CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Social Sciences

Master thesis

2022 **Kylie McCardel**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Social Sciences

Kylie McCardel

The Impact of Edward Snowden on Modern and Ontological Security in the United States and Europe

Master thesis

Prague 2022

Author: Kylie McCardel
Supervisor: Luděk Michálek

Academic Year: 2021/2022

Bibliographic note

MCCARDEL, Kylie. *The Impact of Edward Snowden on Modern and Ontological Security of the United States and Europe*. 66 p. Master thesis. Charles University, Faculty of Social Sciences, Institute of Social Sciences. Supervisor Luděk Michálek.

Abstract

This thesis will discuss the impacts of whistleblower Edward Snowden from his 2013 leaks of confidential documents to global media. In context of these leaks, this thesis will seek to determine the resulting changes and advancements made in the field of whistleblowing, as well as highlight other important whistleblowers in primarily American history to demonstrate the importance of their actions over the years for legislative change. Additionally, this thesis will also examine how corporations and private citizens have reacted to the Snowden revelations, with emphasis on the corporations' reactions following several major events in American society, as these entail the potential data leak from private devices.

Keywords

Securitisation, transparency, personal privacy, data mining, data protection

Range of thesis: character count: 142,778; 66 pages

Declaration of Authorship

1. The author hereby declares that she compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Prague, 30/7/22, Kylie McCardel

Table of Contents

Chapter One: A History of 2013 and Edward Snowden's Publications

On the sixth of June, 2013, the United States was rocked with the revelations that the National Security Agency was spying on them, creating an environment of fear and unrest amongst the American people. Two newspapers, *The Guardian* and *The Washington Post*, began releasing a series of reports that were leaked to them by an at-the-time anonymous source. Laura Poitras, the main journalist and documentarian involved with the Snowden files alongside Glenn Greenwald and Ewen MacAskill, communicated with Snowden for six months before the release of the articles, with Snowden using the pseudonym 'Citizenfour' for the sake of anonymity (Greenberg, 2014). A few days following the release of the articles, Edward Snowden chose to share with the country that he was the source of the information leaked to newspapers around the world.

Snowden, a former security contractor with the National Security Agency (hereinafter: NSA), revealed the now-pervasive fact that the American government utilised the agency in a way which enabled it to spy upon its own citizens (Ralston, 2014). The aspect about this revelation raised the already-elevated fear of the average American, not because the government truly was spying on them, but rather that the spying was not limited to those who were suspected to be terrorists, threats to national security, or merely criminals, but rather included law-abiding citizens as well. This thesis will seek to analyse the impacts of the revelations made by Edward Snowden upon the American people, while also analysing why Snowden chose to act the way he did, in spite of the very real (and ultimately factual) possibility that the United States Government would consider him a traitor. Additionally, this thesis will discuss how the revelations changed the mindset of security for everyday citizens, and what these changes meant for the government's information security legislation.

This thesis additionally seeks to research and analyse the impacts of Edward Snowden's revelations upon the ontological security of individuals both in the United States and in other countries across the world. With this in mind, the thesis will also perform a comparative look of the beliefs of individuals in regard to security in the first few years following the Snowden revelations, as well as the modern-day beliefs nearly a decade following.

Finally, this thesis will aim to highlight the importance of transparency within society and the positive effects whistleblowers generally have on society and on the organisations in which they whistleblow.

Following three days of released reports and considerable upheaval in both the private sector as well as the national security sector, Edward Snowden finally disclosed that he was the source of these reports. Snowden, a contractor for the NSA and the CIA, gave more credence to the potential veracity of these reports. Despite this, having a face behind the leaks as a demonstration of faith that they were not falsified did not quell any fears about false reporting, but rather led to the question of whether or not Snowden's acts demonstrated evidence of treason or traitorous behaviour through his "betrayal" of the NSA's strict security policies. With this in mind, this thesis will also seek to explain the legacy of Snowden's leaks, and how his work has individually impacted surveillance legislation and public opinion regarding government surveillance.

What were the key moments that led Edward Snowden to revealing one of the most shocking secrets of the United States' government in the twenty-first century? Why did a seemingly loyal, highly intelligent man decide to share this information with the world and end his own career (Harding, 2014)? What were the impacts upon domestic and international security, as well as ontological security, due to the impacts of Edward Snowden's revelations? This thesis seeks to research all of these questions and provide a concise response for the understanding of the 2013 Snowden Revelations.

Chapter Two: Literature Review

This thesis will use the publications of Edward Snowden (those from *The Washington Post* and *The Guardian*) to provide evidence for the reasoning behind the changes in ontological security. Specifically, the writings of Laura Poitras, Glenn Greenwald, and Ewen MacAskill will be featured, as these three journalists received the information and directly interviewed Snowden in the days leading up to the information release. Additionally, it will focus on writings and analysis by journalists and academics, who will each individually provide insight into how Edward Snowden impacted the ideals of security for the American people. Such writings will include analyses and theses written by United States-based individuals. These writings and analyses will be additionally supplemented with the documents released by Edward Snowden, published and maintained by the Snowden Archive, a Canadian journalist initiative for the protection of information and free press.

In addition to newspaper articles and reports, this thesis will also draw from Edward Snowden's own autobiography, *Permanent Record*, as well as the documentary released in the year 2014 entitled *Citizenfour*, directed by Laura Poitras, which provides first-person interviews with Snowden regarding his decision to release all of the documentation on the NSA he found during his tenure there. Additionally, I will be looking at other writings by Snowden in the time since his leaks were released, and I will be sourcing those in this thesis.

Chapter Three: Who is Edward Snowden, and How Did He Become a Whistleblower?

This chapter will provide insight into Edward Snowden's background. This information will be coupled with his perspectives and reasonings on why he chose to become a whistleblower against one of the most secretive agencies in the world, the National Security Agency, and how he views his actions to have helped unveil some of the mystery linked to the day-to-day operations of the United States Government's security organisations and the impacts of these organisations upon the average individual's privacy all in the name of safety and security of the very people they supposedly represent.

Edward Snowden was born on the twenty-first of June, 1983, in the small city of Elizabeth City, North Carolina (Ray, *Edward*, n.d.). His family moved to central Maryland during his childhood, relocating not far from the Fort Meade headquarters of the NSA, for his father Lonnie's position with the FBI following his work with the Coast Guard. His mother, Elizabeth, worked as a clerk in the United States District Court for the District of Maryland. Additionally, his sister, Jessica, worked as a lawyer at the Federal Judicial Center in Washington, D.C. His studies were heavily interrupted, as he dropped out of high school due to a difficult case of mononucleosis, eventually attained a GED, and intermittently studied at Anne Arundel Community College from 1999 until 2005, without earning a degree. He did go on to earn an online Master's degree from the University of Liverpool in 2011. In May 2004, he enlisted in the army reserve, but was discharged after only four months due to bilateral tibial stress fractures. By 2005, he began working in security, finding a job at the University of Maryland as a security guard in a research facility that closely worked with the NSA. The following year, he was hired by the Central Intelligence Agency (hereinafter: CIA), as he proved to have an aptitude for computer programming; this led to his attaining top secret clearance levels and an eventual posting to Geneva, Switzerland, in 2007, as a network security technician. By 2009, he left the CIA and chose to work for the NSA as a private contractor, working also for corporations such as Booz Allen Hamilton, a consulting firm, and Dell (Ray, *Edward*, n.d.). In an interview in 2014 with James Bamford, Snowden said that the position with the University of Maryland required a polygraph test, which led to his eventual hiring by the CIA (Bamford, 2014). We can see here that the lax requirements for hiring and security clearance

began from the beginning of Snowden's work with the CIA, raising alarms for their security requirements in general.

As Bryan Buchler wrote, Snowden's entire nuclear family was employed within the federal government and he was fully expected as a child to follow the same path (Buchler, 2016). Throughout Snowden's early personal and professional life, he seemed to be very supportive of the United States Government and the actions of the CIA and other similar organisations particularly with regards to national safety and security. In 2009, in chat logs, Snowden used the alias "TheTrueHOOHA", where he referred to leaked documents involving the US rejecting aid for an Israeli raid on Iranian nuclear site, stating that leakers of classified documents should be shot (Mullin, 2013). However, in 2008, Snowden apparently witnessed a scenario in which the CIA attempted to recruit a Swiss banker to obtain secret banking information. In order to get him to comply, Snowden describes CIA members purposefully getting the banker intoxicated and encouraging him to drive home, after which he would later be arrested for drunk driving and offered a deal in which the charge would be suppressed if he complied. This would be the start of Snowden's disenchantment with the actions of the inner workings of secret governmental organisations, stating "Most of what I saw in Geneva really disillusioned me about how my government functions and what its impact is in the world… I realised that I was part of something that was doing far more harm than good" (Greenwald, 2013). This growing sentiment became a critical component as to his reasoning of why he chose to reveal secrets to journalists in 2013, as he viewed the actions of the government's wide-sweeping surveillance as unacceptable and even immoral and illegal and not something that should be simply swept under the rug as the CIA had been doing with the banker in Switzerland. Snowden began to drastically change following these events, as this was the first time in which Snowden saw members of a governmental agency setting up a private citizen for their own gain at the citizen's expense through purposeful and intentional deceit.

In 2011, Snowden took a trip to New Delhi, India, where he enrolled himself in a professional school just down the road from the United States Embassy, where he was going to work for a short business trip (Harris, 2014). This school focused on computer hacking and programming skills, where Snowden trained with a private instructor in ethical hacking. Ethical hacking is a technique where the user works to exploit flaws in the computer's software to access the computer itself. Of course, those who learn to ethically hack are therefore typically skilled

hackers in general, as the same skill sets are needed for both traditional and ethical hacking. While on the trip, Snowden did not disclose his plans to his bosses at the NSA, choosing to self-pay for the expenses of the course he chose to take. However, his clearance for top-secret security and documents was in the process of being renewed, and investigators into Snowden following his leaks remain shocked that they did not inquire further into his international travels or with whom he interacted outside of the United States, which is a traditional practice when renewing security clearance for a job of this calibre. Continuously, his background check at this time has been labelled as incomplete and tremendously flawed, which is very evident in its blatant lack of clear checks. At this time, he was working with Dell as a technology specialist, specifically located at an NSA facility in Japan, so his trip to New Delhi also corresponded with a time that he was travelling to the United States Embassy there to work on surveillance equipment, which could conceivably explain why the NSA chose to not further investigate his time in India (Harris, 2014). However, the blatant lack of follow-up in regards to his international travels demonstrates a clear lack of proper follow through on the behalf of the NSA in terms of proper clearance and background checks.

By March 2012, he began working at the Oahu, Hawaii, office of the NSA, named the Kunia Regional Security Operations Center (Binder, 2020). His original assignment was to find and stop any attempts at Chinese hacking aimed toward the United States Government's operations. However, while working in this position, he began collecting the classified documentation on secret surveillance programs that seemed to overstep the privacy of American citizens in scope.

Finally, in May 2013, just weeks before the Snowden documents were revealed to the public, he put in a request for a medical leave of absence under the pretext of receiving further medical treatment for his epilepsy, which he was diagnosed with in 2011 (Ray, *Edward*, n.d.). Instead, he flew to Hong Kong. There, he was able to participate in multiple interviews with *The Guardian*, which produced much footage for the 2014 documentary, *Citizenfour*, his anonymous pen name while submitting documents to reporters.

During the 2013 interviews, Snowden clearly discussed his reasonings behind his disclosure: he did not aspire to become an important topic in the news cycle, but rather wished to disclose what the government was doing under the average person's eye without their knowledge (Greenwald, 2013). He also chose to not maintain anonymity because he "know[s] [I] have done nothing wrong", and thus has no reason to hide from his information sharing (Greenwald, 2013).

However, with the removal of the aspect of rose-coloured glasses tinting his view of the world, he points out that he knows "the government will demonise [him]", but still maintains his aspiration of revealing the "federation of secret law, unequal pardon, and irresistible executive powers that rule the world" (Greenwald, 2013). "It was at this time that Snowden first considered exposing classified information but he decided against this for two primary reasons. The first was that the secrets within his possession related to individuals and not computer systems. A leak would thus have potentially harmed other individuals and not exposed ethical concerns with relating to surveillance infrastructure. The second was his belief that the imminent election of Barack Obama might result in sweeping intelligence reforms— the opposite however occurred. Snowden subsequently resigned from the NSA due to his ethical qualms in February 2009" (Bamford, 2014).

Ultimately, Snowden believed that the NSA was repeatedly and continually violating the Constitutional rights of American citizens and that the agency and those working for it were committing felonies under a direct mandate from the White House (Davies, 2019). Snowden himself stated that "I'm not against national security, but we need to make sure that mass surveillance, indiscriminate surveillance, mandatory retention policies, are not being carried out. Because by definition, if you're collecting the communications of everyone, the majority of those impacted are going to be innocents, not the guilty" (Snowden, 2016). This demonstrates that Snowden himself, while understanding the need for some levels of surveillance to protect against acts of violence, strongly disagreed with the total surveillance to which the American people were unwittingly being subjected. Additionally, he abhorred the manipulation of everyday citizens for governmental gain.

During his time working for the CIA, he was required to pledge an oath of service in which Snowden swore to uphold the Constitution of the United States against all enemies from both foreign and domestic domains; this clearly led to an ethical conflict of interest as he viewed the constant collection of private data as a violation of the Constitution's Fourth Amendment (Davies, 2019). The Fourth Amendment reads 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" (U.S., n.d.).

In a glaringly apparent way, the Fourth Amendment protects private data, and thereby does not permit the unreasonable collection or searching of private data without a warrant, which is directly not what the NSA was doing with its information collection. Snowden summarises this position stating that “being a patriot doesn’t mean prioritising service to government above all else. Being a patriot means knowing when to protect your country, knowing when to protect your Constitution, knowing when to protect your countrymen, from the violations of and encroachments of adversaries. And those adversaries don’t have to be foreign countries” (Goodreads, n.d.). Clearly Edward Snowden saw his actions as patriotic rather than treasonous, believing instead the Constitution was written to protect Americans from the overreach of the government from private lives rather than permit ease of access.

As the United States Government would view his acts as a violation of the Espionage Act, which would mean that he would be named a traitor, he left the United States for Hong Kong and flew to Moscow, Russia, en route to Ecuador, under the guise of medical treatment (Davies, 2019). However, upon his arrival into Moscow, the United States Government cancelled his passport, rendering him incapable of leaving. Following this, Snowden spent forty days living in Moscow’s Sheremetyevo International Airport. While stranded, he was forced to apply to twenty-seven different nations for asylum status, of which every country excluding Russia rejected his application. Finally, he remained in Russia, where he is still living. He very begrudgingly remains in Russia, speaking openly of his distrust and dislike for the government, but he faces the possibility of extradition to the United States and life imprisonment if he were to leave the country. He remains critical of Russia, and consistently maintains his dedication to privacy, despite the Russian government requesting his files and data on the NSA. He has maintained that he has not shared any of the information with them.

To this day, Snowden is still called anti-American and Communist due to propaganda, despite his very blatant acts of patriotism and pro-American citizen sentiments of protecting the rights and data of private citizens. Snowden himself tweeted about these sentiments, stating that “every time i acknowledge someone to the left of dick cheney [sic] may have made a point, i—the guy hired by both the CIA *and* NSA—get accused of being a communist. like, really? the first question they ask on the polygraph is, on a scale of 9 to 10, how much do you love billionaires” (Snowden, E, 2022).

Snowden currently, as of early 2016, is the president of the Freedom of the Press Foundation, a nonprofit based in San Francisco which works to protect journalists from malware, hacking, and government surveillance (Greenberg, 2017). Additionally, he works at an unnamed IT company based in Russia (Kelley, 2021). He continues to give interviews, write articles, and give speeches on spyware, surveillance, whistleblowing, and his desire to come back to the United States as he stated in his interview with CBS on September 16, 2016 (CBS, 2016).

Chapter Four: Immediate Impacts upon Domestic Security

In the aftermath of the revelations of Edward Snowden, thousands of further articles were written by journalists and academics wondering what this all meant for national security. Additionally, journalists posed the question of what security in an increasingly technological world means for the average individual (MacAskill, 2013). At what point and to what extent can personal security suffer in the name of the protection of democracy?

One of the revealed secret programs of the NSA was the program entitled PRISM; this program worked to data-mine technological giants such as Facebook, Microsoft, Outlook, Google, and Apple, thereby permitting the NSA and the Federal Bureau of Investigation direct access to their servers, and thus, the information of their customers (Ray, *Edward*, n.d.). PRISM stands for the Planning Tool for Resource Integration, Synchronisation, and Management (Murse, 2019). Naturally, despite the evidence of the existence of PRISM, the United States Government claims that it does not have unfettered access to private data, but rather is only able to collect under PRISM data that is deemed permissible by the Foreign Intelligence Surveillance Court (Sottek, 2013). Additionally, the companies implicated by the PRISM data-mining adamantly denied any allegations that they knew about, or condoned, the data-mining into their servers, leading the American public to be unsure who was fully at fault. Further information regarding PRISM, and the Foreign Intelligence Surveillance Court, will be disclosed here.

PRISM was explained in the sixth of June revelations to be a streamlined source through which the government of the United States could find information through the ease of expedition of court-approved data collection requests (Sottek, 2013). This project came into existence during the Bush Administration, which instigated the start of the intensive spying on network traffic both abroad and in the United States following the terrorist attack on the United States on September 11, 2001. This means that the project would, hypothetically, create a more streamlined method through which the government may collect any data necessary on an individual who was seemingly participating in unsavoury or dangerous activities, and thus ensure the safety of individuals around them. The mechanism through which these court-approved requests were approved was the Foreign Intelligence Surveillance Court (About, n.d.). This Court was established under the 1978 Congressional Act entitled the Foreign Intelligence Surveillance Act. The Court is located in Washington, D.C., and is comprised of eleven federal district court judges. These district court

judges are designated for the position by the Chief Justice of the United States, serving a maximum of seven years in staggered sentences, thereby ensuring one Chief Justice cannot elect every member in an effort to keep the Court politically neutral. The Court's work involves the review of submissions by the United States Government in regards to decisions on physical searches, electronic surveillance, and any other required investigative procedures for foreign intelligence.

However, PRISM's activities, and the actions of the Foreign Intelligence Surveillance Court, existed entirely clandestinely until the publications of Snowden, causing more panic to arise. The clandestine nature of these NSA sectors indicated that the government was able to surveil anyone who was deemed suspicious without their knowledge. Even worse, the surveillance was permitted to the third level— the NSA was able to investigate people three levels of friendship away from a suspicious individual; this means that, for example, if you had the average number of friends on Facebook, which is one hundred ninety, the NSA would be able to investigate not only your friends' friends, but also the friends of your friends' friends, creating a web of over five million people who could be potentially investigated if someone were to be suspected of terror activity (MacAskill, 2013).

With this knowledge, naturally, public unrest regarding the activities of the NSA and PRISM grew, leading the NSA to attempt to reassure and calm the American people. The organisation claimed that it only collected data on a tiny proportion of the internet traffic in the world, stating that it was equivalent in size to a "dime on a basketball court" (MacAskill, 2013). However, in perspective, the Library of Congress, which is one of the largest library collections in the world, gathers over five terabytes of data in a single month. The NSA collects much more than that, indicating that their so-called "dime on a basketball court" is a much larger mark than what they attempt to downplay it as (MacAskill, 2013).

Most importantly, Americans knew that the PRISM program was not the first of its kind, but rather the latest iteration of the NSA's plan to collect data on potential attacks— in 2005, the New York Times published an article revealing the efforts of the NSA to collect personal user data, as a former technician at AT&T, one of the largest phone networks in the US, revealed that AT&T had permitted the NSA to install a computer in the switching centre location where fibre optic cables entered the US, meaning that they were able to monitor not only user data in the US, but also incoming data from other countries (Braun, 2013). This was part of a post-9/11 monitoring system

introduced under the Bush Administration, which permitted the surveillance of internet user data in an attempt to weed out individual potential terrorists or terror cells. However, the traffic through the cables proved to be difficult to discern the source, meaning that the NSA would be wasting valuable time on processing the data of those who would not be a threat to the US's internal security, or even have anything remotely connected to the US, as the cables do not solely process the data of American citizens and residents. In addition to the installation at AT&T, the Federal Bureau of Investigation (hereinafter: FBI) began showing up at Microsoft headquarters with a much greater frequency, with court orders for user information in tow. This became so frequent that Microsoft employees began calling it "Hoovering", named such after J. Edgar Hoover, the first director of the FBI, who instigated a widespread information gathering program on innumerable numbers of American citizens (Braun, 2013).

This 2005 installation at AT&T was permissible under the purview of the 2001 Patriot Act, which sought to allow direct and more lenient access to law enforcement for surveillance; this expansion would permit the use of surveillance in an attempt to prevent crimes of the nature of terrorism (USA, n.d.). The Patriot Act was ratified shortly after the September Eleventh, 2001 terror attacks by President George W. Bush; the Act passed through Congress easily with a Senate vote of 98-1 and a House of Representatives vote of 357-66, demonstrating an untraditional bipartisan agreement for an act of legislation following the tragedy. Commenting about the Act, now-President Joe Biden highlighted that "the FBI could get a wiretap to investigate the mafia, but they could not get one to investigate terrorists. To put it bluntly, that was crazy! What's good for the mob should be good for terrorists" in the Congressional Record on the twenty-fifth of October, 2001, highlighting a clear disconnect between the ease through which terror and mafia or gang activity could be monitored and avoided within the United States (USA, n.d.). This shift was in direct relation to the fact that foreign terrorists were now coming and attacking the United States, which was a contrast to the former home-grown terror that was occurring before, which demonstrated a shift in the needs of the FBI as this created a new realm of possible illegal activities against the United States within the borders.

Furthermore, the Patriot Act permitted investigations by law enforcement without the knowledge of the person being investigated; this was legalised so that the criminals or terrorists would be unable or hard-pressed to destroy evidence or flee from the area and thereby prevent arrest or prosecution (USA, n.d.). This is a clear demonstration of the direct link from the Patriot Act to

the founding of PRISM, as both the Act and the organisation sought to reveal information on future attacks and prevent any harm to United States citizens. While a meaningful goal, one must understand that the Act and the organisation directly permitted the violation of the personal privacy that was formerly believed to exist by American citizens, and the revelations by Snowden brought this to the forefront of the minds of the average American's thinking; never before had they thought of themselves as being suspect.

This post-9/11 monitoring laid the groundwork for the the development of PRISM, as the concepts were very similar (Braun, 2013). However, PRISM improved upon the original work of the Bush Administration under the so-called "Terrorist Surveillance Program" by permitting the creation of a much more secretive information gathering system, thereby circumventing the need for computers installed at corporations. Even with the 2005 revelations, the American public's debate on what type of spying on a government's citizens is permissible for the government was reignited with a fury. With the knowledge that the formerly-known espionage was continuing in the shadows, without anyone's knowledge, Americans became much more upset than they were with the Bush Administration espionage work as their data was freely processed both unfettered and unknown to the civilians by the NSA.

Despite all of the evidence pointing to a corrupted ploy by the United States Government to routinely spy upon its citizens and residents, it is important to note that the Congress itself was unaware of the creation of PRISM (Lee, 2013). This was achieved under the Bush Administration, where the Congress passed the Protect America Act in 2007. When presented to Congress, the Protect America Act (hereinafter: PAA) was explicated as a way to close any gaps in the current American surveillance capabilities. Instead, it was a stopgap designed to circumvent the ruling by the elusive Foreign Intelligence Surveillance Court which reportedly ruled that the government's actions of intercepting two foreign endpoints' communication streams was illegal, even if the information passed through the United States' internet connection. This led to a general panic within the NSA that the United States might lose its full capacity to protect against terror and surveil the activities of terrorists potentially moving against the country; as such, the PAA was pushed through Congress within only a few days of debate. This quick legislative process was heavily linked to the strong emotional connections Congressmen felt from the aftermath of September Eleventh, thereby making the process of passing the PAA that much easier.

Despite this belief, the PAA in reality created a drastic change in surveillance law in the United States: the PAA granted the ability to the NSA to indiscriminately surveil communications through a sweeping "certification" which claimed security concerns related to an incident may be subject to review (Lee, 2013). With this in mind, it seems apparent that it would be prudent for the NSA and the United States Government to claim the need for indiscriminate access to any and all American private communications, as would be permitted under a sweeping certification. Naturally, this is what they chose to do, which ultimately allowed the organisations to track and save every communication from the leading online service networks in the United States, including Microsoft, Verizon, and AT&T. Exactly six years after the induction of Microsoft as the NSA's unwitting first partner under PRISM, *The Washington Post* released Snowden's files.

In regards to the ontological security of individuals in the United States, these programs represented a direct derogation from the legal principle which dictates that individuals are innocent until proven guilty. This principle dictates that a defendant must not be improperly believed to be guilty until his or her guilt is proven in a court of law; by permitting the NSA and other organisations to indiscriminately spy upon American citizens without their knowledge, coupled with the investigations conducted against those of whom law enforcement officials have no real suspicion of criminal activity, potentially creates an environment where the United States Government is inherently distrusting its citizens without granting them the ability to defend themselves or become aware of this surveillance. As such, Snowden's leaks permitted the average citizen to become informed and take precautions against their private documents being accessed through document management.

Resulting from these leaks, the Government Accountability Project (hereinafter: GAP), originally founded in 1977, was reinvigorated, creating a challenge to the United States Government and any officials who chose to disparage Snowden's actions by calling him a traitor (Five, 2019). The Government Accountability Project and its impacts on domestic security will be further analysed in a later chapter, as it demonstrates a pertinent long-term effect of the Snowden leaks. Additionally, the National Whistleblowers Center (hereinafter: NWC), founded in 1988, will also be discussed later, alongside the GAP. The NWC also experienced a resurgence in growth and expansion following Snowden's leaks, expanding their services and activities further globally to account for the expanding number of whistleblowers who need support as well as the growing number of whistleblower protections legislations in the process of being passed around the world

which required the support and litigious knowledge of the organisation. “The first high-impact case that the NWC supported challenged an industry-wide practice of coercing employees to sign non-disclosure agreements prohibiting them from raising safety concerns to federal regulators. The precedents set were groundbreaking,” (*Mission*, 2021). This organisation has remained a tax-exempt, nonpartisan organisation, advocating for the rights of whistleblowers around the world, based in Washington, D.C. More on their work and advocacy will be discussed later.

Chapter Five: The Snowden Effect

The Snowden Effect is defined as the increase of the general public's concern toward privacy and information security (What, 2015). This increase is directly linked to the 2013 release of Snowden's documents, meaning that Americans were more interested in the government's invasion of what was commonly perceived to be personal privacy with only specific exceptions. This effect also directly impacted the belief in the actual security of cloud storage systems in a heavily negative way, leading to 2014 poll with almost ninety percent of respondents stating that they were choosing to either alter or cease cloud storage use or purchasing solely based upon the information leaked by Edward Snowden. The commonly-perceived reputation of cloud storage services as incredibly secure was heavily reduced, a fact clearly demonstrated by the high numbers of respondents who chose to change their storage methods. This impact was so large that cloud services faced an eleven percent reduction in the rate of revenues between Q3 2013 and Q4 2014, with an estimated loss of eighteen billion USD (Song, 2017).

It is important to note something that Edward Snowden discussed within his autobiography: "Over 90 percent of the world's Internet traffic passes through technologies developed, owned, and/or operated by the American government and American businesses, most of which are physically located on American territory" (Snowden, 2019). With this in mind, the sweeping observations permitted under the PAA allowed for almost the entirety of Internet traffic to be tracked and analysed by the NSA. The immediate impacts of the Snowden leaks were seen by United States businesses in reaction to the National Cyber Leading Small Group (hereinafter: NCLSG), an initiative created and chaired by Chinese President Xi Jinping in February 2014 (Binder, 2020). These impacts will be further discussed in this chapter.

The NCLSG was a direct response to the year 2000 creation of the so-called Chinese Great Firewall, which is widely regarded as the first bifurcation in the openness of the once-global and open internet (Binder, 2020). The Great Firewall created censorship applications for sites such as Google, *The New York Times*, Facebook, and other social medias, causing a block of information from outside China into the nation. The Great Firewall was supported and kept up to date by eight corporations whose equipment was created in the United States: Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm were the backbone of not only the Great Firewall, but also many of the Chinese cyber systems. Together, these eight corporations were regarded as the "Eight

Guardian Warriors"; however, with the 2013 Snowden leaks, a "de-Cisco campaign" was conducted internally in China, which called for the removal and replacement of Cisco technologies and systems creating China's internet network. This rallying cry was repeated by not only government officials, but also users across China's internal social media networks, such as WeChat and Weibo.

As a direct result, Cisco, a company which produces components for internet connection, including router boxes and cables, noted an eighteen percent drop in orders originating from China; this accounted for ten percent of their quarterly revenue within one quarter, as reported in November 2013 (Binder, 2020). In the same month, Microsoft announced a slowing in revenue; IBM also reported a twenty-two percent revenue drop from previous quarters in Chinese revenue. Most impacted, however, was Qualcomm, as forty-two percent of their sales came from China, meaning that the company was not only impacted by the punitive measures of the Chinese Government's shift in internet strategies but also by the loss of business from individuals and companies within the United States who held other cybersecurity concerns due to Snowden's leaks directly.

Chapter Six: Long-term Effects on Domestic Security in the United States

In the days following the release of the Snowden documents, American citizens felt strong concern toward their data security, as demonstrated in the previous chapter's mention of the poll regarding cloud storage usage and its reduction (Song, 2017). The demonstration by the United States Government that they would investigate even those who have no ties to or desire to commit criminal activity created divisions amongst Americans, who had different opinions on the acceptability of Snowden's actions as well as their view toward the government itself (Geiger, 2018). The leaks created divisions amongst those who viewed them as helpful to the general public's interest, as well as between those who became more disapproving toward the actions of the United States Government in their efforts to surveil every individual.

Three years on, when interviewed, Snowden highlighted that he did not leak the information in an attempt to change American society (Hattem, 2016). His goal was not to be the reason why society changed, in that he would not force society to change through his leaks, but rather as an attempt to be the reason that society wanted to change its actions. Most importantly, we must consider the reasons for which Snowden chose to become a whistleblower, and why he could not realistically be considered a spy; a mnemonic from the Soviet era, MICE, is often used in reference to the reasons for which individuals can become exploited and therefore become spies for foreign governments (Smith, 2021). MICE stands for money, ideology, coercion or compromise, and ego. In terms of money, Snowden has not become any wealthier, with a net worth of approximately the same as when he originally became a whistleblower. In terms of ideology, while Snowden was displeased with the actions of the United States Government, he still maintains that he has respect for the country, but simply did not find the actions of the NSA to be tenable. Clearly, despite his actions, he was not acting due to radicalisation. Snowden does not appear to be a victim of coercion or compromise, as he actively mentions that he destroyed the files before he left Hong Kong so that no foreign government could gain access to them once they were leaked, therefore one could assume that he was not being coerced by a foreign agency to gain access to confidential documents for the benefit of a foreign nation. Arguably, one could say that he felt that he was superior to other NSA agents and therefore his ego was the reason that he became a whistleblower, but one could also argue that he believed in the good of the American people over allowing the bad actions of the NSA organisation to continue, thereby negating the idea of ego.

One remarkable impact of the Snowden leaks is the impressionable difference in Hollywood movies: while the idea of a “Big Brother” state permeated movies and literature as a direct result from the Cold War era, the leaks once again made this semi-dystopian theme once again popular (Hattem, 2016). Dramatised versions of Snowden’s work became box office hits alongside two of his documentaries, demonstrating a newfound admiration for the dystopian themes within American media consumption. This, coupled with the already-pervasive distrust of American technology companies, meant that the companies were poised to lose billions of dollars solely based upon the actions of Edward Snowden.

The most overwhelming difference in domestic security in the United States following the Snowden leaks was the changes to the Patriot Act originally passed by the Bush Administration. Under the Obama Administration, the USA Freedom Act was passed as an alteration and a continuation to the securities protections allowed under the original Patriot Act (Eddington, 2019). This Act changed what type of cell phone data was permitted to be collected by the NSA, but resulted in even more data being collected. This will be further discussed in the next chapter, as it directly affects the ability of the cell phone carriers in the United States to promise data privacy and security to their customers, as is possible with other major corporations that are commonly used by Americans on a daily basis.

This next chapter will examine more in-depth examples of how the impacts of the Snowden leaks affected change in major corporations, and what their responses were in terms of privacy policy.

Chapter Seven: An Examination of Corporate Review of Privacy Policy

Most critically, corporations began realising their immediate need to respond and react to the very evident security concerns that became more transparent due to Snowden's revelations. As such, and especially in conjunction with events that occurred in the United States in the years following the leaks, corporations began taking much more active stances toward how they approached the government's desire to review and analyse personal data. This chapter will specifically examine the cases of the San Bernardino gunman's found iPhone, which was a very critical case in which the reasoning behind the shooter's motives were completely unknown, but his iPhone was found at the scene of the crime, and Apple was requested by the Federal Bureau of Investigation to create a key to unlock the iPhone. Additionally, this chapter will also analyse a much more recent case of menstrual cycle tracking applications, which are detrimentally selling information that could be used to prosecute women following the overturning of *Roe versus Wade* in 2022. In contrast to the positive attempts at corporations to provide data security to users, this chapter will also highlight the infamous case of Facebook selling and permitting access to private data.

As mentioned in the introduction of this chapter, this chapter will first discuss the San Bernardino gunman's iPhone, and the dilemma of the United States Government and Apple in terms of when a corporation is required to create new methods of accessing private data. This famous dispute, in which Apple refused to provide a "back door" to the Federal Bureau of Investigation, was a request in which a system would be created to essentially allow the organisation to access the terrorist's iPhone through a software that did not exist, allowing them to circumvent security put in place by Apple to protect their personal data (Cook, 2016). The San Bernardino case was an instance in which fourteen people were shot by a married couple at a holiday party in San Bernardino, California. One of the shooter's iPhones was found, and the FBI wanted the aforementioned "back door" key software from Apple for this iPhone to determine a reason why the shooters did what they did. While of course the company was taking this stance because of their famous privacy protection beliefs, it also chose this moment to publish this cited message as it was a very important moment in history for corporations and information security due to the impact of Edward Snowden. This gave Apple, especially as one of the potentially implicated companies in the CIA's crusade to track any potential terror incidences, the opportunity to demonstrate their dedication to personal privacy and information. Ben Wizner, Edward Snowden's lawyer, who works at the American Civil Liberties Union, spoke on this case in particular, stating that "earlier this year,

Apple refused to cooperate when the FBI sought access to the iPhone of one of the killers behind last December's terrorist massacre of San Bernardino, Calif. It seems unlikely that Apple would have taken such a firm stand, and fought so hard in court, if the Snowden leaks hadn't happened. The fact that the most profitable corporation in the world was engaged in a high-profile public dispute with the FBI in a terrorism case is something that would've been unimaginable a few years ago," (Hattem, 2016). Of course, this demonstrates an issue— at what point is collecting data too much or too little in the name of safety and security, but also in the name of personal privacy? One cannot stop something like this shooting from happening without having hard evidence of it having been planned for a specific day, which of course requires the collection of private data. However, one is entitled to private data. The line where the data is ensured to be private is a very difficult line to clearly define.

Despite this very blatant public display by American corporations and the general American public toward the idea of the privatisation of information, and the removal of the government's complete access from personal data, Snowden's revelations had little effect on legislation to change any of the privacy issues evoked by the NSA's data collection. In fact, in 2015, the USA Freedom Act was signed into law under the Obama Administration, thereby continuing the surveillance program that was previously deemed to be unsuccessful by every review source, including the Privacy and Civil Liberties Oversight Board's review of the NSA program (Eddington, 2019). Shockingly, even with the general disapproval of data collection, nearly three times more telephone data was collected by the NSA than before the enactment of the USA Freedom Act in 2015, essentially demonstrating a complete ignorance toward the American public and their stance on the matter.

However, one major change of the Freedom Act is that it does not permit the indiscriminate collection of data from phone calls, specifically the ability to listen to the call's contents without just cause, but rather it permits the collection of simply the data of which number is calling to which number and at what time, thereby severely limiting the original scope of the Patriot Act's permissions to collect the information of phone calls (Bradford, 2019). In some ways, we can see that the Snowden leaks did in fact alter the collection of phone data from American citizens, but we can also see that the USA Freedom Act still permits the government to maintain a similar level of surveillance on those who use any phone within the United States' networks without any problem, thereby maintaining access to tracking data as before. This directly affected the cell phone carriers

in the United States, as it still did not permit them to promise customers the same protections that other corporations in the United States were extending to their consumers in terms of data privacy for their communications and devices.

As quickly as possible following the Snowden leaks, companies and corporations sought to regain the trust and also user base from consumers. As previously mentioned in the example with Apple, many corporations found very public displays in order to demonstrate their loyalty to their customers and their willingness to protect private data. Within the first year following the leaks, companies nearly unanimously implemented mechanisms of encryption meant to protect the user from data breaches (Whittaker, 2018). What we take for granted now in terms of personal security on our private devices became a novelty and then standard across different apps and software, with companies implementing end-to-end encryption in messaging services, coupled with full-disk encryption for the actual device's software, which nearly completely protects the user from the government accessing the contents of the device freely. In line with the earlier information shared on the San Bernardino gunman's iPhone, Apple became the first company to pioneer this level of data protection across its devices in the name of user protection.

From this effort to demonstrate customer loyalty stemmed the transparency report, issued by companies that revealed just how much data was requested by the government each year, and how much data the company comparatively turned over. The report was started by Google, as the NSA began having to show up to the companies' front doors with legal orders for information, as they could no longer simply just listen in as they had been doing before (Whittaker, 2018). In 2012, Twitter followed in Google's footsteps with their own transparency report, and many other corporations began to follow suit in the years following to quell any mass concerns that the companies were choosing to be complicit and handing over bulk data to the government at their request. Over time, even cell service companies began releasing this data, as well, interestingly. This provided a unique look into what corporations and the government do behind the scenes with user data, and especially provided a view into the legal demands the government often issued now that they were required to be more upfront with their data research into private citizens (Whittaker, 2018). While the Snowden leaks did not provide overwhelming government reform in the realm of data privacy and security, they did provide remarkable changes in how corporations chose to be more transparent with consumers in disclosing when the government requests access to data, as well as providing much more secure servers for the data to be stored and shared for the users themselves.

As an added benefit of the corporate securitisation, the NSA and other government organisations had to drastically alter their methods of data research into individuals, which of course did cause hindrance to their research and data tracking of individuals throughout the years of updating their processes.

On the other hand, an example of a corporation exhibiting the opposite behaviour in terms of personal data security and privacy for its users was heavily exhibited in the instance of Facebook. In 2018, Mark Zuckerberg testified in front of the United States Congress regarding Facebook's stance on data collection and what the company does with the information they gather on their users following the issues the company faced with privacy during the 2016 election cycle (Watson, 2018). Traditionally, when someone shares something on Facebook, they are given the option to choose with whom the information is shared— for example, the post could be shared to only themselves, to their friends, or to the general public. This very simple privacy selection model allows the user to interact with and share their posts and profile with a curated audience which can either be very limited or completely open. It would seem that, with a model such as this, that the user has relatively strong coverage over who has access to what data they share. However, this does not reflect the true reality of what happens with user information on the platform. What truly happens is that Facebook, along with most other websites, tracks users' posts, comments, likes, activity, and interests.

Much like with how Snowden revealed that the NSA was tracking individuals through their cell phone usage, this means that the social media applications that many individuals use (especially considering that Facebook owns Instagram as well) were also tracking their usage and creating an algorithm to target advertisements to each particular user based on the advertiser's preferences (Watson, 2018). While Facebook does not explicitly sell data to advertisers, the ability for an advertiser to have Facebook curate their advertising base is a concerning use of the stored data and information on users that Facebook does already maintain. However, the issues of 2018 and Facebook's data security run much deeper than curated advertisements, which caused major issues in both trust and financial loss for the corporation in a shocking revelation. Primarily, Facebook became the source of a hotbed of anger and distrust over the year 2018 due to issues of data privacy, pervasive fake news, and Russian meddling on the site. Despite Mark Zuckerberg apologising and the company working toward remedying the issues, the website was found to have continued with these issues, which led to Zuckerberg's testifying in front of Congress. In December 2018, it was

reported that Facebook permitted companies, such as Netflix and Spotify, to read their users' private messages (Stewart, 2018). This, compounded with the already-known issue, with the information released in March 2018, of Facebook sharing information of approximately eighty-seven million users to the political consulting firm known as Cambridge Analytica, created an atmosphere of strong distrust and upset toward the social media site.

Furthermore, the data breaches of Facebook led to an investigation into the website by the Federal Trade Commission, as Facebook had signed a consent order regarding the handling of users' private data in 2011 (Stewart, 2018). Overall, this led to a more than twenty percent decline in stock valuation of Facebook in 2018. Zuckerberg himself lost an estimated fifteen billion USD. The founders of WhatsApp and Instagram, both subsidiary companies purchased by the Facebook Group, resigned, despite the fact that these two companies are some of the Group's most popular products. Unsurprisingly, this is one of the worst examples of data security breaches in a corporation since the Snowden leaks, and the company handled it quite poorly, leading to a significant amount of backlash and public upset over how their information was handled.

Much of the information regarding Facebook was released by Frances Haugen, a data engineer and scientist who worked for Facebook as a project manager who disclosed tens of thousands of Facebook's internal documents to the Securities and Exchange Commission in 2021. According to her the files show that Facebook leaders and managers have consistently throughout recent years put "the companies image and profitability ahead of the public good — even at the risk of violence and harm" (Chappell, 2021). There has been much response and discussion revolving around these documents ranging from the events of the January sixth, 2021 insurrection to fear of enforcing rules for high profile accounts. Facebook, like every other social media site, uses a strategy in which a user's activity will be curated to them in order to increase time spent on each respective platform. This means that if a user consistently spends time on, comments on, or likes posts which follow specific ideas that they will in turn see more posts which promote that idea. In regards to the so-called "Storm of the Capitol" on January sixth, many Facebook employees were shown to have stated on internal message boards that they had "been feeling the fire for a long time and we shouldn't be surprised it's now out of control" and "we did too little too late" (Chappell, 2021).

While Facebook did admittedly work towards limiting misinformation, too much was allowed to spread publicly before this limitation could make any meaningful impact (Gallagher, *Facebook*, 2021). Additionally, even with the intent to limit this misinformation; new profiles, groups, or chat rooms could be made again following a ban or a restriction. This was also a similar issue that Facebook experienced with the height of the COVID-19 pandemic, with posts promoting vaccine skepticism and COVID denial originally being rampant and promoted to many users, but eventually being limited when it was too late.

These actions of Facebook show a rampant apathy when it comes to using the data of its users for the good. Rather they, at least according to Haugen, would rather put profits and public image over the public health when it came to the COVID-19 pandemic and the health of democracy when it came to the January sixth insurrection.

A more recent instance of personal privacy and the issues the general American public face with its violation is in the aftermath of the landmark overturning of the decision of *Roe versus Wade* by the United States Supreme Court on the twenty-fourth of June, 2022 (*Roe*, 2022). In the weeks leading up to the final decision, a whistleblower leaked the Supreme Court's Initial Draft penned by Justice Alito indicating their intent to overturn the court ruling (Gerstein, 2022). With this early release of information, people were able to begin organising protests and also prepare for the immediate effects of the ruling once it became enacted, especially in states where abortion would become illegal.

One immediate dilemma became hotly debated: a popular tool for women is menstrual cycle applications, which are typically free-to-download apps that allow the user to track fertility and reminds them of upcoming periods (Korn, 2022). However, many individuals are being faced with the dilemma that they may have to delete these apps in order to protect their own privacy, especially in the case where they became pregnant and needed to seek out an abortion, as the states where abortion is becoming illegal intend to prosecute both healthcare providers who grant the procedure as well as women who receive abortions.

This concern of prosecution is not solely circumstantial; there are cases in which women have been prosecuted with charges related to termination of their pregnancies (Zakrzewski, 2022). A pill used for abortions, Misoprostol, was researched and purchased by a woman in Mississippi,

but there was no evidence she actually took the pill. She was prosecuted with murder, with her search history used as evidence against her in the trial. She was found not guilty, with the grand jury in March 2020 giving a ruling of "no billing", meaning that all charges against her were dropped (*Victory*, 2020). However, this demonstrates very evidently the fact that simple Google searches and data on one's phone can be used to prosecute and punish those who wish to maintain bodily autonomy in states where abortion is becoming, or is already, illegal, thanks to the overturning of *Roe versus Wade*.

In regards to the cycle tracking apps, women fear that these apps, as the apps themselves know when the users' cycles are delayed, would be able to be used as evidence of their obtaining an abortion in another state, and therefore be used to prosecute them in these instances. While the user would not report the abortion in the app itself, the phone itself would be used as evidence, as the phone would be able to supply the location history of the user regardless of the application's data (Korn, 2022). As such, many of these apps are introducing anonymous modes, where the user may register for the app without providing any data such as the user's name, email, or date of birth, in an attempt to provide security for these users. Even Google itself is promising to offload tracking data and location history records that show whenever a user was at either an abortion clinic or a fertility centre; the issue lies in the question of how quickly and how accurately the data will be deleted from their servers. Additionally, even outside of these apps and Google location services, one must consider that the user's smartphone itself contains enough biographical and tracking information that the user and the data could easily be matched up if the person who wished to prosecute the supposed offender were motivated enough, thereby making the smartphone itself enough of a weapon even without the requirement of registration for these apps.

On an even grander scale, Snowden warns of the fragility of computer security, and the ease of which it could be undermined, in an article on *The Irish Times* (Snowden, *Edward*, 2019). The article details how encryption, and its removal, would be incredibly detrimental to the security and privacy of our computers. Specifically, in late 2019, the United States, Australia, and the United Kingdom requested that Facebook create a "backdoor", which would work similarly to the one for the San Bernardino gunman's iPhone in that anyone with access to the "backdoor" could access the system without any problems, thereby allowing the governments and their police forces unfettered access to the encrypted messaging apps under the Facebook umbrella. If Facebook were to unencrypt their web traffic, anyone would be able to steal a copy of the data and record it, thereby

permitting them to use that data in whatever way they choose. However, if the data remains encrypted, only those with a decryption key are able to unlock the data, ensuring that it is much safer for the user. Approximately eighty percent of web traffic today is encrypted, which demonstrates the incredible level to which encrypted data is tremendously important in our online footprint (Snowden, *Edward*, 2019). While the idea of encryption is not explicitly limited to one specific company (aside from the specific example of Facebook), it is a pervasive enough part of our internet presence that it must be taken into consideration as the governments of the three mentioned nations feel secure enough in their ability to request a key that would absolutely decimate any form of privacy we currently maintain on the internet.

In the documentary *Citizenfour*, Lavabit is discussed, as it is an encrypted email server used by Edward Snowden during the time of his leaked documents (Poitras, 2014). An email company owned by Ladar Levison, Lavabit capitalised on the idea of total data encryption and privacy for the user, boasting three hundred fifty thousand users at its height (Ackerman, 2013). However, following Snowden's leaks, Levison found himself as the target of FBI investigations, as the emails on the server sent by Edward Snowden would be critical evidence for the government if they were to be accessed, as the government was not entirely sure which documents Snowden sent to the media during his leaks, and therefore had to consider every piece of information he ever had access to during his employment as compromised unless they gained access to his account. Instead of complying, Levison chose to shutter the company, choosing this route instead as he felt that permitting the government to have access to his internal computers and his company would be a violation of the Constitution. For nearly three years following this event, Levison was barred from speaking about whom the attempted spying was aimed at, with threats of possible jail time if he were to reveal the target of the investigation (Zetter, 2016). In a twist, the government accidentally revealed the target when the case documents were published; on March fourth, 2016, the documents were posted to Pacer, which is a federal court system.

Levison had been fighting for years to gain access to transparency so that he would be able to finally disclose more details as to why he was forced to close his business (Ackerman, 2013). In December of the year previous, Levison filed a motion to have the court documents unsealed and unredacted, and ultimately vacate the nondisclosure agreement that disallowed him from speaking about the intended target of the FBI. The court denied the motion to unseal and to vacate, but they ordered the United States attorneys involved to rerelease all documents with everything unredacted

excluding the “identity of the email subscriber and the subscriber’s email address” (Ackerman, 2013). While this still did not permit Levison to speak about the intended information the government was seeking, the documents were rereleased. Interestingly enough, one of the emails on the document was released without redaction, therefore confirming the general public belief that Edward Snowden was the intended target, as the email was “Ed_Snowden@lavabit.com” (Ackerman, 2013). This put to rest any issues Levison may have faced with his company, and he reopened the email server in 2017.

Chapter Eight: Long-term Effects of Created Institutions (Such as the Government Accountability Project)

Directly resulting from the Snowden leaks, institutions were reinvigorated to provide a source for whistleblowers who needed support and protection during and after their whistleblowing activities; these organisations existed prior to Snowden, but gained much more interest in the public eye as Snowden's actions were more public and accessible through the internet. As previously mentioned in this thesis, the Government Accountability Project is an example of such an institution. The Government Accountability Project (hereinafter: GAP) operates as a non-profit organisation with a nonpartisan public interest law firm (Devine, 2015). This public interest law firm specifically works to maintain the protection of genuine whistleblowers; this includes the protection of individuals who choose to exercise their Constitutionally-protected right to free speech to whistleblow and challenge institutional illegality, such as the abuse of power or other problems which would fall under the domain of betrayal of the public's trust of the corporation, within their workplace. Additionally, the National Whistleblower Center (hereinafter: the NWC) will be discussed as it has been an organisation working for whistleblowers and their protections for over thirty years.

As is evident in the case of Snowden's whistleblowing, the laws written to protect such individuals often are more counterproductive than anything (Devine, 2015). This means that those who choose to whistleblow often face retaliatory treatment, such as demotion, termination from their job, and/or the prosecution as a traitor, as in the case of Edward Snowden. With the help of the GAP and other organisations like it, the whistleblower protection laws have been reviewed by the United States federal government, and attempts to close or eliminate entirely any loopholes have been made. Clearly, it is critical to ensure that whistleblowing laws entirely protect the individual, with no loopholes, or the results may be that their case against the institution or corporation, as well as their own individual protections, may be at risk. In addition to protections for the whistleblower themselves, these laws must also extend full protection to any witnesses, as they should not be subjected to harassment and other penalties based upon their relationship with the information shared by the whistleblower.

Outside of the GAP, whistleblowers are protected in the United States by the Occupational Safety and Health Administration (hereinafter: OSHA) (United, n.d.). OSHA works for employees to protect workers' rights, a mission that includes protections of more than twenty federal whistleblower statutes. This protection includes adverse reactions to whistleblowing such as workplace retaliation (including the demoting, disciplining, or firing of the employee, the denying of opportunities for promotions or overtime hours, or the reduction of the worker's hours or pay). Most critically, this protection also applies to temporary workers, meaning that anyone who would be witness to any activities that may lead to whistleblowing would be a recipient of protections against retaliation under OSHA. Aside from protections, OSHA also permits employees to file a whistleblower complaint with the organisation itself; the worker may also file a complaint of retaliatory behaviour against the employer in question, giving them access to multiple types of protections based upon the company's actions and the employee's needs.

The NWC is not a strictly an organisation based in the United States, but rather works to protect whistleblowers around the world (*About Us*, n.d.). Over the years in the United States, the NWC has been instrumental in lobbying Congress to pass bills such as the Dodd-Frank Act, the Sarbanes-Oxley Act, and the Whistleblower Protection Enhancement Act, which all focus on furthering the protections allowed for whistleblowers in the United States. Outside of the United States, the NWC launched a campaign ahead of the December twenty-first, 2021, deadline within the European Union to strengthen the then-current whistleblower laws, thereby demonstrating their dedication to the NWC initiative of increasing global advocacy.

However, a glaring issue still faced in the realm of whistleblowing is the overall ineffectiveness of what claims to be full protection under the legislation. As evidenced within this thesis, and of course this chapter in particular, those who choose to whistleblow will most likely still be subjected to punitive measures. While considered technically illegal under whistleblower protection legislation, the legislation has left too many glaring loopholes, and therefore possibilities, for corporations to exploit the law and gain the ability to fire or punish the employee at their discretion. This trend of whistleblowers struggling to gain recognition for the demonstrated ills of the company has been a trend for as long as corporations have existed; one of the most prominent examples of this in the 1920s were the Radium Girls, who worked to gain financial assistance from the factory at which they were employed due to the incredibly detrimental nature of radium (Vaughan, n.d.). These women will be further discussed in the next chapter.

In the case of Edward Snowden, the use of the Espionage Act allowed for the government to aspire to prosecute Snowden (as he would need to be either extradited or willingly return to the United States to formally stand trial) under its vague writings that have historically permitted the unconstitutional prosecution of individuals who should have been protected under the whistleblower protection legislation (Younger, 2021). Additionally, when speaking on the case of Edward Snowden, then-President Obama remarked that Snowden should return to the United States to face the charges of which he was accused in court (Radack, 2014). However, Snowden pointed out what Obama neglected to mention in regards to the Espionage Act in particular: if he were to return for prosecution, he would be denied the right to make his case in court, thereby entirely denying his Constitutional right to defend oneself in front of a jury of one's peers.

Naturally, this loophole, combined with the natural fear that people would face of the inability to defend oneself in court if they were to be whistleblowing against the government as in the case of Edward Snowden, can be used by corporations and government agencies to oppress those who would choose to come forward with information of unsafe or unsavoury practices within said corporations and government agencies (Younger, 2021). Individuals may fear financial ruin, legal troubles, and even corporate or governmental retaliation in the form of loss of position or being "blackballed" from working in their desired field again. This type of retribution has occurred over and over again and can drag on for months if not years, ruining the life of the whistleblower and their family. In the case of Edward Snowden, legal troubles could ensue in the form of being labelled a traitor and him spending years if not his life behind bars if he returns to the United States. This means that many other covert organisations such as PRISM could exist without our knowledge simply due to someone's inherent fear of speaking out, even in spite of these organisations and their work to benefit individuals such as these mentioned in this thesis.

Chapter Nine: The Impacts of Other Whistleblowers Upon American Society as Compared to Snowden

This chapter will research information on Julian Assange and Chelsea Manning, as these two individuals laid much of the modern-day groundwork for the idea of whistleblowing in society and in the United States Government. While Julian Assange is Australian, not American, his work with the founding of WikiLeaks in 2006 directly resulted in the sharing of confidential military documents onto the site by Chelsea Manning, who will also be discussed here (Ray, *Assange*, n.d.). Additionally, this chapter will discuss the case of Samuel Morison, the first person ever convicted using the Espionage Act, as this is the legislation under which the United States also seeks to prosecute Edward Snowden. Joshua Schulte, a recently convicted whistleblower and former CIA employee, will also be mentioned here. Another individual who impacted the NSA through whistleblowing, Thomas Drake, will be discussed, as his actions of whistleblowing most closely aligned with the actions of Snowden. The largest difference between Drake and Snowden's cases is that Drake was convicted under the Espionage Act and Snowden has yet to be tried under these similar charges. Finally, for historical context, this chapter will also discuss the Radium Girls, as these women were a historical example of whistleblowers who also fought to receive recognition for horrendous working conditions in the 1920s and suffered without any assistance.

Whistleblowers such as Julian Assange of WikiLeaks and Chelsea Manning of the United States Army, who worked together to release Manning's documents, have laid the groundwork for how their information is perceived by both the United States Government and the American people. Chelsea Manning released thousands of classified documents via WikiLeaks, including the names of specific individuals, working closely with Julian Assange to share these documents without any intervention from the United States Military, for whom Chelsea worked. "While working as an army intelligence analyst in Baghdad in 2010, Manning learned of violations of the U.S. Military's Rules of Engagement, as well as thousands of civilian deaths that were unreported and uninvestigated by the military….Manning uploaded to WikiLeaks more than 700,000 classified documents regarding the wars in Iraq and Afghanistan, as well as a video, dubbed "Collateral Murder," taken from a military helicopter. The gunsight video shows soldiers in a U.S. military helicopter shooting down suspected insurgents, who were in fact civilians" (Coliver, n.d.).

Within the leaked documents, Manning allowed for the individual names of people associated with the incidents to be included in the publications. This release of individuals' names created a massive safety concern for the said individuals. This is in direct contrast to Snowden's leaking of classified information as he purposefully chose to avoid the naming of specific individuals in order to maintain their security. Although the Manning and Snowden cases parallel in that both chose to leak classified documentation, this is where the connection begins and ends between the two. Chelsea Manning released documentation, with the help of Julian Assange, entire pieces of classified information, including names of individuals, whereas Snowden purposefully redacted names and chose to release information solely related to the blatant issues in surveillance oversteps by the United States Government, and omitted any information that may undermine security.

Despite revealing documents that were upsetting to the American people due to the graphic and callous nature of the military regarding human life, Manning received a thirty-five year prison sentence, which was commuted after two years served by President Barack Obama in January 2017 (Ray, *Chelsea*, n.d.). Interestingly, although the very blatant security concerns committed by Manning versus by Snowden, Snowden still has not received a pardon for his leaks, likely due to his continual residence outside of the United States and lack of standing trial.

The connection between Manning and Snowden is evident: even though the two did not associate or release documents pertaining to the same organisations, Manning's imprisonment highlights the United States Government's strong desire to keep information regarding their most secretive organisations and classified documents under wraps, even if the information directly violates the safety and security of citizens worldwide. Additionally, Manning was prosecuted and convicted by court-martial in the United States Military Court under the Espionage Act, similarly to the charges the United States Government wishes to prosecute Snowden under, twisting the whistleblower protections legislation by demonstrating a lack of protections for those who wish to demonstrate the truth of problematic behaviour within the United States military and its related organisations, leading to their prosecution as a spy regardless of their patriotic actions. Manning's prosecution under the provisions of the Espionage Act is the second time an individual has been found guilty under these statutes since the Act was enacted into law in 1917, with the first being the prosecution of Samuel Morison in 1985, who was (almost entirely similarly to Manning) a naval intelligence expert who shared classified documents to newspapers (Pilkington, 2013).

The Samuel Loring Morison case was tried in 1985 under two separate provisions of the Espionage Act (Vile, 2009). An article from Colman McCarthy, published in 1985, highlighted that "The Justice Department is saying that this prosecution is not an attack on the press. No one should believe it. This is the administration that has been regularly trying to dam the free flow of information from the government to the public. It has attacked the Freedom of Information Act. Government censors are now empowered to review before publication the writings of federal employees and former employees" (McCarthy, 1985). A former employee of the Suitland, Maryland location of the Naval Intelligence Support Center, Morison routinely viewed and had access to classified information; for this reason, he was required to sign a nondisclosure agreement upon his hiring (Vile, 2009). However, Morison was found to have sent top secret photos of Russian ships to a news publication called *Jane's Fighting Ships*, which is a publication that works to assess global military strength. In turn, the publication printed the photos. During the trial, Morison argued that the prosecution was a violation of his First Amendment rights, as he was guaranteed freedom of the press under that Amendment. Additionally, he leaked the photos to a news outlet, rather than a foreign government, which is more akin to a press leak, rather than espionage for the sake of benefitting a foreign government.

Specifically, the two sections of the Espionage Act under which Morison was being prosecuted were sections (d) and (e). Section (d) covers specifically the transmission of information to foreign governments; section (e) discusses the sharing of information to others outside of foreign governments, which includes the press (Vile, 2009). While the rights of the First Amendment are very clear in their respect of the freedom of the press, the precedent set by prior court cases *United States versus Marchetti* (1972) and *Snepp versus United States* (1980), whose decisions are not pertinent enough to discuss in depth, but whose precedents are important enough to highlight in terms of the outcome of the Morison case, upheld that the employees of the CIA must continue to honour their promises to not reveal classified information. As such, and also as someone who had been held to such a promise, Morison was able to be convicted of his charges. Sentenced to a two year sentence, Morison served only eight months. Several years later, he was ultimately pardoned of the crimes in 2001 by President Bill Clinton (Clinton, n.d.).

The case of Chelsea Manning, and of course the 1985 Samuel Morison case, elucidate a clear problem in the United States' court system— those who find issues that should be exposed and

corrected within the federal system are instead punished for actions such as these. While it is noble that these individuals are willing to risk their freedom for the protection of American citizens and the promotion of transparency within the government, it is certainly unjust that they are treated punitively for actions when the information shared pertains to the safety and security of civilians and citizens around the world. However, the information released in several of these instances may cause more damage to American citizens, especially named citizens, than benefits, thereby again questioning the true benefit of these leaks.

Most recently, Joshua Schulte was convicted on the thirteenth of July, 2022, of a 2017 data leak that involved the sending of approximately eight thousand, seven hundred and sixty-one documents to WikiLeaks (Murphy, 2022). The files sent to WikiLeaks included detailed information of the CIA's cyber-warfare tool entitled "Vault-7", which was a project that permitted the CIA to hack any smartphone overseas or otherwise and modify them, therefore turning them into listening devices for the organisation. Originally, Schulte, representing himself in court, was tried in 2020, but the original case was declared as a mistrial due to a deadlock on the behalf of the jury. During his tenure at the CIA, Schulte worked as a data engineer, building the very program for the organisation which he would later expose to WikiLeaks in what is considered one of the biggest thefts in the history of the CIA. His programs in Vault-7 focused on the abilities to hack iPhones, Androids, computers, and smart televisions. He faces decades in prison now for whistleblowing on this project that permitted something that was absolutely unacceptable for the government to allow, as it directly violates the privacy rights of individuals all over the world.

However, during the trial, prosecutors focused on his growing resentment for the CIA, with an emphasis on dislike for how his management treated him (Al Jazeera, 2022). Having resigned in November 2016, the leaks began in March 2017 on WikiLeaks, with prosecution claiming that Schulte was motivated to publish the documents pertaining to Vault-7 due to continued feelings of spite. He was arrested in August 2017 on unrelated charges, and held in prison once his bail permissions were revoked after a four month period. Schulte maintained his innocence toward the leaks during the trial, claiming that he was framed and used as a scapegoat solely because of his issues with his management. However, if he were to have been the source of the leaks, this would be an example of whistleblowing as it provided insight into unsavoury practices that permitted backdoor access into private individuals' cell phones and other technology remotely, naturally without their knowledge, from anywhere in the world (Murphy, 2022). His whistleblowing

potentially protected the privacy of thousands of people as the program was revealed to individuals around the world, thereby permitting governments to show disdain for the American organisation's work.

Thomas Drake began working for the NSA on September 11, 2001 (60, 2021). His first day became more memorable than most individuals' first days on the job, as this day was the day an attack on the United States was perpetuated. Over time, Drake and other employees began to feel frustrated at the vast amount of data, meaning hundreds of thousands of terabytes of data, that was kept yet not searched through by the NSA, especially in light of the recent events of the 9/11 terror attacks (Wise, 2011). The agency had a program entitled ThinThread that these individuals strongly believed could have not only have uncovered the 9/11 plot but also the characters behind the attacks, thereby allowing for the thwarting of the plan. ThinThread works to sift through all of the agency's collected data, thereby eliminating the need for hand sorting data. The software then can hide individual names and identifying information unless the researcher requires knowing their identity, thus permitting the data to be rematched to the individual themselves without any issue. This program was fully functional before 9/11, and the NSA had plans to implement it against it the leaders of Al-Qaeda, the perpetrators of the terror attacks (60, 2021). However, it was never fully implemented, and the data was never found on the terror attacks prior to the incident, clearly indicating a need to utilise systems such as ThinThread to properly benefit from the intensive data mining utilised by the NSA. We can see a clear parallel here between Drake and Snowden as the two began to feel that the overreach of the NSA was infringing upon the rights of the American citizens, as codified by the Constitution and continually upheld through the entirety of the history of the United States by the Supreme Court. With Drake's case, however, we can see that he went through the proper channels for four years, as demonstrated in the next few paragraphs, and still was unable to find a solution for the problem of these violations of privacy rights, which led to his decision to become a whistleblower.

In combination with a new NSA program entitled Trailblazer, a program meant to do essentially the same thing as ThinThread but for a much more expensive cost, Drake found himself more and more upset with the NSA's actions and initiatives toward violating the American peoples' privacy. Drake also found issues with the Trailblazer program as he and others believed that it permitted the violation of privacy rights of the American citizens much more easily than the ThinThread project, which was a violation of their Constitutional rights (Wise, 2011). With these

two projects in mind, in combination with the events of 9/11, Drake went to his boss, who instructed him to speak to the NSA inspector general. While speaking with his immediate boss, Maureen Baginski, Drake was told that the NSA had decided to go with implementing another program instead of ThinThread (Public, n.d.). In turn, Drake responded with similar commentary as Snowden to his boss: he mentioned that, through the utilisation of the other project, the NSA was in direct violation of the Constitution and the Fourth Amendment, and questioned why they were choosing to do this in spite of these grievous violations. His concerns were brushed off. After speaking with several other individuals who worked with the legal team of the NSA as well as the House of Representatives and a joint Congressional inquiry, he felt that his pursuits for justice were going nowhere (60, 2021).

In 2005, Drake stated that he was contacted by former Republican staff member Diane Roark, who worked on the House intelligence committee monitoring the NSA (Wise, 2011). Drake claimed that Roark asked him to speak to a reporter named Siobhan Gorman at the *Baltimore Sun*, which Roark later denied during Drake's indictment as her pushing him to speak to the press could lead to him losing his job. Regardless of the reasoning behind it, Drake did choose to speak with Gorman, and the two wrote via encrypted emails. During the indictment hearing in 2011, Drake's defence attorneys mentioned that he gave Gorman two documents that he believed were unclassified, but did not give her any other documents. This amount of literature is in comparison to the amounts of classified documentation given by Snowden to the journalists who wrote on his leaked information, therefore demonstrating another small difference between Snowden and Drake. During the years 2006 and 2007, a series of articles was published by Gorman regarding the NSA's projects ThinThread and Trailblazer (Wise, 2011). None of these articles ever cited Drake, but cited various sources; the articles also specifically mentioned the inefficiency of Trailblazer, combined with the exorbitantly high cost of the project, that led to its eventual abandonment by the organisation.

It took until November 2007 for federal agents to finally connect Drake to the articles and raid his house to search for the information (Wise, 2011). At the time, there were also articles published in the *New York Times*, to which he had no connection, but they questioned him regarding those and the ones in the *Baltimore Sun* to see what information he had given out. He fully disclosed that he gave the unclassified information to the *Sun* regarding Trailblazer, demonstrating full transparency. For two and a half years, the federal investigation into Drake continued. Finally,

in April 2010, the Baltimore federal grand jury issued an indictment against him, charging him with five counts of “wilful retention of national defence information” under the Espionage Act (Wise, 2011). An organisation mentioned in this thesis, the Government Accountability Project, provided legal advice for Drake during his trial (60, 2021). Drake maintained that he was unable to simply ignore the actions of the NSA despite his confidentiality agreement as he strongly believed that the public had a right to know that the tools available to the NSA could have saved lives if implemented while another tool burned through over a billion USD without regard to how well it functioned or affected the privacy of the American people. Drake himself points out the similarities between the Snowden leaks and his own, as he knew that Snowden chose to study his case before going to the press with his information (Public, n.d.). Drake mentioned that “he learned that you could not go through any channels at all. You’d be totally compromised; it was a waste of time. And he knew that if you did go to the press that you’d be jacked up on Espionage Act charges” (Public, n.d.). This explains the main difference between the two: Snowden had the precedent of Thomas Drake to follow in his footsteps. Without Drake’s example, Snowden likely would have ended up in the very same position as Drake, sentenced to prison for a number of years for pointing out the unfair violations of the Constitution. By leaving the United States and studying the Drake trial, Snowden was able to evade the charges that would have been levied against him as in this case, while also simultaneously presenting the facts unbiased to the American people.

The Radium Girls, as mentioned in the previous chapter and in this introduction, were women in the 1920s who worked in a factory. As in the name, they worked with radium, painting clock dials (Vaughan, n.d.). To do their jobs, they dipped their brushes into radium, licked the tips so the ends were a finer point, and then painted the dial. At the time, radium had only been discovered twenty years prior by the Curies, and therefore not much was known about the new element. The allure of using radium on clock faces was that it would glow in the dark, and young women were hired for the position as they had small hands, allowing for more precise painting work to be accomplished. During the twenty year period since radium’s discovery, it had been successfully used to treat cancer, which led to the belief that radium was a miracle element; naturally, people began putting radium in everyday items such as cosmetics and toothpaste to create different effects.

Over time, the Radium Girls earned the nickname of “ghost girls” as they began to get an eerie glow in not only their clothing but also their skin and hair due to the daily exposure to the

radium dust; this led many of these women to wear their finest dresses to work so that they would look more magnificent for when they went dancing. Even worse, many women chose to apply the radium paint to their teeth for a glowing smile. Of course, they were already ingesting the radium paint as they were told to lick the paintbrushes before applying the paint to the dial faces, and were constantly told by their managers and factories that the paint was harmless (Vaughan, n.d.).

However, after such a huge amount of exposure, women began to get incredibly ill. One of the first women to become ill was Amelia Maggia, a woman who worked at the Radium Luminous Materials Corporation, which later changed their name to the United States Radium Corporation. The factory was located in Orange, New Jersey (Vaughan, n.d.). Originally, Amelia had a toothache, which led to an extraction. Not long after, the teeth around it had to be taken out. Ulcers formed in their place, and eventually, her lower jaw entirely had to be removed. Further parts of her body had to be removed, until she died in September 1922. Doctors eventually determined that she died of syphilis, despite not having many of the similar symptoms of the disease, but they were unsure what else could have caused her early demise. More and more, these women from the radium factory began developing these same symptoms, and for two years their employers strongly denied any connection between the radium and these mounting deaths. With growing public distrust of the company, and a resulting decrease in profits, the company finally paid for an investigation into the health problems of these women, which determined that the radium was absolutely the cause of these deaths and illnesses. However, the corporation refused to accept the results of the report, still claiming that the radium was safe.

Finally, in 1925, Harrison Martland, a pathologist, was able to develop a test that conclusively was able to tell that radium poisoned the Radium Girls (Vaughan, n.d.). The Radium Girls continued to fight, hoping to protect their colleagues who were still working at the factory. They found an attorney in 1927 willing to take their case, but due to their worsening conditions, the girls took an out-of-court settlement to pay for healthcare expenses as many of them only had a few months remaining to live. Despite the settlement, the story made front-page news globally. It took until 1938, over a decade later, for the Radium Dial Corporation to be successfully sued by another dying worker named Catherine Wolfe Donohue for the workers to finally be protected. This case is one of the first examples in the history of the United States in which a corporation was actually held responsible for the health of their employees, which demonstrates its importance to the realm of whistleblowing (Vaughan, n.d.).

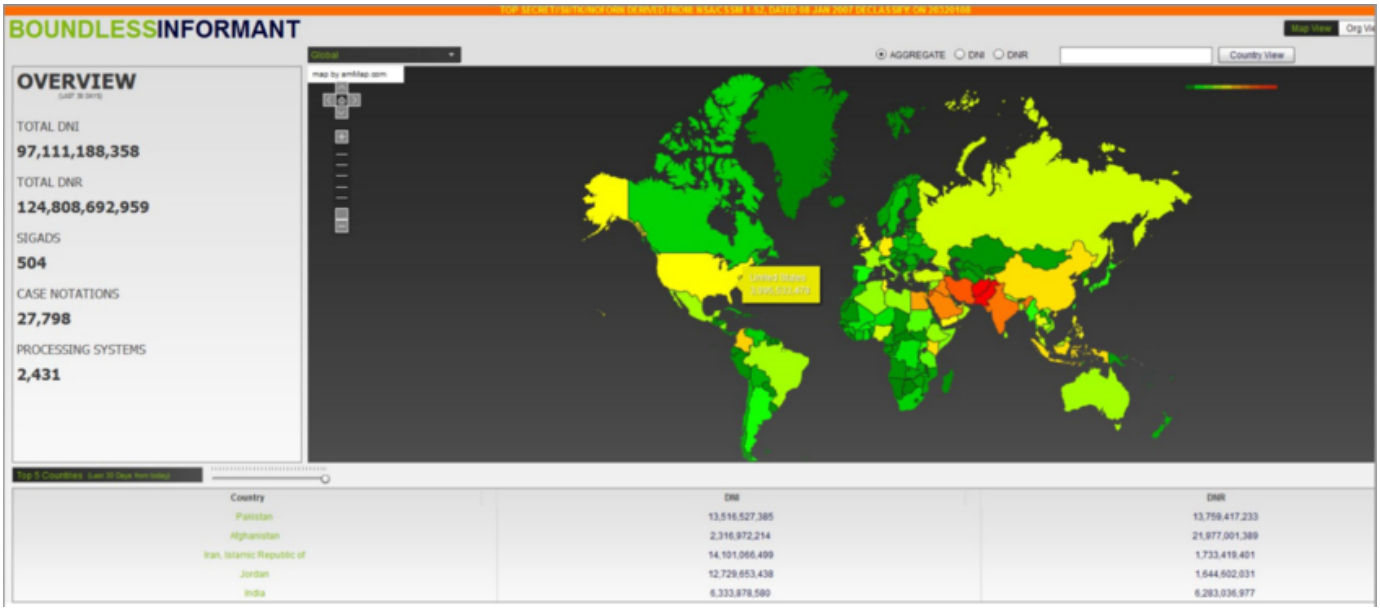
As a direct result of the Radium Girls, the United States Occupational Disease Law of 1936 was passed, providing coverage for "injury to health or death by reason of a disease contracted or sustained in the course of the employment and proximately caused by the negligence of the employer" (Sharkey, 1937). While the legislation passed is a notable change to employment rights as it provides a more direct access to ensuring healthcare protections for the employees whose health was negatively impacted by their working conditions, it must be heavily noted that the women who brought the health concerns of the radium factory to their managers were not supported at all, but rather were forced to suffer for months with debilitating symptoms that led to their eventual, tremendously painful, deaths, with no support from the company for their medical bills. As such, the importance of the Occupational Disease Law cannot be understated, as it would have permitted these women to gain access to the critical healthcare and aid they would have needed during their end of life care.

The link between the Radium Girls and modern-day whistleblowers is undeniable as they helped pave the way for many of the legislative protections— even if they are not fully protective— these whistleblowers are afforded in modern society (Vaughan, n.d.). The Radium Girls were also trailblazers as they were women in the workforce fighting for rights often not afforded to women and children, which demonstrates their continued desire to protect their fellow dial painters as the women who were sick continued to fight up until their deaths for those who would follow in their footsteps no matter how much pain they were in, leaving a lasting legacy for women and children for years to come. Another example of a trailblazing group of whistleblowers will be discussed in the next paragraph, as these individuals chose to speak out against violence at the very founding of the United States, allowing for the creations of the first whistleblower protections legislations to be inscribed by the Founding Fathers.

In spite of the expansion of organisations such as the ones mentioned in the previous chapter who are meant to work for the benefit of the whistleblower themselves and protect the work of whistleblowers such as Snowden, the NSA is collecting more data than ever. As evidenced by the data mining tool of the NSA called Boundless Informant, a heat map demonstrates the levels of data collected from each country, thereby allowing the user to show the countries with the most data collected (Greenwald, *Boundless*, 2013). Boundless Informant is a data analysis and visualisation

tool, pictured in the image below, that helps the user understand the amount of data collected from a specific country.

As shown in the image below, a heavy focus of data is mined from the Middle East, with a focus on Iran. More than fourteen billion reports of data is taken from this specific country, making it the highest amount of data mined globally (Greenwald, *Boundless*, 2013). In second place, Pakistan has thirteen and a half billion amounts of intelligence gathered. Jordan has the third-highest amount of data collected, with nearly thirteen billion reports, despite being one of the United States' closest allies in the Middle East. With nearly eight billion pieces of data, Egypt is in fourth, and finally India is in fifth place with just over six billion reports of intelligence collected. This demonstrates that, despite the belief that the NSA is meant to protect the internal borders of the United States, much of its work is outwardly focused, as the country itself is not even within the top five of the highest amount of intelligence gathered. Of course, this may strongly lead other nations to feel as if the United States Government is violating their citizens' privacy, and therefore Snowden provided them the opportunity to protect their citizens from spying.



Greenwald, *Boundless*, 2013

Chapter Ten: Necessity of Transparency in Society

Within a society that aims not only to uphold the tenets of democracy and freedom while also keeping up the security of said nation there arises a problem in which secret programs are believed to be a necessity by the government to protect the aforementioned freedoms. While naturally law-abiding citizens may wish to be kept apprised of such government surveillance projects such as PRISM, as they could be strongly considered a violation of their personal privacies, the fact remains that there is no definitive and distinctive line to ascertain the degree to which a citizen is law abiding from an outside perspective without further investigation into their actions in their daily life, which often requires covert studies of their actions through the utilisation of these sorts of projects. When such violations of privacy are kept a secret behind closed doors from the public and such a thing is outside of their voting power it almost entirely becomes the responsibility for someone with the knowledge of these projects to make this known to the public. In order for a society to be truly free or democratic there is expected to be some base level of transparency in how the state treats its own citizens. Privacy of thoughts, both shared and unshared, are vital and sacred to the people and how the government conducts its business must be clear and uncorrupt in the eyes of its constituents. The need for surveillance in order to offer protection to the citizens of a country has merit, but the conundrum of how much surveillance and who should be surveilled is problematic.

After Snowden's revelations, Congress passed the Freedom Act in 2015, thereby drastically reducing the mass collection of phone data, and rather replacing this data with "call detail records" (MacAskill, 2018). Call detail records simply show identifying information such as which phone numbers are calling which at what time, but not the contents of the call itself. The year following, the United Kingdom's Parliament passed the Investigatory Powers Act. However, conversely to the Freedom Act, the Investigatory Powers Act vastly overstepped the privacy regulations often viewed as necessary between the government and the citizens of the nation (Cropper, 2017). Snowden himself considered the Investigatory Powers Act to be "the most extreme surveillance in the history of western democracy", indicating a remarkable shift in how governments were responding to the Snowden leaks in spite of voter pushback. The Act was meant to be a replacement to the expiring Data Retention and Investigatory Powers Act, originally passed in 2014, that would have expired at the end of 2016. The provisions in the updated 2016 Act called for much more widespread capacity for the government and police forces in terms of the ability to intercept communications, as well as

their ability to request communications data, interfere with equipment, request bulk warrants for communications data, and technical capability notices. In many ways, this Act more strongly resembled the Patriot Act passed under the Bush Administration in the United States due to the overreaching capabilities of the government to gain access to private data, especially through the abilities of bulk warrants. Often, this Act was referred to as the "Snoopers' Charter", indicating a public distrust for the abilities the government would gain under this with its passage. It was passed in November 2016, much to the dismay of the general public in the United Kingdom.

Reflecting on the actions of Snowden, the former Government Communications Headquarters director Sir David Omand spoke about the current Director Fleming's assessment of the damage caused by these leaks. In the same vein, however, the agency also admitted Snowden had contributed to the introduction of new legislation and technologies for the organisation. "A sounder and more transparent legal framework is now in place for necessary intelligence gathering. That would have happened eventually, of course, but his actions certainly hastened the process," stated Omand (MacAskill, 2018). Critically, Snowden's revelations revealed just how delicate of a balance security and securitisation is for a nation— and how much one must reflect on what the citizens would consider to be oversecuritisation and overstepping the boundaries of their privacy. Simply put, Snowden put the emphasis and focus on these topics for the general public, and this change made governments incredibly uncomfortable as it created the realisation that what they were doing may not be completely acceptable in every aspect, and therefore must be reevaluated to ensure that their citizens, as the ones who pay for these systems through taxes, are understanding and accepting of these systems. Secrecy of governmental activities may not be afforded in this day and age as people are less willing to look the other way when disreputable situations surface on their watch.

In consideration of the transparency of a nation, one must consider two indices which will be discussed here. The twelve categories of the Human Freedom Index are rule of law, security and safety, expression and information, movement, religion, association assembly and civil society, identity and relationships, size of government, legal system and property rights, access to sound money, freedom to international trade, and regulation (Freedom, 2022). While many of these tend to have positive relationships such as demonstrated in the relationship between movement and freedom with international trade; generally, countries with stronger passports have more access to international trade. There are several indices here that seems to have a negative relationship such as

size of government and regulation; if a country has more regulation it inherently has a larger government. Likewise, the two sectors of security and safety as well as expression and information seem to have a negative relationship in recent trends as well. The highest rated country in 2022 is Switzerland, with a Human Freedom Score of 9.11. Not even placing in the top ten, but rather at number fifteen, the United States has a score of 8.73, tying with Japan. The score includes a personal freedom score of 9.09 and an economic freedom score of 8.24, placing the country in the first quartile of ranked countries under the index.

Similarly, the United States ranks twenty-seven out of one hundred and eighty countries, with a score of sixty-seven out of one hundred, on the corruption perceptions index in 2021 (*2021*, n.d.). To explain the score, the closer to one hundred the result of the perceptions index, the less corruption is demonstrated within the government. The highest ranking countries tied for first place are Denmark, Finland, and New Zealand, with a score of eighty-eight. These scores are analysed and calculated based upon at minimum three data sources, which are the result of thirteen different corruption assessments and surveys. The sources of the data come from a wide net of reputable organisations, such as the World Economic Forum and the World Bank, which therefore helps eliminate bias, which would naturally occur if a government were to assess itself (*2021*, n.d.).

The relationship between both the human freedom index and the corruption perceptions index seem to be related as Switzerland, New Zealand, Denmark, Sweden, and Luxembourg all rank within the top ten countries for both of these indices, indicating high freedom and low levels of governmental corruption (*2021*, n.d.; Freedom, 2022). While freedom of information is not the only important aspect that goes into measuring the level of freedom within a country, it does make an impact and it seems that countries with lower levels of corruption, and therefore more transparent governments, also rank higher in levels of human freedom. On the other hand, countries such as Syria, Venezuela, and Somalia seem to rank lower for both of these indices, with these three ranking in the bottom ten for each the human freedom index and the corruption perception index. In order for a country to have higher levels of freedom within their society, they must be able to have more access to knowledge of the actions of their government and be able to vote upon whether or not those actions should be taking place or not.

As previously mentioned in this paper, when it comes to the PRISM project, the legalisation of this addition to the NSA was something that was voted on by Congress, yet the members of

Congress apparently were not given the entire story about what said project would include. Not only was it hidden from American citizens, but it was kept hidden from the very people who approved it in the first place. This is a clear demonstration of a lack of transparency in government, which is a tremendously explicit reason as to why individuals such as Edward Snowden must remain in society and should be pardoned, not penalised, for their actions as they play a critical role in holding the government accountable for their actions. Whistleblowers are the oversight to secrecy and without a check and balance system, governments can overpower their constituents.

There are currently roughly 4.3 million people in the United States that have a form of security clearance as of October 2015 (Jansen, 2017). Most interestingly regarding security clearances is the fact that these statuses do not expire, but rather they require a renewal investigation into the individual to ensure that they do not have any contraindications that would pose a problem for someone with access to sensitive materials, such as the ability to be coerced by a foreign government. Traditionally, people with top-secret clearances, of which in the United States there are 1.4 million, are renewed every five years. For those with secret, these renewals occur every ten years for the nearly 2.9 people who have either secret or confidential level clearance. For individuals with confidential, their renewals occur every fifteen years. However, it is necessary to reflect on how less than a tenth of the United States' population is able to have access to knowledge regarding specific inner workings of the government, while everyone else is required to wait for whistleblowers and those who are upset at the actions of these secretive organisations to reveal that they exist.

One must also consider that the government believes a leak of confidential data to be a grievous crime, however, with a leak from even the lowest level of confidential individuals causing "damage to the national security" (Jansen, 2017). Going further into higher clearance levels, a secret clearance level leak would be considered "serious damage", while most critically a top secret level document leak would be considered as "exceptionally grave damage". As such, it is clear to see that while whistleblowers are incredibly important for the general public to ensure that all parties know what is going on with their information and to ensure transparency, it is also critical to note how negatively the government views the actions of whistleblowing, even if it were to be for the best interest of the American peoples.

The act of whistleblowing, however, should not only be something that is allowed in order for citizens to truly know what their government is doing but it should be encouraged in order to protect those who could be in harm's way. Circling back on the justification that Snowden gave in which he states that he aimed to uphold the inherent rights in the Constitution, we can reflect on one of the first cases of whistleblowers in the United States (*Timeline*, 2022). The events of this whistleblowing incident resulted in the Second Congressional Congress (a group of people which included many of those who took part in creating the Constitution in the first place) creating the nation's first whistleblower protection law. In 1777, two naval officers, Samuel Shaw and Richard Marven, witnessed one of their commanding officers torture British prisoners of war and decided to report him. Much like how modern whistleblowers are treated, they were both dismissed from the Navy, placed in jail, and charged with a criminal libel lawsuit. The two would later ask Congress for help and, in turn, the Continental Congress in 1778 unanimously enacted the first whistleblower protection law, named the Whistleblower Protection Act of 1778, and helped them win their lawsuit through the donation of money for their lawsuit, despite the Congress lacking much money itself due to the country just having been founded. Ultimately, their legal bill amounted to one thousand, four hundred and eighteen USD, which was fully paid by the Congress.

The Whistleblower Protection Act of 1778 states that "it is the duty of all persons in the service of the United States, as well as all other inhabitants thereof, to give the earliest information to Congress or any other proper authority of any misconduct, frauds or misdemeanours committed by any officers or persons in the service of these states, which may come to their knowledge" (Klein, 2019). No dissent to the passing of the legislation was recorded. Additionally, their commanding officer was ordered to be fired. With the wording of the 1778 Act, it clearly demonstrates the dedication of the Founding Fathers to receiving clear and unhindered information in any context that demonstrates a failure on the behalf of someone in the employ of the United States, or a company in the United States. It seems in line with their wishes to comply with this and not continue to seek punitive measures for the acts of whistleblowers, contradicting the current measures and actions of the government and military.

In modern America, many politicians argue that the Constitution is one of, if not the most, important document for the country. If this were to be true, then the ability to uphold its contents, even if it makes those violating it uncomfortable, should be an indelible right as a path to make the country more law-abiding and in line with the wishes of the founders of the nation. In this line of

thinking, what Snowden did by publishing the documents of the NSA was simply providing evidence to the American people that the government was not completely transparent with what was happening to their data, which again falls under the Constitution. It can be argued, naturally, as Snowden himself has stated, that what he was doing was simply protecting the values and statements upheld in the Constitution, which is in line with the beliefs and statements of the Founding Fathers of the United States— as such, there is no viable reason why the United States Government should seek to prosecute him as he is working to achieve similar goals, on a larger scale, as the naval officers in 1777 were working to accomplish.

We can see as well that Snowden is not alone in how the United States Government has chosen to treat him for his decision to speak out, as evidenced by Chelsea Manning, Joshua Schulte, and the other examples given in this thesis. Historically, despite the evidence that the Constitution should be upheld, the government works to suppress rather than support whistleblowers, which directly contradicts what they claim to uphold in terms of belief in the Constitution, calling into question their true focus and belief in the document. Additionally, these aims in prosecuting whistleblowers who work to uphold the Constitution fall directly in contradiction to the historical examples of the Founding Fathers themselves supporting whistleblowers, which is another argument for why the Congress and government itself should be supporting rather than suppressing the actions of these brave individuals who choose to speak out against unfair or unsafe practices by companies or the government— the Founding Fathers themselves supported the actions of whistleblowers and worked to support their cases in court. To truly uphold what the Founding Fathers believed, the Congress and government should do the same.

Chapter Eleven: Conclusions

The American Civil Liberties Union, on the fifth anniversary of the Snowden leaks, spoke out on the articles, stating that "thanks to Snowden's disclosures, people worldwide were able to engage in an extraordinary and unprecedented debate about government surveillance," (Gallagher, 2018). The Snowden Effect has most definitely created a drastic change in society's understanding of their personal privacy with regards to the internet and the freedom to maintain that privacy from the United States Government and other entities. Their newfound awareness led to massive protests against corporations and legislation regarding privacy which has in turn led to changes in security in both of these realms, but mainly regarding corporate policy. This change is demonstrated through the renewed commitment of corporations to personal privacy and the protection of personal data to the fullest extent possible, which was explored through the instances of the case San Bernardino shooter's iPhone and through apps used to track fertility and menstrual cycles of women following the reversal of the court decision *Roe versus Wade* in the United States Supreme Court. While Edward Snowden did not revolutionise American data security legislation, he was the catalyst for significant changes in how corporations interact with their customer base and the United States government, as they typically choose to emphasise data security and their methods through which they are able to accomplish this.

In regards to the impact of the Snowden leaks themselves, we can take a look at the results of Snowden from nearly a decade later and see that, while his revelations seemingly were quite shocking not only in the United States, they also had the potential to elicit significant change in privacy policy in not only American politics but also global politics in general; however, these revelations were generally ignored and often majorly forgotten after the initial shock of the news articles wore off from the general public's mind. The fact that the American people, as well as the general global population, were in an uproar, meant that corporations were forced to look at how they responded to their users' demands in terms of personal data security and privacy both on the internet and on personal devices. In spite of the changes and outrage toward Snowden's revelations, it must be noted that, as of 2018, an estimated eight hundred and fifty million individuals around the world are iCloud users, backing up their data to the amorphous cloud, demonstrating that their memories of the leaks and the government's desire to look at personal information was very short lived (Novet, 2018). Bruce Schneier, an author and security technologist, spoke on this very issue,

stating that “suddenly, everybody knows, and nothing’s changed. It was never a campaign issue. We tried to make it one. We failed… the subsequent changes are very small” (Gallagher, 2018).

To sum up the legacy of Snowden’s revelations, an article written by Sean Gallagher five years following the release of *The Guardian’s* articles involving Snowden’s leaks provide insight into how individuals had been affected by his actions due to changes in both institutional and political policy. For essentially the first time in history, citizens across the globe were able to en masse discuss their opinions on a government surveillance policy that had been very blatantly named and explicated to be spying on everyone indiscriminately (Gallagher, 2018).

In spite of this massive global change to the general public’s ability to speak on privacy as well as the knowledge of what privacy actually entails versus the former belief that individuals did have some modicum of privacy within their personal devices, very little changed in terms of the policy that protected citizens for several years following the Snowden revelations. While some people did generally advocate for changes to the security policy, this advocacy led to very little impact in actuality, and in very few instances are the leaks cause for change and continued discourse in politics. Of course, there were two major pieces of legislation passed, and a few examples of major corporations choosing not to release or provide backdoors into their products have become major news within the United States. For example, the 2015 USA Freedom Act changed both what type of and how phone data is collected, which in some ways created a semblance of security for private citizens while also creating much more access to data collection for the NSA. The second major piece of legislation was not in the United States, but rather in the United Kingdom, but still changed how the government and the police could gain access to private information with ease, to the dismay of the general public.

Unfortunately, it is apparent that the actions of Snowden, while causing an initial stir for many around the world, impacted very little in terms of changing how governments and citizens interact to protect personal data, but created a new system in which corporations feel, at least on the surface, more obligation to the customer to demonstrate their dedication to privacy and data protections in circumstances where the corporation is able to deny requests from the government. Realistically, this lack of governmental change in regulation is likely due to the fact that they wish to maintain access to device information and data sources in an attempt to prove that terror attacks and even other criminal activity can be successfully thwarted using this method, despite all

evidence pointing to the contrary, as stated earlier in this paper, with the research mentioned from the Privacy and Civil Liberties Oversight Board (Eddington, 2019).

However, it can be argued that the work that many corporations are doing to implement data security mechanisms for their customer base do provide at least some layer of protections in areas where the government is currently not legislating their access to data directly. This ensures that the individual data security is relatively secure barring a government request for data, which would require a legal process, which would then be typically reported in the company's transparency report, thereby alerting customers to the government's request. In some ways, this method provides some more transparency for the user than if the government had provided more legislation, as the corporations typically work to ensure the continued loyalty of their customer base, and have often ensured everything in their power to exploit the current loopholes of the legislation and government processes to provide data security to the customers. In this way, it is evident that, for some individuals, Snowden has provided a lasting impact with positive changes in spite of the general smear campaign against him by individuals who wished to frame him as a communist and a conspirator against the American people.

Sources

2021 corruption perceptions index - explore the results. Transparency.org. (n.d.). Retrieved July 14, 2022, from https://www.transparency.org/en/cpi/2021

60 Minutes. (2021). *60 Minutes Archive: U.S. v. Whistleblower Tom Drake*. YouTube. USA. Retrieved July 27, 2022, from https://www.youtube.com/watch?v=ewFZ5FZwVQM.

About the Foreign Intelligence Surveillance Court. About the Foreign Intelligence Surveillance Court | Foreign Intelligence Surveillance Court | United States. (n.d.). Retrieved March 3, 2022, from https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

About Us. National Whistleblower Center. (n.d.). Retrieved July 14, 2022, from https://www.whistleblowers.org/about-us/

Ackerman, S. (2013, August 9). *Lavabit email service abruptly shut down citing government interference*. The Guardian. Retrieved July 16, 2022, from https://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden

Al Jazeera. (2022, July 14). *Ex-CIA engineer convicted over massive data leak*. WikiLeaks News | Al Jazeera. Retrieved July 26, 2022, from https://www.aljazeera.com/news/2022/7/14/ex-cia-engineer-joshua-schulte-convicted-of-largest-data

Bamford, J. (2014, August 13). *Edward Snowden: The untold story*. Wired. Retrieved July 23, 2022, from https://www.wired.com/2014/08/edward-snowden/

Binder, E., & Northrop, K. (2020, December 6). *The Snowden Effect*. Baucus Group. Retrieved March 23, 2022, from https://www.baucusgroupbeta.com/wp-content/uploads/2020/12/The-Snowden-Effect-The-Wire-China_12.6.20.pdf

Bradford Franklin, S. (2019, March 28). *Fulfilling the promise of the USA Freedom Act: Time to truly end bulk collection of Americans' calling records*. Just Security. Retrieved July 23, 2022, from

https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/

Braun, S., & Flaherty, A. (2013, June 15). *Prism is just part of a much larger, scarier government surveillance program*. Business Insider. Retrieved March 12, 2022, from https://www.businessinsider.com/prism-is-just-the-start-of-nsa-spying-2013-6

Buchler, B. (2016, November 11). *Snowden and civil disobedience.* Medium. Retrieved July 23, 2022, from https://medium.com/@bryanbuchler/snowden-and-civil-disobedience-15907b9a0704

CBS Interactive. (2016, September 16). *Edward Snowden wants to Come Home: "I'm not asking for a pass. what I'm asking for is a fair trial"*. CBS News. Retrieved July 23, 2022, from https://www.cbsnews.com/news/edward-snowden-nsa-cbs-this-morning-interview-today-2019-09-16/

Chappell, B. (2021, October 25). *The facebook papers: What you need to know about the trove of insider documents.* NPR. Retrieved July 28, 2022, from https://www.npr.org/2021/10/25/1049015366/the-facebook-papers-what-you-need-to-know

Clinton Digital Library (n.d.). *Pardon - Samuel Loring Morison - Collection Finding Aid*. Retrieved July 13, 2022, from https://clinton.presidentiallibraries.us/items/show/36273

Coliver, S. (n.d.). *United States v. private first class Chelsea Manning*. Open Society Justice Initiative. Retrieved July 25, 2022, from https://www.justiceinitiative.org/litigation/united-states-v-private-first-class-chelsea-manning

Cook, T. (2016, February 16). *Customer letter*. Apple. Retrieved May 14, 2022, from https://www.apple.com/customer-letter/

Cropper, L. (2017, April 2). *The investigatory powers act 2016 – a "snoopers' charter" or a legitimate surveillance tool for today's society?* Fieldfisher. Retrieved July 25, 2022, from https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-investigatory-powers-act-2016-a-snoopers-charter-or-a-legitimate-surveillance-tool-for-todays-society

Davies, D. (2019, September 19). *Edward Snowden speaks out: 'I haven't and I won't' cooperate with Russia*. NPR. Retrieved March 3, 2022, from https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia?t=1646325834785

Devine, T. (2015, July 1). *Supplemental Submission for United Nations Rapporteur: International Best Practices for Whistleblower Policies*. OHCHR. Retrieved April 5, 2022, from https://www.ohchr.org/sites/default/files/Documents/HRBodies/CEDAW/ClimateChange/OxfamPhilippines.doc

Eddington, P. G. (2019, June 6). *The Snowden effect, six years on*. Just Security. Retrieved May 22, 2022, from https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/

Five years after Snowden blew the whistle, the NSA shutters controversial program. Government Accountability Project. (2019, March 7). Retrieved March 11, 2022, from https://whistleblower.org/uncategorized/five-years-after-snowden-blew-the-whistle-the-nsa-shutters-controversial-program/

Freedom Index by Country 2022. Freedom index by country 2022. (2022). Retrieved July 6, 2022, from https://worldpopulationreview.com/country-rankings/freedom-index-by-country

Gallagher, F. (2021, December 3). *Facebook 'failing' to tackle covid-19 misinformation posted by prominent anti-vaccine Group, study claims*. ABC News. Retrieved July 28, 2022, from https://www.google.com/amp/s/abcnews.go.com/amp/Technology/facebook-failing-tackle-covid-19-misinformation-posted-prominent/story%3Fid%3D81451479

Gallagher, S. (2018, November 21). *The Snowden Legacy, part one: What's changed, really?* Ars Technica. Retrieved July 23, 2022, from https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/

Geiger, A. W. (2018, June 4). *How Americans have viewed government surveillance and privacy since Snowden Leaks*. Pew Research Center. Retrieved April 3, 2022, from https://

www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/

Gerstein, J., & Ward, A. (2022, May 2). *Exclusive: Supreme Court has voted to overturn abortion rights, draft opinion shows*. POLITICO. Retrieved July 9, 2022, from https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473

Goodreads. (n.d.). A quote by Edward Snowden. Goodreads. Retrieved July 11, 2022, from https://www.goodreads.com/quotes/10129123-being-a-patriot-doesn-t-mean-prioritizing-service-to-government-above

Greenberg, A. (2014, October 13). *These are the emails Snowden sent to first introduce his epic NSA leaks*. Wired. Retrieved March 11, 2022, from https://www.wired.com/2014/10/snowdens-first-emails-to-poitras/

Greenberg, A. (2017, February). *Edward Snowden's New Job: Protecting Reporters From Spies*. Wired. Retrieved July 11, 2022.

Greenwald, G., & MacAskill, E. (2013, June 11). *Boundless informant: The NSA's secret tool to track global surveillance data*. The Guardian. Retrieved July 20, 2022, from https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). *Edward Snowden: The whistleblower behind the NSA surveillance revelations*. The Guardian. Retrieved March 6, 2022, from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Harding, L. (2014, February 1). *How Edward Snowden went from loyal NSA contractor to whistleblower*. The Guardian. Retrieved September 30, 2021, from: https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract

Harris, S. (2014, January 13). *What was Edward Snowden doing in India?* Foreign Policy. Retrieved July 12, 2022, from https://foreignpolicy.com/2014/01/13/what-was-edward-snowden-doing-in-india/

Hattem, J. (2016, December 25). *Spying after Snowden: What's changed and what hasn't*. The Hill. Retrieved April 11, 2022, from https://thehill.com/policy/technology/310457-spying-after-snowden-whats-changed-and-what-hasnt/

Jansen, B. (2017, June 7). *Who has security clearance? More than 4.3M people.* USA Today. Retrieved July 16, 2022, from https://eu.usatoday.com/story/news/2017/06/06/who-has-security-clearance/102549298/

Kelley, M. (2021, September 30). *Snowden flouts court ruling with paid speeches, Substack: 'He's above the law*. Yahoo! Finance. Retrieved July 11, 2022.

Kerr, O. (2015, April 9). *Edward Snowden's Impact*. The Washington Post. Retrieved March 3, 2022, from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/04/09/edward-snowdens-impact/

Klein, C. (2019, September 26). *The United States began protecting whistleblowers in 1777*. History.com. Retrieved July 26, 2022, from https://www.history.com/news/whistleblowers-law-founding-fathers

Korn, J. (2022, July 8). *Period-tracking apps are trying to make women feel safer about their data after the end of Roe v. Wade*. CNN. Retrieved July 9, 2022, from https://edition.cnn.com/2022/07/08/tech/period-tracking-apps-data-privacy/index.html

Lee, T. B. (2013, June 6). *How Congress unknowingly legalised prism in 2007*. The Washington Post. Retrieved March 23, 2022, from https://www.washingtonpost.com/news/wonk/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/

MacAskill, E., Dance, G., Cage, F., Chen, G., & Popovich, N. (2013, November 1). *NSA files decoded: Edward Snowden's surveillance revelations explained.* The Guardian. Retrieved March 3, 2022, from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

MacAskill, E., & Hern, A. (2018, June 4). *Edward Snowden: 'the people are still powerless, but now they're aware'*. The Guardian. Retrieved July 16, 2022, from https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware

McCarthy, C. (1985, November 17). *Samuel Morison: A leaker, not a thief*. The Washington Post. Retrieved July 25, 2022, from https://www.washingtonpost.com/archive/lifestyle/1985/11/17/samuel-morison-a-leaker-not-a-thief/6887525a-896e-4e7b-92e8-b9116c494774/

Mission & History. National Whistleblower Center. (2021, October 28). Retrieved July 20, 2022, from https://www.whistleblowers.org/mission-history/

Mullin, J. (2013, June 26). *In 2009, Ed Snowden said leakers "should be shot." then he became one.* Ars Technica. Retrieved July 14, 2022, from https://arstechnica.com/tech-policy/2013/06/exclusive-in-2009-ed-snowden-said-leakers-should-be-shot-then-he-became-one/

Murphy, M. (2022, July 13). *Joshua Schulte: Former CIA hacker convicted of 'Brazen' data leak*. BBC News. Retrieved July 14, 2022, from https://www.bbc.com/news/world-us-canada-62158799

Murse, T. (2019, March 27). *What does the NSA acronym PRISM stand for?* ThoughtCo. Retrieved March 11, 2022, from https://www.thoughtco.com/nsa-acronym-prism-3367711

Novet, J. (2018, February 11). *The case for Apple to sell a version of icloud for work*. CNBC. Retrieved July 27, 2022, from https://www.cnbc.com/2018/02/11/apple-could-sell-icloud-for-the-enterprise-barclays-says.html

Pilkington, E. (2013, July 31). *Manning conviction under Espionage Act worries Civil Liberties campaigners*. The Guardian. Retrieved April 7, 2022, from https://www.theguardian.com/world/2013/jul/31/bradley-manning-espionage-act-civil-liberties

Poitras, L. (2014). *Citizenfour*. RADiUS-TWC.

Public Broadcasting Service. (n.d.). *The frontline interview: Thomas Drake – United States of Secrets*. PBS. Retrieved July 28, 2022, from https://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-drake/

Radack, J. (2014, January 22). *Jesselyn Radack: Why Edward Snowden wouldn't get a fair trial*. The Wall Street Journal. Retrieved July 25, 2022, from https://www.wsj.com/articles/SB10001424052702303595404579318884005698684

Ralston, R. J. (2014, May 9). *Ontological Security: State Identity and Self-Image in the Digital Age*. Virginia Polytechnic Institute and State University. Retrieved September 30, 2021, from: https://www.history.com/this-day-in-history/edward-snowden-discloses-u-s-government-operations

Ray, M. (n.d.). *Chelsea Manning*. Encyclopædia Britannica. Retrieved April 5, 2022, from https://www.britannica.com/biography/Chelsea-Manning

Ray, M. (n.d.). *Edward Snowden*. Encyclopædia Britannica. Retrieved March 3, 2022, from https://www.britannica.com/biography/Edward-Snowden

Ray, M. (n.d.). *Julian Assange*. Encyclopædia Britannica. Retrieved April 7, 2022, from https://www.britannica.com/biography/Julian-Assange

Roe v. Wade overturned: Our latest resources. Guttmacher Institute. (2022, June 28). Retrieved July 9, 2022, from https://www.guttmacher.org/abortion-rights-supreme-court

Sharkey, C. F. (1937, December). *Discover economic history: St. Louis Fed*. United States Department of Labor. Retrieved July 16, 2022, from https://fraser.stlouisfed.org/

Smith, C. (2021, August 24). *How ordinary people are convinced to become spies*. The Conversation. Retrieved July 14, 2022, from https://theconversation.com/how-ordinary-people-are-convinced-to-become-spies-166688

Snowden, E. (2019, October 16). *Edward Snowden: Without encryption, we will lose all privacy. this is our new Battleground*. The Irish Times. Retrieved July 14, 2022, from https://

www.irishtimes.com/opinion/edward-snowden-without-encryption-we-will-lose-all-privacy-this-is-our-new-battleground-1.4052599

Snowden, E. (2016, May 26). *They know when you're sleeping, they know when you're awake*. The Sydney Morning Herald. Retrieved July 14, 2022, from https://www.smh.com.au/opinion/they-know-when-youre-sleeping-they-know-when-youre-awake-20160526-gp4cei.html

Snowden, E. (2022, July 9). Twitter. Retrieved July 11, 2022, from https://twitter.com/snowden/status/1545775610559078401?s=10&t=3zkl5tEKDHmP8utD-SwFIQ

Snowden, E. J. (2019). *Permanent Record*. Picdor.

Song, H., & Wilkie, S. (2017, February). *The Price of Privacy in The Cloud: The Economic Consequences of Mr. Snowden*. Retrieved April 3, 2022, from https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf

Sottek, T. C., & Kopfstein, J. (2013, July 17). *Everything you need to know about PRISM*. The Verge. Retrieved March 3, 2022, from https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

Stewart, E. (2018, December 21). *Facebook's very bad year, explained*. Vox. Retrieved July 25, 2022, from https://www.vox.com/technology/2018/12/21/18149099/delete-facebook-scandals-2018-cambridge-analytica

Timeline of famous US whistleblowers. Employment Law Group. (2022, May 10). Retrieved July 18, 2022, from https://www.employmentlawgroup.com/timeline-us-whistleblowing/#

United States Department of Labor. (n.d.). *Whistleblower Protection Program*. The Whistleblower Protection Programs. Retrieved April 5, 2022, from https://www.whistleblowers.gov/

USA PATRIOT Act: Preserving Life and Liberty. (n.d.). Retrieved April 3, 2022, from https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

U.S. Constitution - Fourth Amendment - Library of Congress. Constitution Annotated. (n.d.). Retrieved July 11, 2022, from https://constitution.congress.gov/constitution/amendment-4/

Vaughan, D. (n.d.). *Radium girls: The women who fought for their lives in a killer workplace*. Encyclopædia Britannica. Retrieved July 14, 2022, from https://www.britannica.com/story/radium-girls-the-women-who-fought-for-their-lives-in-a-killer-workplace

Victory for Latice Fisher in Mississippi - New York. National Advocates for Pregnant Women. (2020, September 24). Retrieved July 12, 2022, from https://www.nationaladvocatesforpregnantwomen.org/victory-for-latice-fisher-in-mississippi/

Vile, J. R. (2009). *United States v. Morison (4th cir.)*. The First Amendment Encyclopedia. Retrieved July 13, 2022, from https://www.mtsu.edu/first-amendment/article/291/united-states-v-morison-4th-cir

What is Snowden Effect? TechTarget (2015, October 27). WhatIs.com. Retrieved April 3, 2022, from https://whatis.techtarget.com/definition/Snowden-effect

Watson, C. (2018, April 11). *The key moments from Mark Zuckerberg's testimony to Congress*. The Guardian. Retrieved July 23, 2022, from https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments

Whittaker, Z. (2018, June 6). *Five years after Snowden: What changed?* ZDNet. Retrieved July 25, 2022, from https://www.zdnet.com/article/edward-snowden-five-years-on-tech-giants-change/

Wise, D. (2011, August). *Leaks and the law: The story of Thomas Drake*. Smithsonian.com. Retrieved July 27, 2022, from https://www.smithsonianmag.com/history/leaks-and-the-law-the-story-of-thomas-drake-14796786/

Younger, N. (2021, February 23). *The Case of Edward Snowden*. National Whistleblower Center. Retrieved April 7, 2022, from https://www.whistleblowers.org/news/the-case-of-edward-snowden/

Zakrzewski, C., Verma, P., & Parker, C. (2022, July 6). *Texts, web searches about abortion have been used to prosecute women*. The Washington Post. Retrieved July 9, 2022, from https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/

Zetter, K. (2016, March 17). *A government error just revealed Snowden was the target in The lavabit case.* Wired. Retrieved July 16, 2022, from https://www.wired.com/2016/03/government-error-just-revealed-snowden-target-lavabit-case/