computing Technology* (5th ed., pp. 78–164), Pearson.

16. Macaskill, E., & Dance, G. (2013, November 1). Nsa Files: Decoded - What the revelations mean for you. *The Guardian*. Retrieved from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5.

17. Savage, C., & Weisman, J. (2015, May 7). N.S.A. Collection of Bulk Call Data Is Ruled Illegal. *The New York Times*. Retrieved from https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html.

18. Usa Freedom Act: What’s in, what’s out. (2015, June 2). *The Washington Post*. Retrieved from https://www.washingtonpost.com/graphics/politics/usa-freedom-act/.

19. Gellman, B. (2020, June). Since I Met Edward Snowden, I've Never Stopped Watching My Back. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2020/06/edward-snowden-operation-firstfruits/610573/.

20. Savage, C. (2019, September 25). Intelligence Whistle-Blower Law, Explained. *The New York Times*. Retrieved from https://www.nytimes.com/2019/09/20/us/whistleblower-law-explained.html.

21. Risen, J. (2013, October 17). Snowden Says He Took No Secret Files to Russia. *The New York Times*. Retrieved from https://www.nytimes.com/2013/10/18/world/snowden-says-he-took-no-secret-files-to-russia.html.

22. (2020, October 1). *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2020/oct/01/edward-snowden-book-permanent-record-court.

23. Reitman, R. (2016, June 5). *3 years later, the Snowden leaks have changed how the World sees NSA Surveillance*. Electronic Frontier Foundation. Retrieved December 9, 2021, from https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.

24. Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: how Us and Uk spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

25. Peterson, A. (2013, December 31). Here's what we learned about the Nsa's spying programs in 2013. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/12/31/heres-what-we-learned-about-the-nsas-spying-programs-in-2013/.

26. Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. (2017, November 12). *The New York Times*. Retrieved from https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.