LEBANESE AMERICAN UNIVERSITY

The Snowden Files: What did they reveal about the surveillance state in the US?

By

Jessica Maroun Ishaya Hanna

A thesis
Submitted in partial fulfillment of the requirements for the degree of
Master of Arts in International Affairs

School of Arts and Sciences

December 2020

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS APPROVAL FORM

Student Name: Jessica Maroun Ishaya Hanna I.D. #: 201605907

Thesis Title: The Snowden Files: What did they reveal about the surveillance state in the US?

Program: MA in International Affairs

Department: Social Sciences

School: Arts & Sciences

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

Masters in the major of International Affairs

Thesis Advisor's Name: Dr. Sami E. Baroudi

Signature: [redacted] Date: 14 / 12 / 2020
Day Month Year

Committee Member's Name: Dr. Imad Salamey

Signature: [redacted] Date: 14 / 12 / 2020
Day Month Year

Committee Member's Name: Dr. Jennifer Skulte-Ouaiss

Signature: [redacted] Date: 14 / 12 / 2020
Day Month Year

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants the Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic formats and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name: Jessica Maroun Ishaya Hanna

Signature: [redacted]

Date: 14/12/2020

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU's Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Jessica Maroun Ishaya Hanna

Signature: 

Date: 14/12/2020

ACKNOWLEDGMENT

This project would not have been possible without the support of many people. A huge thanks to my advisor, Dr. Sami Baroudi, who read my numerous revisions and helped make some sense of the confusion. Also, thanks to my committee members, Dr. Imad Salamey and Dr. Jennifer Skulte-Ouaiss, who offered guidance and support.

And finally, thanks to my parents, and numerous friends who endured this long process with me, always offering support and love.

The Snowden Files: What did they reveal about the surveillance state in the US?

Jessica Ishaya Hanna

ABSTRACT

Surveillance in modern western societies has always been a challenge to the foundation of these democratic liberal societies. The line that separates acts of surveillance for the purpose of national security from illegitimate acts that a surveillance state exhibits has always been a blurry one. This study aims at exploring the NSA files that were leaked by Edward Snowden in 2013 during the Barack Obama administration. These files exposed practices that the US government engaged in the post 9/11 era; practices that were constitutionally dubious yet promoted under the umbrella of advancing national security. By shifting from targeted surveillance to mass surveillance in the post 9/11 era, and with the expansion of technology, the US government has exhibited elements of a surveillance state that run contrary to the liberal democratic principles on which the U.S. was founded. These surveillance activities went well beyond safeguarding national security to serve other interests, including economic ones and the quest for international influence.

Keywords: USA, Surveillance State, Snowden, NSA, National Security

TABLE OF CONTENTS

Chapter **Page**

List of Abbreviations

CIA	Central Intelligence Agency
CT	Counterterrorism
ECPA	Electronic Communications Privacy Act
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court Review
FOUO	For Official Use Only
FVEY	Five Eyes
GCHQ	Government Communications Headquarters (UK's signals intelligence agency)
IC	Intelligence Community
IT	Information Technology
NOFORN	No Foreign Nationals
NSA	National Security Agency
SI	Sensitive Information
SIGINT	Signals Intelligence
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TS	Top Secret
U	Unclassified
UK	United Kingdom
UN	United Nations
US or U.S.	United States
USA FREEDOM Act	Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Drag-Net Collection and Online Monitoring Act
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

Chapter One

Introduction

In this thesis, I am aiming to examine how the U.S government's surveillance practices in the post 9/11 era have impacted the state of democracy in the United States. I will be doing so through analyzing the classified National Security Agency (NSA) documents that were leaked in 2013 by Edward Snowden. Despite being viewed as a liberal democratic state, the study argues that the U.S has been exhibiting, especially since the September 11 attacks, some elements of a surveillance state that are against its constitutional foundation and are not essentially directed at safeguarding national security.

1.1 Background

On June 5, 2013, Edward Snowden, a 30 years old NSA contractor, entered the annals of history when the first batch of disclosures regarding the activities and behavior of the United States National Security Agency (NSA) was published in the prominent UK newspaper *The Guardian*. In the period that followed, the documents that Snowden obtained while working for the NSA continued to be leaked, thus increasing the public's shock. The revelations of the leaked files uncovered a secret world that startled and confused not only U.S citizens, but the entire world who tried to make sense of the extent of what was revealed and what should be done, now that it is known. By his acts, Snowden has made the public an accomplice in calculations of surveillance, national security, human rights, ethics and laws. Snowden's move and the impact it had in the US and internationally, was unprecedented and created a ground-breaking point in areas of policy and politics: national security, cyber security, foreign policy, international laws and rights.

The large number of top-secret documents that Snowden leaked showed the extent of the mass surveillance that the NSA has exercised in the post 9/11 period and the technological expansion it had undertaken to ensure maximum data collection. The documents that were delivered to journalists and published mostly in *The Guardian* and *The Washington Post*, uncovered several top-secret surveillance programs such as Tempora, Xkeyscore, Bullrun, PRISM, Boundless Informant and Edgehill, and exposed the mission of each of the them. Via a number of procedures that capture and store phone calls, mine data from information repositories and technology providers, intercept electronic messages and break encryptions, these secret programs sought to provide the NSA with actionable intelligence (Hayes 2014), meaning information gathered from different sources that enables decision makers to take timely and appropriate action when faced with a threat to national security. These programs have accessed and mined data from big companies such as Facebook, Google, Yahoo, Microsoft, YouTube, Apple and Skype, which servers process billions of people's data and communications on a daily basis.

The US government had always justified its approach in implementing extensive mass state surveillance by arguing that it is for the purpose of eliminating threats against American soil and fighting global terrorism. However, after examining the exposed files, one is tempted to reach the conclusion that the U.S government has been engaging in some sort of illegal surveillance and has in some instances abused the power of the methods applied in the post 9/11 era with the goal of gaining economic expansion and diplomatic influence.

1.2 Surveillance and liberal political order

An important component of national security and a crucial function of security bodies includes the use of different analysis techniques that aim at profiling and grouping individuals based on their similarities and their likelihood to indulge in risky behaviors and unlawful acts.

The inclusion of these tools and processes in facilitating better national security is a necessary strategic approach for any country “willing” to monitor their population. Such practices have become even more important in the wake of global terrorism and have been prioritized in the United States, since the latter was one of the primary targets of terrorism, suffering many attacks on its soil, including the infamous 9/11 bombing that marked a crucial turning point of how the security apparatus works in the “western world”.

While what is known as the “western world” is mainly characterized by a political order that is liberal democratic, many western countries, especially the United States, can also be described by its advanced technological-enabled environment known and defined as a “surveillance society” by a number of scholars. (Gandy, 1989).

Lyon (2007) describes surveillance as the precise, streamlined and routine acquisition of information about people for the sake of monitoring, management, protection and providing future strategies on national security. The core objectives of surveillance include the creation of strong monitoring profiles to facilitate preventative measures and quick actions to activities that threaten national security. Profiling and surveillance are different, but they work together when it comes to matters of national security. Lyon (2007) indicates that profiling in matters of national security encompasses the collection of mass personal data and creating risk profiles that allow the prediction and picking out of risky behavior.

Other definitions made by Reichmann and Marx (1984) characterize profiling as "systematic data searching" that allows "a number of different data items to be correlated to evaluate how close an individual or an event is to a predetermined characterization or model infraction". The principle of this kind of practice is more preventative and risk-oriented, which means that rather than focusing on the presence or absence of risk, one predicts potential threats and evaluates them (Ceyhan, 2008).

While Lyon describes the state profiling activities as a “form of power organization through surveillance” (Lyon, 2007), Monahan on the other hand claims that the aim of surveillance is control, and that social control is characterized as "mechanisms for ordering society through the regulation of individual and group behavior" (Monohan 2010). Monohan argues that the extensive use of surveillance practices in liberal societies have negative impact on the defining principles of a liberal democratic state.

It has always been clear that the US government, whenever facing extreme risks and threats to its national security, does not always apply or abide by their own declared political, ideological and structural values (Rogerson and Milton 2013).

It is stated that surveillance against terror and the process of knowledge production should not require the consent or approval of the person of interest, especially in the fight against terror which should be a covert activity to reach its goal (Kitrosser, 2007); the knowledge, and technically the consent of the person of interest is not valid in the process of knowledge production (Lyon, 2001). According to the Bush administration, the secrecy of classified mass surveillance systems was of great importance and a necessity, where disclosure could lead to the disruption and eventually failure of intelligence and security agencies' missions which would risk permanent harm to national security (DoJ, 2006). However, such processes within liberal democracies contradict the defining values of the liberal state’s constitutional form, thus creating negative forces, compatibility problems and controversies. (Kreimer, 2004).

Provision of security is a major issue in liberal nations which seek to ensure that all the various rights of the citizens are protected by the government and that the nation is committed to meeting the needs of the citizens. However, some governments try to avoid their responsibility in showing transparency and accountability in their process of conducting

intelligence activities: they try to bypass the checks and balances in their quest to safeguard national security (Bigo, 2012). Bigo states that "exception" powers given to governments in unusual security contexts that undermine constitutional rights and civil liberties are always justified by the argument that the intended purpose is to ensure national security. However, he claims that the "rhetoric" of justifying going beyond constitutional barriers to protect the political order and ensure its survival is in itself a prominent threat to the political liberal order. The George W. Bush administration claimed that national security issues and essential public interests outweighed the values and ethics of "normal times". Furthermore, the administration tried to frame the legitimacy of its acts within the presidential authority given in the event of an emergency or crisis that threatens the country, and thus has not been entirely directed in its acts by the FISA (Foreign Intelligence Surveillance Act) directives (Kitrosser, 2007). Yet, this was not unproblematic.

With the fact that September 11 triggered an adaptive and comprehensive security system that deployed mass surveillance to counter risks and threats, it became increasingly obvious that such activities can be seen to contradict some US constitutional rights. As it will be discussed in this study, in the post 9/11 period, there has been a shift from targeted surveillance to mass covert surveillance. This "collect-it-all" process signals that the government has no trust in its citizens and assuming that everyone is a potential threat goes against the concept of the presumption of innocence of individuals, which is a critical legal entitlement for citizens in a constitutional democracy

Also, while the public was extensively monitored and subjected to strict methods of social control, Edward Snowden disclosed in 2013 that the watchers themselves had been exempted from surveillance. As Monohan claims, these are signals of a structure of social control and surveillance states.

1.3 Surveillance in the modern digital world

The use of surveillance technologies by the US government for security purposes has produced controversial consequences and debates, especially as the reduction of threats has become a top priority for the modern state in general (Lyon 2007) and after the 9/11 attacks more specifically.

Lyon (2003) says that among scholars, government officials, and public intellectuals, there is consensus that more study needs to be done to determine the effect of advanced surveillance technologies on the foundation of society and the state. In 2013, former US President Barack Obama assigned an important task to the Presidents Review Group on Intelligence and Communication Technology; he initiated a thorough investigation to study the significant effects that intelligence and communication technology have from the perspective of the liberal democratic American state. In the "Report and Recommendations of the Presidents Review Committee on Intelligence and Communication Technologies", the Committee notes that the concept of the balance between liberty and security contains elements of fact but is "often incomplete and deceptive" (The Presidents Review Group report, 2013).

Nonetheless, Lyon and Ceyhan described surveillance systems and technology as critical security enablers and important resources in the “War on Terror” (Lyon 2003, Ceyhan 2006). Also, former U.S. Director of the Federal Bureau of Investigation, James Comey, and the current Head of the National Security Agency, Michael S. Rogers, have described technological systems as “critical, indispensable, [and] vital” tools to U.S. national security (Ceyhan 2006).

Decades ago, Michel Foucault, a renowned philosopher, claimed that in modern times, western societies have tended to increase the monitoring of citizens in order to create a more controlled, standardized and obedient society (Foucault, 1977). He described this practice using the example of the Panopticon model developed by Jeremy Bentham. The Panopticon model

represents a jail which is designed in a way that inmates could be watched all the time, but they can never know when they are exactly being watched. By making surveillance pervasive, governments can discourage activity that they consider unusual or suspicious (Brunon-Ernst, 2012).

The Panopticon designed by Bentham is a circular grid with the cells parallel to the outside walls; in the middle of this circular shape, there's a tower where the prison officer resides and supervises the inmates. In each cell, there are large external windows and small internal windows that would enable the officer to monitor the prisoners' activities. Bentham argued that the principle was that the inmates would not know when they were surveilled, which in turn would make them believe that they were continuously under surveillance and that would eventually force them to be self-disciplined. This type of setting would encourage obedience and discourage inmates from misbehaving or engaging in criminal acts in the future. The panopticon philosophy has been used subsequently to enable powerful people in controlling populations and to regulate and alter their conduct.

In his book *Discipline and Punish* published in 1975, Foucault reshaped the idea of a panopticon. In the aim of subjugating citizens, Foucault argues that the Panopticon was used as a disciplinary mechanism in societies. Foucault analyzed the modern world's increasing technologies and its use of power. Today the panopticon's surveillance context is used in various settings such as the workplace, daily life, and government administration. When we start comparing the modern forms of surveillance to the central tower in the prison portrayed in the panopticon model, the significance of the panopticon as being only a metaphor begins to fade (Foucault, 1991a). Foucault argues that the Panopticon prison model of governance started to exist and became functional in many aspects of the western societies starting with the rise of the digital age. However, for Foucault, this system's elements remain somehow unnoticed

because they exist in the threads of everyday life, and this makes them so ubiquitous and powerful (Schofield, 2009).

In Foucault's analysis there were specific limits on individuals' rights and government powers, which is not the case today; as technology continues to grow and citizens become more liberated, there is an overlap in these spheres. Therefore, Deleuze, a post-structuralist thinker, calls for different frameworks of analysis regarding the balance of power and meeting the demands of democracy. Deleuze noted that the institutions described by Foucault and their aspects of practice no longer exist, rather, they have shifted to other methods of surveillance and practice of power. Deleuze, in partnership with Guattari, has developed this shift from the disciplinary society towards a society of control in the western modern world (Deleuze & Guattari, 1987). While the Panopticon is not rejected explicitly, Deleuze and Guattari shift from the Panoptical thinking by concluding that the socio-technical scenery has drastically changed. Deleuze explicitly rejects the idea of discipline as a driving force or goal of 'state surveillance', but rather found in the form of control.

Deleuze discusses how Western cultures are being transformed by globalization and capitalism and how organizations have become corporations: hospitals and schools for example. However, the distinction resides between the system and its mechanism. Where businesses depend on short-term outcomes, control is designed to achieve a long-term, prosperous and docile society that aims to enable resources to be used effectively to reach government-issued goals. Constant supervision is needed for this purpose, and this is done by constant monitoring and examination of markets, the labor force, and policies.

Another new position in theorizing surveillance from a post-panoptic viewpoint is neo-Marxist surveillance theory. Connecting Marx's philosophy to surveillance is not particularly recent (Fuchs, 2012). In reality, Marx also saw surveillance as a central feature of the modern

nation state and capitalist market systems, seeing surveillance as both a political and economic phenomenon (Fuchs, 2012). Surveillance is therefore a repressive and technological means of regulating and creating obedience among workers, but it is also a political system of dominance.

Following the 9/11 attacks, many governments have expanded on Foucault's panoptic concept to incorporate the openness of citizens and governments to mass surveillance and profiling in controlled situations. Modern technologies accommodating more information within a single period of observation allow for the analysis of the information through bundling data based on observable traits and behaviors associated with risk. Therefore, the government no longer uses the approach of watching citizens as a means of control but the use of sophisticated systems in linking the mass data collected to connect the dots. Without realizing that one is being surveilled, surveillance is taking place whether regarding our public or private aspects of our lives. State and business entities capture totally innocent actions that no one is especially ashamed of, using data gathering technologies to draw remarkably powerful inferences about people's behavior, attitudes, and values (Gorman, 2013). These innocent actions are tools that can only become more powerful over time as we leave tracks of ourselves all the time: our location, our communications, and even our DNA.

Mass data gathering enables surveilling both direct and indirect targets, which means that data about other people, with whom the targeted person lives and communicates are also collected and analyzed. Joined together, governments and private businesses are able to observe and study the targeted person's behavior (Lichtblau, 2007).

More public discussion about mass data gathering has raised awareness about how the most innocent actions and behaviors seemingly support docile obedience and create chains from which it is difficult to break free. The surveillance process may culminate in a significant

level of awareness about issues that some people are not aware of about themselves and their connections. Besides, the surveillance and profiling process results in the discovery and collection of information about other people who are in contact with 'persons of interest.' People are no longer be able to defend themselves simply by preventing the government from observing them, since the government no longer has to watch them specifically to obtain information, they are watched all the time.

With the same magnitude, the emergence of a mass surveillance state marks "the death of amnesia", since the observations are conducted without the knowledge of the persons (Foucault, 1977). If people indulge in abnormal or humiliating activities or take part in political demonstrations, their most powerful defense might be that they are oblivious of who they are, and they will quickly be forgotten. Consequently, their actions will not be remembered as they affect a small portion of the community or there is no video or photographic support to show their participation and activities to others. However, governments and companies keep track of what occurs at specific locations by technological means such as cameras, location tracking tools, and face recognition technologies. Those when paired with records of various times and locations can be easily collected then analyzed, forming a database for profiles of individuals, which enables tracking and facilitates the anticipation of their actions (Nakashima, 2014).

1.4 Modern surveillance vs. Liberal democracies

Having discussed the practices of a surveillance state, one can easily conclude that a liberal democracy, which is defined by government that is limited by a constitution and a commitment to human rights is hence threatened by the rise of a surveillance state. There are three main threats identified in the specific case of the United States.

The first threat is that the government will establish a parallel system of preventive law enforcement that goes around the conventional safeguards of the Bill of Rights[1]. An example of this is the practice of military detentions that took place under the Bush administration and the NSA surveillance programs that were expanded under his term. The Bush administration defended the detention and questioning of American citizens and the breach of the constitution by claiming that these were not ordinary times and there was no time to pursue ordinary law enforcement (Military Order of November 2001). The administration denied that the President or individuals close to him had been involved in any sort of criminal acts but rather that their involvement was for the purpose of gathering information that would prevent the reoccurrence of terrorist attacks. Therefore, the administration justified its use of warrantless surveillance on U.S citizens through the "war on terror" (Moschella, 2005).

The second threat resulting from a Surveillance State is that the government, once it gets accustomed to accessing information and advanced ways of collecting data, might become interested in using the data for other security, social, political, or economic benefits. As Derosa (2004) argues, if mass surveillance and collection of metadata can indeed identify and stop individuals from being involved in terrorist attacks, there is nothing that can stop a government from using these surveillance tools to find people who have committed simple felonies, such as not paying a parking ticket. Goldsmoth and Katyal (2007) also say that these tools, used with no supervision, can be implemented to establish a system that goes beyond the conventional criminal justice system. A stronger and more efficient surveillance system might entice the government to take advantage of the developed surveillance and analysis tools and use them in day-to-day law enforcement and in government services, thus detecting potential

[1] The Bill of Rights are the first ten amendments of the American Constitution: https://billofrightsinstitute.org/founding-documents/bill-of-rights/

troublemakers more quickly and efficiently by getting around warrants and breaking bureaucratic barriers.

The third threat is private control and public-private partnership. Since the private sector is not restricted by the Constitution as much as the public sector, the government intends to rely on the corporations to gather and produce information for it (Donohue, 2006). For businesses, this system allows them as well to collect mass data about people and target new potential customers and tailor their services accordingly. Therefore, businesses will strive to learn more and more about their clients and will sell this valuable data to other companies or to the government.

It is apparent that there is a debate regarding surveillance between realist scholars, who see that a state has to do all in its power to ensure national security, and liberalists who promote human rights and freedom above all else. Realists argue that "great powers should seek to maximize their overall power, because this is still the most reliable way to survive in an anarchic system" (Mearsheimer 2001). On the other hand, liberalists justify their objection to surveillance by emphasizing on the liberal democratic values such as liberty and privacy. Liberalists argue that surveillance in the modern world seems to be traducing values cherished by democracies (Bigo, 2010). In addition, the contemporary debate in the wake of terrorism involves transferring the justification of using surveillance technologies into areas of social and private life, and whether this is seen as constitutional in a liberal political order. Schulte argues that while modern surveillance is almost always justified by security reasons, its practices "often go on to be used for reasons that have nothing whatsoever to do with security" (Schulte, 2006). Therefore, it is important to examine and understand how surveillance systems put in place in the post 9/11 era have been used, and how they have impacted the liberal American state.

1.5 Research question and methodology

In this thesis, I am aiming to examine how the U.S government's surveillance practices in the post 9/11 era have impacted the state of democracy in the U.S.

Despite the institutional constraints of the United States and wide public opinion over the extent of surveillance, this thesis demonstrates that the executive branch in the U.S government, especially under the Georges W. Bush administration, had engaged in unconstitutional practices in the name of "War of Terror", and had been able to use surveillance for purposes beyond safeguarding the national security of the U.S, such as achieving political and economic advantages. Knowing that every state exercises some surveillance in the aim of safeguarding national security, it is when it goes too far beyond its mandate that it starts undermining liberal democratic principles and starts exhibiting elements of a surveillance state.

By shedding light on the information that Snowden shared, this thesis aims at analyzing how much this information demonstrates that the U.S has abused elements of surveillance to serve power interests. The thesis discusses some documented instances in which intelligence agencies overreached beyond their mandate and engaged in activities that were intended to achieve some economic and diplomatic gains.

The study will utilize a qualitative approach in analyzing the Snowden case to ascertain the extent to which the U.S has exhibited unconstitutional surveillance practices and to measure the success of mass surveillance in combating terrorism. One of the primary justifications for selecting the qualitative approach is the ability of the technique to allow the evaluation of literature and other material in-depth. Rahman (2017) recommends the qualitative procedure in collecting and analyzing the information as it is capable of accommodating new information in situations where there is a lot of existing insights and other sources of emerging data. The approach is useful in this study as it will allow the analysis of existing information used in

previous studies, new books on the Snowden case, and a review of emerging information on the situation.

Materials used in this study include legislative acts on surveillance, leaked classified documents published by *The Guardian* and *The Washington Post* (the first recipients of the Snowden Files), articles of investigative journalism and books such as *No Place to Hide* by Glenn Greenwald (the journalist Snowden contacted), *The Snowden Reader* by David Fidler and *Surveillance after Snowden* by David Lyon. Additional material includes statements made by Snowden himself and by former members of U.S intelligence community and government officials.

Following this introduction, the thesis will go through a brief history of the NSA and the scope of its work and role, then move to define national security in the context of the United States. It will also include a brief on the growth of state surveillance in the post 9/11 United States, explain the difference between targeted surveillance and mass surveillance, and state the necessity of the US government activities as seen by the pro-surveillance advocates versus the concerns and reservations the anti-surveillance community holds.

In Chapter 3, I will introduce Edward Snowden, his career timeline and some background information about his actions. I will also present his claim of justifying his act. The chapter will also present some of the major revelations that were exposed through the documents he handed to journalists from *The Guardian* and *The Washington Post*. Revelations mainly discuss the major surveillance programs put in place post 9/11, their objectives and how they were used.

Chapter 4 will focus on the analysis of the files and on the incidents of abuse of power they revealed. The chapter will be answering the following: did mass surveillance contribute in stopping a terrorist attack? What has this extensive surveillance been used for? Why this wide expansion in mass data gathering? This chapter mainly lays out the findings.

Chapter 5 presents the US government's reaction and defense against the accusations pointed towards its alleged overreach on its soil and globally. It will discuss the political implications of the Snowden files on domestic U.S. politics and how surveillance has undermined the democratic liberal principle in the U.S. This chapter will also discuss the international response to the actions leaked by Snowden, especially from Germany and Brazil, states that are considered allies of the US.

Chapter 6 discusses the aftermath of Snowden's revelations and the regulations that were put in place to ensure a government as powerful as the US does not overreach under the cover of protecting national security. The chapter concludes that the fact that these actions continued from an administration to another makes it difficult to argue that the executive branch was not aware of the activities that intelligence agencies were involved in. The U.S. remains a liberal state, but these surveillance activities manifested have undermined faith in the liberal democratic principles in which the U.S. was founded upon and have complicated relations with countries that are considered allies.

1.6 Significance and limitations of the study

While surveillance is important in all countries to ensure national security, it is important to understand how in emergency contexts and in the expansion of technology, surveillance systems put in place to safeguard national security can negatively impact legal and political norms and can be abused in an unconstitutional manner should there be lack of assertive oversight. The files leaked by Snowden raised awareness about the practices of mass surveillance made in the name of national security, and by analyzing their revelations and implications, an opportunity emerges to look for ways to lessen the tension existing between the surveillance state and individual liberty. Knowing that surveillance programs are vital to

national security and cannot be eliminated, understanding their loopholes is important in order to address them not only in the U.S, but in other democratic countries as well.

While the thesis argues that surveillance practices of liberal democratic states can sometime defy democracy and constitution and give way to an overreach of governmental power, the capacity of scholars to study this field remains empirically very limited, mostly because the nature of surveillance practices is secret. The only information existing so far on surveillance practices is from leakages made by whistleblowers such as Snowden & Wikileaks, and these represent only one point of view. While they claim that their motive is solely to raise awareness and include the public in the decision, it is still debatable if they are considered heroes or traitors.

Chapter Two

NSA and Surveillance

2.1 History of the NSA

Established in 1952, the National Security Agency, better known by its acronym NSA, became the premier entity for signals intelligence (SIGNIT) gathering in the United States intelligence community and the specialized entity in the information war of the rising digital age. Its role was to produce foreign intelligence by collecting, processing and analyzing communications or other type of data that pass through a wire or radio (Margulies, 2014). Upon its creation, the agency was kept as a secret. Its presence was only acknowledged in 1957 (Fidler, 2015). The NSA has monitored, collected and gathered foreign information on suspects whom are believed to pose a threat to the United States. To work with the NSA, one must hold a high security clearance and assure that they will never reveal the secrets and actions of the NSA.

The NSA's main task is to conduct researches into all types of electronic transmissions. Its main role is to protect and formulate codes to be used by government agencies and mainly the U.S military. It is also in charge of intercepting and analyzing coded communications transmitted electronically or through any other means around the world. To better coordinate the work between the NSA and the U.S military, a joint organization was established in 1971 which became known as the Central Security Service (CSS).

Later in the study, it will be discussed that in 1978, the establishment of the Foreign Intelligence Surveillance Act (FISA) imposed restrictions on the NSA. By the regulations of FISA, the agency could not conduct domestic surveillance unless in very critical circumstances it is granted authorization (e.g. when a U.S citizen is doubted to be "an agent of foreign power"). However, post the 9/11 attacks, the FISA lessened its restrictions and allowed the

NSA to monitor domestic communications as long as one party in the communication line is a non-legal resident of the U.S, is a foreigner or is believed to be outside the U.S.

The former director of the NSA, Michael Hayden, said that while the CIA is most known to the public, it is the NSA who has wider resources and is bigger in size in terms of budget and workforce.

As stated then, the NSA's main task is to gather intelligence that can be put in play to ensure national security. However, defining national security is important to understand the scope of work of the NSA.

2.2 Defining national security

The word 'security' is described by Ole Waever and Barry Buzan in the Copenhagen School as:

"a successful speech act through which an intersubjective understanding is constructed within the political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat" (Stritzel, 2007)

Addressing and defining an issue in a security frame is an option, not a given. It is only when things and incidents are defined and addressed by a government as being related to security that they can become classified as threats to national and/or international security. When a government makes a cautious decision to treat an issue as related to security, this issue is then considered "securitized". In a simpler manner, only when a government announces that a matter is related to security, does the matter become a security issue. An example of this would be clean energy and climate change: when the British government decided in 2008 in its national security strategy to address these problems as a matter of security for the country, they technically became set as national security-related issues (HM Government, 2008).

The executive branch of the U.S. government is the one responsible for releasing the National Security Policy Plan. The latter is a brief document in which it is stated what is

considered to be international priorities and objectives that are crucial for the protection of the U.S. national security. Reporting indicators include all actions essential for the prevention of violence and the enforcement of a national security policy.

The 2006 US National Security Strategy, describing the global security climate, starts by comparing security threats and context of the preceding years to the era of the beginning of the Cold War (US White House, 2006). The U.S government faced throughout that time the fear of communism. The 2006 security strategy describes the year's security climate as somehow similar to the one that existed when the battle against communist ideology was the main threat to democracy.

However, in the 2006 context, it was not the ideology of communism, but rather the one of extreme Islamism which is defined as a radical form of Muslim religious practice. The emergence of global terrorism was met in parallel with the efforts to launch a war on terror and defeat it (US White House, 2006). The other factor viewed in the 2006 NSS policy plan that resided in the security climate of that year was increased globalization that had affected the world both negatively and positively. Globalization and the advancement of technology had made the world more prone to breaches of security as "everything" was in the open now. Furthermore, there were increased opportunities for hacking and stealing information. In summary, the main global threats that shaped the security environment in 2006, according to the NSS plan, were globalization and radical Islamism. However, global terrorism was on the top of the list for the U.S as the main challenge to be addressed (US White House, 2006). According to the 2006 NSS, global terrorism is divided into four main categories: traditional, which is when an attack happens on U.S soil against citizens; catastrophic, which is defined by the use of weapons of mass destruction; irregular, which is characterized by the rise of radical insurgencies such as Al Qaeda; and finally, disruptive such as cyberattacks against the nation's infrastructure (see Table 2) (US White House, 2006).

In the section of national interests in the 2006 NSS, experts noted that the policy seemed a bit too vague and not as clear as previous NSS. The policy mainly describes how the US can form its upcoming responses to face the challenges, while establishing a range of key interests. While defeating global terrorism seems like the direct response against this threat, promoting democracy, free trade and free markets can be seen as indirect strategies to defeat the new enemy and secure the continued existence of a liberal democratic liberal U.S. government (US White House, 2006).

Hence, promoting economic freedom was decided by the 2006 NSS to be the best option that would allow the expansion of modern democracy, which in return would eliminate totalitarian regimes described as “terrorist”. It is worth noting that while the NSS usually reflects the domestic priorities of the U.S., this one was more focused on the defeat of global terrorism which appeared to be an interest itself rather than just a mean to protect national territory. The concept of “War on Terror” is mentioned almost everywhere in the 2006 NSS (US White House, 2006).

In addition, regarding goals for the future, or 'the path forward' in the NSS, the 2006 plan seeks to 'open societies' through democracy and the propagation of liberalism (US White House, 2006). According to the 2006 NSS, economic freedom is equivalent to political liberty and, as such, is "a spiritual obligation" (US White House, 2006).

Table 1: The 2006 US National Security Strategy under Georges W. Bush (US White House, 2006)

Security Environment	Battle against totalitarian ideologies (i.e. radical Islamism); Comparable to the Cold War era; Globalization accelerating.

National Threats	**Global Terrorism (high priority)** Divided into four Categories: -Traditional (military aggression, national-based) -Catastrophic (WMDs and global pandemics) -Irregular (insurgence, terrorism and illicit trafficking) -Disruptive (threats to space and cyber infrastructure)
National Interest	Defeat of terrorism; Democracy expansion; Protect and expand liberal markets.
Future Priorities	Promote freedom and justice; Lead a rising democracies community.

2.3 Surveillance history in the US

The emergence of technology was not the beginning of surveillance in the United States, but a more sophisticated approach to acquiring and spreading different forms of information. In fact, while mass surveillance traces back to the establishment of the United States, major communication advances, particularly during the two World Wars, witnessed significant intensification of government-led mass surveillance (Lovelace, 2015). Military developments such as the extensive use of radio technology during World War I and the establishment of the Cipher Bureau to aid in cryptology led to increased information gathering. In 1929, this bureau was dissolved but then recreated as the base of the Signal Security Agency in World War II (McNiff, n.d.). The first decree, the Federal Communications Act, tackling eavesdropping and wiretapping was established in 1934 by the Federal Communications Commission (FCC). This Act stated that wiretapping is not seen as illegal as long as the information gathered during this process is protected under a “nondisclosure agreement”.

In World War II, the USA was highly engaged on the scene, and the unexpected attack in 1941 on Pearl Harbor played a major role in expanding surveillance tools and measures and transforming the military intelligence agencies.

In 1947, under the National Security Act, the Central Intelligence Agency (CIA) and National Security Council were created to fight “new threats to American security” (Gallagher, 2013).

The setting up of the Armed Forces Security Agency (AFSA) in 1949 was in line with efforts to enhance electronic communication in the Defense ministry and promote better national security coordination. Critics considered the move highly ineffective and thus the AFSA was transformed into the NSA through an order by President Truman in 1952. The memo indicated that it is the responsibility of the NSA to systematically organize and control the SIGNIT activities in the USA against “enemy” governments (Gallagher, 2013).

Another major transformation to the US surveillance and intelligence agencies was during the Cold War era. Due to the global communication development after WWII, and the fear from the Soviets and their nuclear weapons, the NSA was full focused on collecting and decoding as much as possible information about what was believed to threaten the national security of the US. In pursuing this goal, communications had to be electronic so that the NSA could intercept them and later decrypt (crack the codes).

Following this process, Senator Joseph McCarthy came into the picture after using deceptive approaches to get elected. A quick look at McCarthy’s history reveals his background as a lawyer and a judge in the state circuit, which propelled him to become at 30 years old, the youngest judge in Wisconsin. His campaign strategies were characterized at the time as bare-knuckled, vicious, deceptive, and devastatingly successful (Reeves, 1982).

Post Pearl Harbor, McCarthy joined the Marines and was assigned to the South Pacific. Planning to run for Senate, he released his own press releases and called himself "Tail Gunner

Joe"—although he was no tail gunner (Reeves, 1982). After claiming that he injured his foot in battle, he faked a service award and then later in 1964 when running for senate, he accused his rival of assisting Russians to penetrate Eastern Europe (Reeves, 1982). Furthermore, during the campaign period, he also presented his will to get rid of communists from the public service payroll and accused President Truman for attempting to allow Soviets to take over their farms (Bennett, 1988). Through such deceptive tactics, McCarthy managed to win the election and expressed a commitment to investigate the Communist infiltration in the federal government's bodies as well as the nation's colleges and universities (White, 1956).

The McCarthyism period, which extended from the late 1940s until 1954, was characterized by repression and undermining of the Bill of Rights of the Constitution in the name of maintaining "national security". McCarthyism was the method of examining and indicting people in positions of power or control with dishonesty, treason, or subversion (operating secretly to disrupt or topple the government). Civil freedom was specifically restricted by the Espionage Act, in particular freedom of speech.

Though Senator McCarthy was finally brought down by his own Republican party, the legacy of seeing the threat of communism throughout the US government and American society was more durable. McCarthyism's legacy is twofold: one aspect rejects democracy in politics and liberty in culture; the other promotes successful opposition to those restrictions (Hamilton, 1995).

In 1968, the first ever federal law was established, known as the Omnibus Control and Safe Streets Act, with the role of restricting wiretapping. Later in 1972, the Watergate scandal broke, in which President Nixon's was accused of wiretapping and seizing secret documents. Watergate caused a rise in national awareness regarding governmental practices and use of eavesdropping. More transparency was demanded from the political sphere and calls for reforms increased. However, the NSA and national surveillance practice largely remained

unknown to most of the public and to the world. Following the technological advancements in data wireless communications and the commercialization of computers, an adjustment to the Omnibus Crime Control and Safe Streets Act of 1968 was later put in place and was named the Electronic Communications Privacy Act (ECPA). This Act restricted monitoring phone calls and internet activities and provided new guidelines for the access of the storage of gathered electronic communications (McNiff, n.d.; & Vicens, 2013).

Historically, mass surveillance has had some consistent attributes, regardless of the particular techniques involved. Initially, it is often the opponents of the nation or the most vulnerable and deprived that have to bear the burden of surveillance, which causes those more privileged and whom show support to the government to believe that they are exempt from surveillance. Any mass surveillance technology or adjustment to the existing frameworks is adequate in stirring conflict between parties who believe that some of the people in power are exempt from the monitoring process. One assumption is that individuals who are aware of being observed find ways of slowly seeming obedient or end up living in fear. In the mid-1970s, the Church's committee (named after Frank Church, the Senator who chaired the select committee) was created to investigate the intelligence community's espionage activities. The committee was surprised to find that the FBI had listed almost half a million citizens as possible threats to national security and it regularly monitored their activities, only because they had a "different" political view. The list of regularly monitored individuals and groups included the Reverend Dr. Martin Luther King, the women's liberation movement, John Lennon, and many others (Cohn, 2013 & Gallagher, 2013). The Church Committee also found that the CIA has violated law and policy, and intercepted domestic communications (telegrams), which led the Congress to adopt in 1978 the Foreign Intelligence Surveillance Act (FISA).

In order to fix certain violations by the Central Intelligence Agency (CIA) in the 1960s and 1970s, congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA). FISA

has set up control of the NSA, the CIA, and other intelligence agencies to make sure these agencies are targeting external threats and not American citizens. FISA has created a Classified Foreign Intelligence Surveillance Court, to which intelligence agencies might request permission to conduct surveillance and gather information from foreign suspects. The Chief Justice of the United States Supreme Court appoints 11 judges to the FISA Court. The decisions of the FISA Court can be reviewed by a special court. The FISA's job is to regulate government's data gathering of foreign intelligence inside the U.S., requiring it to get prior review and approval by a special court named the Foreign Intelligence Surveillance Court (FISC).

After the September 2001 attacks, the US government endorsed what came to be known as the USA PATRIOT Act which has set since then a milestone and a drastic change in the way surveillance works in the US. The US PATRIOT Act was strongly debated in Congress because there were concerns on its global impact. This act removed all restrictions that were previously used to protect privacies and gave way for the US government to expand widely the use of its surveillance activities to reach domestic and international targets (Smith & Hung 2010). The US government, by reference to the PATRIOT Act, was allowed to gather mass electronic data and store personal data of US citizens without any checks and balances to overrule this process and with very minimal legal oversight.

The most crucial amendments made to the surveillance scope under the PATRIOT Act were:

(1) Under Section 213: the government can search a private property without notifying or getting prior approval from owner;

(2) Under section 214: the authorization of tracking and accumulating personal Internet content material and URL activities;

(3) Under Section 215: the government can gather and store personal data from records of third parties such as hospitals, schools and Internet providers;

(4) Under section 218: the FBI can perform, in secret, wiretaps and physical searches on US citizens without proved cause but rather only by “assuming” that the information gathered would be an evidence linked to a crime (Smith & Hung, 2010).

After 9/11, the large-scale terrorist danger ceased to be abstract and became more real and tangible. To ensure the prevention of the reoccurrence of such tragic events, the US government has taken unconventional extreme measures that go beyond what a democratic liberal country is “allowed” for. Intelligence gathering and law enforcement methods exceeded the “usual” and were permitted to conduct operations with no jurisdiction approval or oversight and with the only rational as being “relevant” (USA PATRIOT Act, 2001).

2.4 Surveillance practices in the post 9/11 era

The coordinated terrorist attacks on September 11, 2001 that targeted the Pentagon and New York marked a turning point in history and signaled an unparalleled increase in national security efforts within and also outside the US soil. With the influence and pressure of citizens seeking the security of the US and its citizens, the US government took radical action in what has been known as the "War on Terror," a term invented by President George W. Bush, and discussed earlier in the thesis. The 9/11 attacks on the US led to the invasion of Afghanistan on 7 October 2001, which evolved into America’s longest conflict in its history, gave way to new legislative measures in surveillance, under expressed intentions that it was needed to protect the nation and prevent future attacks similar to those of 9/11.

Following these events, the NSA had flipped the traditional way to a vaster technique of data gathering. The traditional way involved information collection about specific individuals believed to pose a threat to the US national security. However, the NSA now “gathers data on a huge number of people in large amounts and uses “mind-boggling”

capabilities of the intelligence community to sift through all the data looking for links to terrorism or other threats" (Fidler, 2015).

This collection of metadata can disclose a great deal of information about a person's behavior and personal life, even if a person poses no security issue whatsoever. Technology and the digital world we live in have helped surveillance activities develop immensely. This modern era development is a massive extension of a government's power and it requires legitimate justification in practice.

What makes the use of advanced technologies in mass surveillance activities a tricky subject, particularly in the political sphere, is that the technology used in it is evolving at an accelerated rate that can make it extremely difficult for proper legislation to keep pace (MacAskill, 2013). In the absence of laws and legal doctrine on these surveillance systems, illegal conduct appears acceptable merely because there has not been time to set down sufficient regulations to track it. Since national security is a big issue in the wake of the 9/11 attacks, many of the justifications used for the search and detention acts under the PATRIOT Act have been formed by relying on the environment of terror that pervaded American society in the aftermath of September 11. For instance, the fourth amendment specifies that people can't have an expectation that their "papers and belongings" will remain private after having given them to third parties. Under the new digital panopticon, most telecommunications are housed on the computers of a corporation, effectively rendering them kept in the possession of a third party.

In 1978, in an attempt to reel this kind of authority and power and avoid covert abuses like those disclosed by the Church Commission, the Congress banned intelligence surveillance within the US, unless having a warrant from the special FISA court. However, President Bush insisted that he has both the congressional and constitutional authority to pursue the surveillance program as he sees fit to protect American soil (Alden, 2006).

Being a conservative political advisor who served in the Justice Department for 12 years under the Ronald Reagan and Richard Nixon administrations, Bruce Fein believes that presidents should be granted significant discretion to defend national security in the way they see fit. However, if the President is unable to distinguish when something is out of bounds, despite the Congress' actions, Fein says that the President would then be establishing a principle of "trust me" as a measure to civil liberty, which is considered an impeachment. He states that President Georges W. Bush's rejection to abide by the law "is a direct assault on the separation of powers" (Alden, 2006). Fein claims that we can fight terrorism without compromising our fundamental system of checks and balances. "No one wants to downgrade the fact that we've got abominations out there and people want to kill us," Bill says, "but we should not inflate the danger, and we should not cast aside what we are as human beings" (Moyers, 2013).

The Bush administration claims that under the constitution, the President has the absolute authority to order unwarranted surveillance on US citizens in the interests of national security. The administration acknowledges that regular criminal investigations require a court's warrant but insists that security investigations come within the legislative authority of the president to maintain US security. The administration further claims that Congress' support in September 2001 for the US to initiate a counterattack on al-Qaeda has also allowed the President to use all necessary means, including interception of phone calls and e-mails in and out of the US. That approval, the administration claims, basically reversed the ban on warrantless intelligence surveillance by the FISA court.

Critics argue that such claims are clearly violating the law and constitution. In a letter addressed to Congress in January 2016, a team of 14 constitutional scholars, most of them previous senior government officials, said that the 1978 FISA Act was explicit in banning domestic surveillance without a warrant and that no other legislation had superseded it. The letter argues that should the administration see that the FISA act was inefficient, it should have

asked Congress to amend the legislation rather than disregard it. “The president cannot simply violate criminal laws behind closed doors because he deems them obsolete or impractical”, argues the letter (Alden, 2016). However, little has been done to alleviate the concerns of many whom believed that the risk for violating this power is strong.

As stated by Bloss and Stevens, an essential component of the social contract in the American constitution is the right to personal privacy. However, personal privacy was deeply challenged in the wake of 9/11, the rise of global terrorism and the development of surveillance tools that had to be conducted in secret even without the knowledge of legislative authorities.

While it has been established in the 9/11 Commission Report that the reason the US government had failed to prevent the 9/11 attacks was because of not sharing information among various agencies and failure to set the right goals at the executive level, the endorsed US PATRIOT Act has then allowed the extensive share of data between agencies, both vertically and horizontally (Kreimer, 2004). While this might enhance communication and collaborations between security and intelligence agencies, it further compromises the privacy of individuals as their personal data is now shared with a wider range of audience which makes it subject to scrutiny for reasons not previously applicable.

In conclusion, in the post 9/11 era, two concurrent mechanisms of "compromising citizens’ privacy rights" to the intelligence community forces have taken place in the United States. The first is the "transformation of the privacy system" or the process of modifying the constitutional norm in favor of more surveillance and a reduction in citizens' rights to privacy (Bloss 2007). The second is the technological development that has made it possible for intelligence services to carry out their assignments in ways that transcend operational legal entitlements. A very significant aspect of this process is that the compromising of identities by technology removes awareness, willing involvement and the consent of targets.

2.5. Supporters of mass surveillance

The main defensive argument on mass surveillance focuses on the value of the practice to any country's contribution to security, particularly in deterring terrorism and reducing or eliminating crime. As stated by Lyon, because emerging global terrorism operates in a developed technologically globalized world, the need to continuously grow surveillance tools becomes a crucial factor in the pursuit of safeguarding national security. Besides the security perspective, mass surveillance also provides an opportunity to control social unrest to create a more orderly nation. Allen (2008) and Walpin (2013) indicate that post the 9/11 tragic attacks, supporters of mass surveillance emphasized on the constitutionality of it and its necessity to prevent the reoccurrence of such events. Supporters of mass surveillance claim that there is a need to include up-to-date technologies to a government's infrastructure in order to facilitate the observation of both international and domestic communication (Inkster, 2014 & Toxen, 2014). They stress on the value of high-end and sophisticated technology in facilitating the government's security measures to keep away terrorists and safeguard national security. The success of modern technologies in gathering information and incorporating artificial intelligence is a step forward in enhancing security and reducing terrorism (Lomas, 2014 & Allen, 2008).

In addition, pro-surveillance groups argue that constraining mass surveillance has disadvantages when it comes to the efficiency and effectiveness of fighting terror and preserving information for current and future uses that can be used to prevent threats. For example, the Corporation for Community and National Service's General Inspector Gerald Walpin (in office from 2007 till 2009), indicates that the surveillance technology helps in identifying the phone numbers and codes used by the terrorists, and having this information is crucial for future cross-checking. Hence, his argument suggests that putting limitations on the mass surveillance policies will lead to contradictory regulations and obstruct the efforts of

nabbing terrorists (Walpin, 2013). By constraining the work of police and security agencies, they will have a difficult time dealing with the restrictions and fighting internal and external threats at the same time. In his article, Walpin claims that any attempt of putting the Intelligence community under oversight would jeopardize its effort in its "war against terror", which is a task already hard enough.

> "That enemy exists, the evidence for it consisting of 3,000 lives lost on 9/11, the Boston Marathon massacre, and even the unsuccessful terrorist attacks on our airplanes and at Times Square. The NSA program is logical. Our intelligence people know phone numbers or area codes used by terrorists in various world locations. Wouldn't you want our intelligence services to know who in the United States called those numbers and area codes and to examine the information to determine whether those calls were innocent or not? I certainly would. If this program had been applied to identify the Boston bombers, that attack could have been prevented".

One of the main limitations of mass surveillance is the overlapping nature of the process with personal privacy rights. Supporters of mass surveillance accuse their counterparts (those who oppose mass surveillance) for being too naïve and too politically correct. They even accuse them as being threats to the national security by always trying to promote personal privacy over national security. Walpin (2013) indicates that anti-surveillance groups are focused on privacy rights forgetting the benefits of the process. While mass surveillance has a negative impact on the privacy of individuals on social media or in their bank statements, the sophisticated systems beat this challenge by ensuring that they are safe from any danger to their lives (Scott, 2017). Therefore, the disadvantages of mass surveillance can be countered through continued use of sophisticated systems that are designed to pick out terrorists, as pro-surveillance groups argue.

2.6 Opponents of mass surveillance

The promoters of privacy rights are at the forefront of highlighting the limits and concerns of mass surveillance as they suggest that the process goes against the democratic

rights of U.S. citizens. Greenwald (2014) and Boghosian (2013) indicate that anti-surveillance advocates are putting pressure on ending mass surveillance as it is an abuse, overreach and abuse of power since it goes against the democratic rights. Gellman and Poitras (2013) highlight democracy as a tool that supports the people and aligns with their wishes and not with the desires of those in power. Anti-surveillance groups quote Abraham Lincoln on his tagline that democracy is a "government of the people, by the people, and for people."

The first wiretapping case against the NSA in 2006 culminated in a ruling in favor of the American Civil Liberties; Judge Anna Taylor ruled that the process was in violation of the Fourth Amendment. The ruling cited that the President had been given more power than necessary, prompting him to go against the set parameters in the Bill of Rights regarding the collection of information (Bamford, 2008).

In addition, numerous anti-surveillance advocates proclaim that it is the sacred right of the people to have their privacy protected and this should be the top priority over any expectation or demand concerning the actions of the government and state (Gellman & Soltani 2013). Anti-surveillance advocates indicate that the setting up of mass surveillance systems is ineffective and inefficient in dealing with terrorism, since there is increased collection of information which makes it difficult to filter through the data (Boghosian, 2013). Therefore, the process is illegal and goes against the goals of mass surveillance, since it is ineffective and prompts the collection of private information both domestically and internationally which is against agreed-upon human rights (Bamford, 2008).

On a different level, the increased mass surveillance and growth of technology for information collection and analysis is leading to abuse of power, detention, militarism and State secrecy. According to Greenwald (2013), who is the main recipient of the Snowden leaked insights, there is a growing rise in the assault of individual freedom and promotion of militarism. In the process of cross-checking the information and nabbing terrorist, the United

States has increased secret missions, grown radical executive power notions, detained people illegally and encouraged militarism. Greenwald describes the US intelligence agencies as non-transparent since the government has the limitless power to monitor the world, while it remains secret for the world to see its actions.

Anti-surveillance advocates raised a concern regarding behavioral conformity. They suggest that such surveillance could make citizens fear being watched all the time and that would lead them to act in a certain way. This means a loss of autonomy where individuals will refrain in acting in a unique way, that is according to their personality, and will act in accordance with what they expect as correct by the government. Peissl relates this conformity in behavior to the "panoptic society," where if people are aware that they are being surveilled, but can't tell when they are and when they are not, there is an impulsive power turn that takes place between the watchers such as the US government here and those being watched (civilians). Those in favor of this view claim that this loss of autonomy in democracies will most likely lead to a negative economic and societal results (Boghosian, 2013).

Other concerns related to the US government's surveillance acts, include views that the government misleadingly uses the cover of national security for the purpose of conducting surveillance of economic influence and diplomatic espionage. Several international relationships between the U.S. and their allies, are facing hardships due to international spying missions coordinated in the name of mass surveillance (Hakim, 2014 & Traynor, 2013). Anti-surveillance advocates point out that the United States is stretching their powers on international surveillance to collect insights for use in espionage with the allies to manipulate decisions. The process is not only a means of abusing the power granted to the country but also a development of an authoritarian totalitarian country as the amount of information against the other countries continues to increase over time.

From a legal perspective, there is no agreement on the constitutionality of the mass surveillance process and technology nor any parameters in place to prevent the violation of the Bill of Rights. While in his 2013 book, *The Supreme Court vs. The Constitution*, author and attorney Gerald Walpin strongly argues in favor of the necessity of government's surveillance, as a fundamental tool for fighting terrorism, his "opponent", Chief Federal Judge of the 2011 Foreign Intelligence Court, John Bates indicates that the secret surveillance projects conducted by the NSA have culminated in mass violation of the civil rights. Moreover, Bates acknowledged that part of the problem was the misrepresentation by the NSA officials in submission of cases to the secret FISA court.

This debate between supporters and opponents of surveillance has intensified significantly in 2013, when an ex-NSA contractor leaked classified files that showed the extent to which the U.S government has been conducting monitoring. In the next chapter, the study will introduce Edward Snowden, the ex-NSA contractor, and explain his actions and revelations.

Chapter Three

The Snowden Files

This chapter will begin by introducing Edward Snowden, his career timeline and some background information about his actions. It will also present his claim of justifying his act. The chapter will proceed to present some of the major revelations that were exposed through the documents he handed to journalists from *The Guardian* and *The Washington Post*. Revelations mainly discuss the major surveillance programs put in place post 9/11, their objectives and how they were used.

Up to this date, it is still debatable whether Snowden is considered a traitor who disclosed U.S secrets, or a patriot who exposed violations of the constitution. While his actions intensified the international debate over security and privacy, it is important to have a look at his background, understand his claimed motivations, and examine the exact nature and extent of his revelations.

3.1 Who is Snowden?

Edward Joseph Snowden, born in 1983 in North Carolina, is the man behind some of the most controversial revelations of the 21st century. In 2013, he unveiled vast surveillance systems, mainly led by the NSA.

Edward's maternal grandfather was a high senior official at the FBI and was at the Pentagon during the 9/11 attacks. His father, mother and sister also worked for the federal government.

In his early twenties, Snowden wanted to contribute in its fight against terrorism, and therefore joined the Army at the age of 20 (Greenwald, 2014). However, he was discharged

shortly afterwards due to injuring both legs and thus, landed his first job as a security guard at the NSA. He had never completed high school or undergrad studies, but he was able to study online and obtain a master's degree. Very soon, however, while attending a job fair focused on intelligence agencies in 2006, the CIA recognized the gift of Snowden working with information technology and security and offered him a job position. His role was in the global communications division at Langley. In his interview with Poitras, Snowden admitted that his tenure with the CIA had exposed him for the first time to the immense scope of work of the intelligence agencies.

In March 2007, with diplomatic cover, the CIA stationed Snowden in Geneva, Switzerland, where he was responsible to maintain the security of the computer network. After being assigned by the CIA to a U.S Permanent Mission to the United Nations (a diplomatic mission representing U.S. interests before the UN and other international organizations), Snowden resigned in February 2009. After that, he began working for private contractors such as the tech consulting firms Dell and Booz Allen Hamilton which are. During his work with Dell, Snowden was a subcontractor for the NSA office in Japan and then he was transferred to Hawaii. His task was to maintain computer systems, and this has obtained him a security clearance that gave him access to classified information.

As an NSA contractor, Snowden had access to highly classified information, and he had attained a collection of documents estimated to be around 1.7 million pages (Storhm & Wilber, 2014). He used keyloggers to catch coworkers' passwords and was able to access even more confidential information from their accounts. Although USB drives were banned by the NSA, Snowden managed to copy all the documents on USB drives.

During this time, he contacted *The Guardian* journalist Glenn Greenwald, documentaries filmmaker Laura Poitras and *The Washington Post* reporter Barton Gellman, to build channels in the aim of disclosing information through credible sources (Fidler, 2015).

In mid-May 2013, Snowden left his home in Hawaii and headed to Honk Kong to meet Greenwald and Poitras for the first time in the beginning of June.

3.2 What did he do?

On June 5, 2013, the first Greenwald story broke revealing the documents leaked by Snowden. Over the next days, disclosures based on the leaked documents Snowden handed to journalists continued to break worldwide. Stories from China, Brazil, Spain, Germany, the United States and the United Kingdom based on Snowden's leaked file appeared and produced overwhelming reactions. The disclosures created intense debates around diverse issues and heated controversies around matters that are heavy in substance, significance and scale. The revelations portrayed in the documents provoked reactions not only in USA but also in other countries as they showed that the NSA committed surveillance activities in friendly nations.

Greenwald explains in his book *No place to hide,* how he was one of Snowden's first contacts. Since 2005, Greenwald has vigorously sought to increase public awareness of the US government's drive against public privacy in the aftermath of 9/11, through the National Security Agency's activities. According to Greenwald, his long-standing history is what prompted Snowden to make him one of his first contacts in late 2012 under the nickname 'Cincinnatus.'

Snowden also contacted Laura Poitras, a documentary filmmaker and Greenwald's colleague (Maass, 2013). Poitras was behind several documentaries criticizing the behavior led by the U.S Government and its foreign policies, which made her subject to unwelcome scrutiny by the airport security and general US authorities. According to *The Guardian*, an article written by Greenwald titled "US filmmaker repeatedly detained at the border" about Poitras' regular struggle at the airport with intensive security checks, captured Snowden's attention in choosing them as his whistle blowing gateway (Greenslade, 2013)

After Poitras shared her encryption key, as asked by Snowden, he sent her documents detailing several government-run secret surveillance programs. Poitras also advised and assisted Greenwald in installing encryption on his account, enabling the two of them to communicate. The level of confidentiality and value of the passed-on information was so strong that Poitras became cautious about Snowden's real motive. Initially, she assumed it could be a secret agent trying to win her trust and reveal information about the individuals she had interviewed for her documentary, including Julian Assange, the founder of the infamous WikiLeaks. Therefore, Poitras needed to contact Snowden to verify the credibility of these top-secret documents (Maass, 2013). In the meantime, Snowden took leave from his current position in Hawaii in 2013 to treat epilepsy on the mainland, as he informed his supervisors. Instead, he left for Hong Kong and instructed Poitras and Greenwald to meet him there. He told them to meet him at a designated time outside a restaurant and he would be carrying a Rubik's Cube to help them identify him (Greenslade, 2013).

After the initial contact was made, Snowden instructed them to follow him to his room. In his room, Poitras began the filming of an interview between Snowden and Greenwald. Almost at the same time, the first report on the subject, "NSA collecting phone records of millions of Verizon customers," was published by *The Guardian* on 6 June, and began to catch everyone's attention.

Concurrently, Barton Gellman, a *Washington Post* journalist, made his first contact with Snowden as well. *The Washington Post*, however, missed a couple of the original documents that Snowden had not leaked to *The Washington Post*, as they were unable to reassure their publication in under 72 hours (Gellman, 2013). As a result of the turn of events, Greenwald (from *The Guardian*) had the opportunity to gain access to more documents on his own. Later, he revealed that at least 9000 to 10000 documents had been handed to him

(Germany, n.d.). However, even after a large number of media stories, *The Guardian* editor in-chief announced that only 1% of the document had been released in their newspaper.

3.3 Why did he leak the files?

Apart from being convinced by Glenn Greenwald that a publication to his findings will result in greater awareness about U.S-government mass surveillance, Snowden revealed his identity in the hope that people would focus on the process and not the person behind the leak. Snowden focused on leaking the information he sees relevant to the public, and which he was certain would not cause harm to any parties involved in the process (Greenslade, 2013). The first article published in *The Guardian* in 2013 specified that Snowden was confident that letting out the information would create awareness. Greenwald, MacAskill and Poitras (2013) echoed that Snowden wanted the United States citizens and other involved parties to realize what was being done to their privacy and against their will. The process sought to create discussions on privacy rights and the limits of mass surveillance as opposed to focusing on his process of acquiring the information. Therefore, the first justification for leaking the files was to enhance awareness without hurting the citizens or persons involved in the process and the government as well.

In the interview aired following the publication of the first article, Snowden made it clear that the sole purpose of leaking the insights was to bring to light the NSA violations of human rights to privacy that went against the restraints set out by FISA. In a statement, Snowden indicated that he wished to make the public aware that the U.S civil authority in collaboration with the Five Eyes—that is the U.K. Canada, Australia and New Zealand, in addition to the U.S—are encouraging the growth of mass surveillance with no restraints. Greenwald (2014) highlights that Snowden was clear that these states were keen on using the

excuse of security and citizen protection to prevent the citizens from realizing when the government infringe their liberties.

At the same time, knowing the authenticity of the documents gave Snowden the confidence to leak the data and provide a platform for discussing the future of mass surveillance. The information pointed out the intentions of the government and security agents in developing more data storage technology, collection systems and establishing a surveillance center in Utah. According to Greenwald (2014), Snowden was clear that the leaked files were authentic and showed the intention of creating repositories and catalogues for managing the huge amount of information available and expected in the future. “They protect their domestic systems from the oversight of citizenry through classification and lies, and shield themselves from outrage in the event of leaks by overemphasizing limited protections they choose to grant the governed... The enclosed documents are real and original and are offered to provide an understanding of how the global, passive surveillance system works so that protections against it may be developed” Snowden indicated (Greenwald, 2014). He claimed that his position at the NSA and conversations he had with computer experts resulted in his knowledge of various information and some of them appeared to go against the constitutional rights of the citizens. His idea was to empower the citizens to question policies and mass surveillance activities as much as he had learned to scrutinize them from a constitutional perspective (Greenwald, 2014).

Snowden mentioned an example of when the CIA attempted to recruit a Swiss banker to provide them with the classified financial transactions of people they claim to be under monitoring in the United States. Snowden explained how one of the undercover CIA officers identified the weakness of the banker through his communication platforms, befriended him, got him drunk on one occasion, and persuaded him to drive home. When the banker was arrested by the police for Driving Under Intoxication, the CIA agent offered him direct support in a number of ways, in return of the banker cooperating with him. Eventually, the recruiting

attempt failed, but the damage has been caused. "They destroyed the target's life for something that didn't even work out, and simply walked away", he said. Regardless of the plan itself, Snowden was bothered by how the agent bragged about the techniques he used to haul his catch, by lurking into the banker's private live through the internet. (Greenwald, G. 2014)

Snowden's efforts to make his superiors mindful of the problems in the field of information security and programs that he felt were unethical, were not handled nor addressed, and this increased his disappointment. The response he got when he tried to raise any issue related to that matter, was that this was not something under his scope of responsibility and that he did not have enough information to make such judgments. It is due to that, that he had developed a "bad" reputation among colleagues that his supervisors weren't fond of. "This was when [Snowden] really started to see how easy it is to divorce power from accountability, and how the higher the levels of power, the less oversight and accountability there was." (Greenwald, G. 2014)

Edward Snowden, as well as other privacy advocates, have expressed their view that keeping all data for an infinite period of time will lead to a lack of democracy when that power is abused:

> "Even if you don't do something wrong, you're being watched and recorded. The storage capability of these systems increases every year, consistently, by orders of magnitude, to where it's getting to the point you don't have to have done anything wrong, you simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer. ... The public needs to decide whether these programs and policies are right or wrong." ("You're Being Watched", n.d.)

3.4 What were his major revelations?

The first information regarding the NSA secret surveillance programs was leaked in 2005 (before Snowden) and created a huge controversy in the U.S. The leaks showed a secret domestic surveillance program put in place in 2002, shortly post the 9/11 attacks. This program,

authorized by then President Georges W. Bush, allowed the NSA to wiretap U.S citizens without getting a warrant. The NSA was authorized to intercept any communication coming from or to the U.S, as long as one party is outside American territory.

This authorization was criticized as being a serious violation to the FISA act and to the Fourth Amendment of the Constitution (see appendix A for the texts of the key US laws linked to the Snowden leaked files). The move to allow illegal searches in the name of dealing with terrorism resulted in an outrage from governmental officials whom believed the approach was unconstitutional and went against their democratic rights. However, the Bush administration has justified this program and its clandestineness by the "war on terror" necessity. The administration claimed that only the duration and time of connected phone calls were collected without capturing scripts and contents. However, this statement was challenged by what Snowden revealed in 2013.

In 2008, FISA implemented amendments to accommodate the infringements as opposed to completely taking away the powers from the NSA to search persons suspected of terrorism. The amended law served as a reference to distinct between what is considered the "U.S people", which are the people residing on U.S. soil, citizens, legal residents, and other people. For the NSA to be able to tap into the "US people" calls and emails, it was required now to get an individual FISA court warrant. However, no warrant was required from all other people that do not fit into the category of "US people" no matter where they reside and even if they are communicating with "US people" (Greenwald, 2014).

The Snowden's revelations had disclosed a great deal about the NSA, its activities in terms of mass surveillance and the oversight offered by the President's administration, Congress and FISA court.

While the 2008 FISA amendments put in place post the 2005 scandal were supposed to restore the trust of American citizens in their political order, the Snowden files showed that the

government was still able to find ways around the new amendments to conduct domestic monitoring.

As per the 2008 FISA amendment, the NSA is required only once a year to present its targets list for the year to the FISA court to get approved warrants. However, there is no need to convince the court that the target is guilty of something, nor address the reasons behind suspicion of the target. The only thing needed is to claim that monitoring this individual would support data gathering for “legitimate foreign intelligence analysis". Furthermore, there is no need to filter out the US citizens who end up being monitored along the process. Whenever, the NSA gets the yearly approval from FISA to monitor the targets, it can proceed with gathering all sort of communications needed and thus order internet service providers to handle them any data of all non-US people, and surprisingly, US citizens and people legally residing in the U.S. In 2015, it was revealed that FISC hasn’t denied any of the 1457 requests of surveillance made by the NSA and FBI.

The Snowden files showed that under “Section 702” of the secret FISA court, the NSA is permitted to target non-U.S. persons residing outside the country. However, this means, if a U.S. citizen on American soil is communicating with someone residing outside, the NSA has the right to collect, use and disseminate the communication (Fidler, 2015).

Furthermore, “Section 702” also allows the NSA to engage in mass or bulk surveillance of foreigners’ communications outside the U.S. from inside the U.S (such as a foreigner located in Europe using Gmail). Snowden believes that this violates international laws and human rights to privacy. For this reason, the Snowden disclosures had a large impact on the international level as well.

While American citizens thought that the unwarranted domestic surveillance program authorized by the Bush administration ended when it was made public in 2005, the first article published by *The Guardian* on June 6, 2013 regarding the Snowden Files showed that the

Obama administration has also ordered the telecom company Verizon to handle the NSA all call data of US customers. *The Guardian* published a copy of the order that showed how under the Obama administration, the communications records of millions of Americans are being collected in bulk on a daily basis-regardless of whether they innocent or suspected of anything. This order was granted by the FISA court and bluntly forbids the company (Verizon) to disclose to the public that intelligence agencies are collecting their phone records.

The court order also shows how two U.S senators (Mark Udall and Ron Wyden) have been trying to raise public awareness about the scope of surveillance practices under the Obama administration. "We believe," they said, "that most Americans would be stunned to learn the details of how these secret court opinions have interpreted the "business records" provision of the PATRIOT Act" (*The Guardian*, June 6, 2013).

While it was previously argued by the Bush administration and later the Obama administration (post Snowden), the collection of phone records of Americans is not considered unconstitutional because it is not covered by the Fourth amendment. Phone records and toll data do not include content and citizens do not have a valid reason for expecting this info not to be disclosed. However, as revealed by the Snowden files, email metadata is different and is definitely unconstitutional. Through emails, intelligence agencies can access private contents.

According to the documents published by *The Guardian*, the collection of American's emails records began in 2001 under the Bush administration as a program called "Stellar Wind". This program did not rely on any court for authorization but was not allowed to capture and analyze email records from communications solely transmitted inside the United States. Upon revolts in 2004 made by senior officials in the Congress, Bush had to discontinue the program. However, only two months post it discontinuation, the FISA court chief legally authorized internet metadata.

While this email metadata system was restricted by the scope of which the NSA could analyze the bulk of records, a memorandum leaked by Snowden shows how the NSA sought to remove those restrictions and expand the scope of the system (*The Guardian*, June 27, 2013). The memorandum states that "giving NSA broader leeway to study American's online habits would give the agency greater visibility into the online habits of foreigners".

Upon approval, this program expanded to become the basis of much more sophisticated surveillance systems such as Boundless Informant.

Snowden revealed the presence of a data mining framework known as 'Boundless Informant' which is implemented for the sake of phishing information from computers and telephone networks (Greenwald, MacAskill & Poitras, 2013). The leaked files indicate that the Boundless Informant is a critical component in data collection due to the collaborations between the U.S and other intelligent partners conducting mass surveillance. On a different level, the documents revealed how the use of the Bullrun technology enhanced the mass surveillance activities by creating an opportunity for closer monitoring which may result in a breach of privacy (Borger, Ball, 2013).

Other technologies also revealed in Snowden's leaked insights include the use of the PRISM program which encompasses the monitoring of social media platforms and collecting as much information as possible. Secondly, it is the XKeyscore, which gave the NSA agents the ability to collect insights from anyone's email communications, social media accounts or browsing history, only with little resources as their personal emails. An agent with only an email address, can access someone's private life.

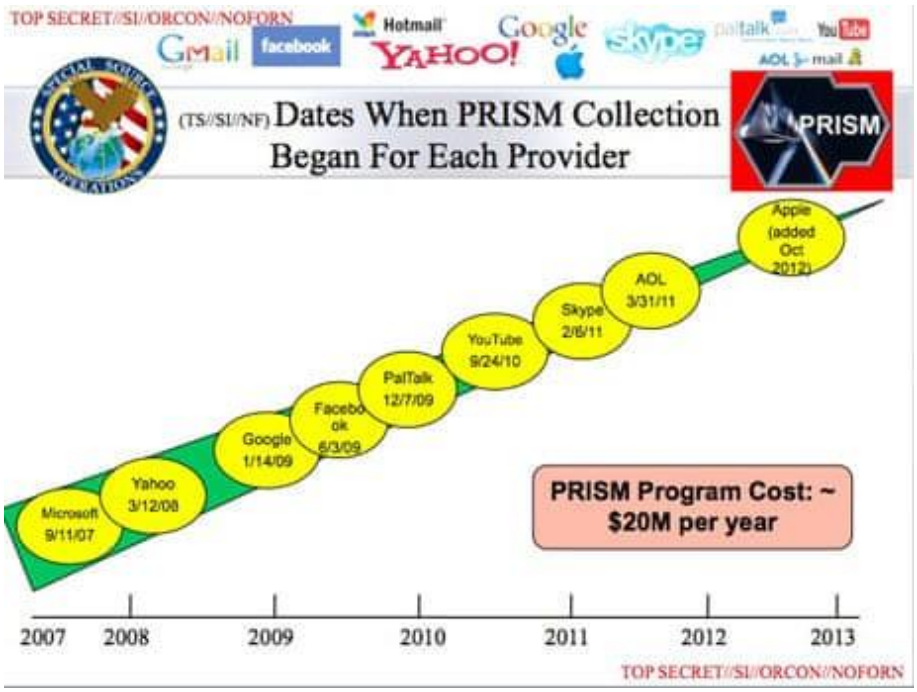
The programs revealed by Snowden, that had the largest impact, are explained in the following:

PRISM:

PRISM is a surveillance program used by the NSA to gather data in real time from big service providers in the US that comply with court-approved search terms. These providers

include, but are not limited to, Google, Microsoft, Facebook, Yahoo, Skype, Apple and YouTube. With the escalating internet use and rise in the quota of subscribers, the PRISM framework proves to be an effective approach in accessing mass insights at a go from the various internet platforms from across the globe. The NSA focused on defending their PRISM strategy based on the legislations enforced after the 9/11 tragedy that allowed the U.S. to monitor sites. The legislations allowed for limitless and unwarranted surveillance of both foreigners and citizens making it easy for the NSA and other agencies to collect information or violate rights (Levi & Wall, 2011). The regulations and the proposed or implemented technologies culminated in major complexities that caused concerns for internet users, although the NSA was benefiting from the continued internet use and rising number of subscribers.

In the aftermath of 9/11, and by the endorsement of the U.S government, unwarranted surveillance was made possible, which provided the NSA with expansive powers to track Americans and with nearly limitless authority to carry out unjustified mass surveillance of foreigners.

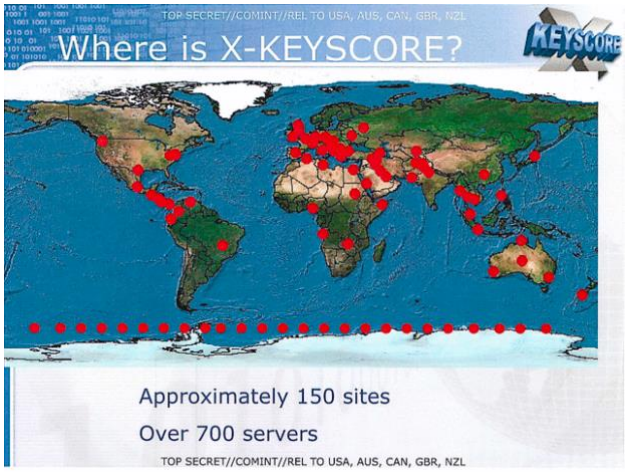


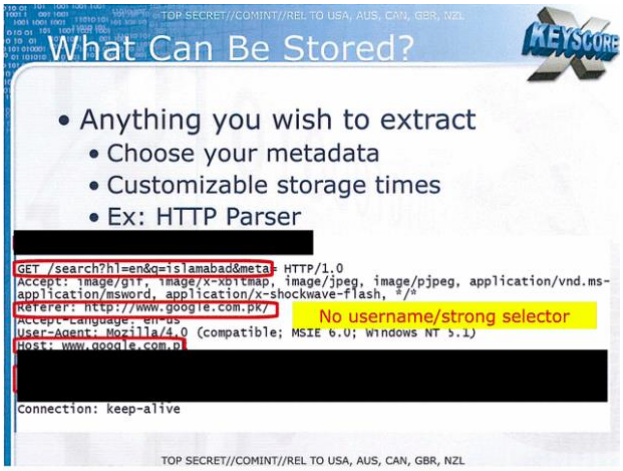
Source: NSA's Prism program taps into user data of Apple, Google and others. The Guardian. 2013

XKeyscore:

XKeyscore is a previously secret computer system built to search and analyze Internet communications on a large scale. Intercept's article called it a "powerful spy system" with 700 servers across 150 sites across the world storing data for a few days and metadata for up to 30-45 days (“XKEYSCORE: NSA’s Google for the World's Private Communications,” n.d.). XKeyscrore was also used to collect employee contact data to steal millions of cell phone encryption keys from Gemalto, which is the largest SIM provider.

NSA agents with the right level of authority could make any query by filtering information in real time. As Edward Snowden said, he would wiretap virtually anybody without any supervision whatsoever. The filter parameters are referred to as "selectors." This may be a username or an e-mail address for a particular person. (Greenwald, 2013b)





Source: XKeyscore presentation from 2008. The Guardian. 2013

Collecting text messages:

On 16 January 2014, *The Guardian* published an 8-pages article about the NSA's bulk text message collection program called DISHFIRE. The article revealed that the NSA has received 200 million messages every day. They were used to obtain useful data, such as location (including border crossing or other location specific messages), communication networks (building call chains by examining who first called by looking at missed calls) and financial transaction information (e.g. use of credit card). The documents also note that NSA is able to conduct searches in this broad database without any warrant. (Ball, 2014)

Intercepting and collecting phone calls in some countries:

On 19 May 2014, another series of revelations indicated that all phone calls were recorded in the island nation of the Bahamas under the SOMALGET program. According to the documents presented by Snowden, this program is part of a high-classified system that has been enforced without the awareness or permission of the government of Bahamas. The NSA seems to have used access legitimately gained in partnership with the US Drug Enforcement Administration to access a back door to the country's cell phone network allowing it to secretly monitor and record "full audio" of any mobile phone call made to, from and inside the Bahamas - and can be stored for one month (Greewald & Devereaux, 2014). SOMALGET is an advanced application that runs under a more general Mystical counterpart that, in turn, "only" captures metadata. Mysterious mobile phone interceptors were also found on US soil in 2014. A team of researchers using a hardened smartphone named Cryptophone noticed that 19 cell phone towers redirected calls and even made it possible to install spyware on devices within their range. (Levine, n.d.). The FAIRVIEW software was also used to spy on foreign countries under the authority of the Transport Authority.

Taping Google and Yahoo data center links:

The NSA have secretly broken into the main communication channels of the world's largest e-mail providers, Google and Yahoo. The companies were shocked by this surreptitious action and started to introduce end-to-end encryption beginning in 2014 (Rushe, Ackerman & Ball, 2013).

Cracking encryption and undermining Internet security:

On September 21, 2013, it was disclosed that the NSA supported poor security regulations through the American National Institute of Standards and Technology (NIST), and providers such as RSA (Arthur, 2013). Service provider cooperation at this level sent a clear negative message to customers and caused major harm to RSA 's image, as trust is mostly about the security in this particular industry.

Spying on foreign countries and world leaders:

A report released in June 2013 revealed that the NSA used a wide array of spying techniques, including bugs embedded in electronic communications gear to tap transmission cables with advanced 'antennae' to collect information from the offices of political alliances (such as the EU), embassies of adversarial and even 'allied' nations. Angela Merkel, the German Chancellor criticized this behavior, which led to an increased criticism over the US policies in treating allies as adversaries.

Intercepting and collecting phone records in bulk:

Under the Foreign Intelligence Surveillance Act (FISA), secret court orders have allowed the NSA to sweep American call records since 2007 (Greenwald & Ackerman, 2013). But even before that, the bulk data collection involving foreign countries was dated back to 1985 as part of the FAIRVIEW program. The very first disclosure of the Snowden Files on June 6th, 2013 was through an article published by Glenn Greenwald that detailed how Verizon was forced by the government to hand the NSA call data from millions of US citizens on a

daily basis. This includes, for example, who called whom, from where, and when. The importance of such data is often underestimated by the NSA but is very important because it provides a context to human relations and circumstances (MacAskill, Dance, Cage, Chen, & Popovich, 2013).

See Appendix B for summary of the programs.

With this brief on the surveillance programs developed by intelligence agencies in the post 9/11 era, the next chapter will provide an analysis of the purpose these programs served as revealed through the leaked documents.

Chapter Four

National security or overreach of unconstitutional power?

The need for “special power” and the call for expansion of mass surveillance methods in special times, such as the fight against global terrorism, has long been argued that it can be seen as a way to promote and legitimize overreach of power (Kitrosser, 2007).

Before Snowden, even legally approved surveillance practices were debatable. However, post Snowden’s revelations, it turned out that the actual conducts of intelligence agencies have went far beyond what is legally approved. In fact, as shown in the leaked documents, one can criticize the surveillance practices as being not only unconstitutional but also an abuse of power. The main reason why these surveillance systems can be seen as unconstitutional is for the fact that they conduct unauthorized mass data gathering and storing on innocent people, which goes against the foundation of a liberal society. Also, the lack of effective checks and balances raises concerns about the possibility of abusing such a powerful system for purposes such as economic or diplomatic dominance.

Even with all the scrutiny and criticism, the NSA continued to strengthen its unwarranted global surveillance programs long post 9/11. The NSA sticks to its argument that the mass surveillance activities and systems are designed to meet the interests of the people and that is the bottom-line. However, in January 2014 in an interview with Snowden aired on the German Television, he criticized the NSA for carrying out these operations for “industrial espionage”. In one given examples Snowden clarified, "If there's information at Siemens that's beneficial to U.S. national interests, even if it doesn't have anything to do with national security then they'll take that information nevertheless" (Kirschbaum, 2014). In addition, programs such as "Black Pearl" were designed to track private networks of large companies, and their real goal of protecting national interests was somewhat unclear (Watts, 2013).

When journalist Glenn Greenwald wanted to publish the first article about the Verizon court order, in which the US government asked the Verizon cell company to provide all phone data of American, he was told by *The Guardian* that he'd need to inform the government and get their approval before publishing. When the government tried to complicate things and act as a joint editorial partner to determine what to publish and what not, Glenn claimed that it was then that he realized that the government had no viable national security case against the Verizon report, which is a simple court order that shows how American telephone records were collected. Greenwald (2014) emphasized that publishing this article would have only created public awareness for the American citizens and wouldn't have served any terrorist group as the government claimed. He argued that the government claiming that this article would benefit terrorists is ridiculous as terrorists are well-aware that they are obviously being surveilled.

A major feature in Snowden's revelations involved exposing the agency's espionage on foreign countries not considered as "enemies", rather fellow democracies and close allies. Also, it was shown that NSA spied on international institutions such as the United Nations (UN) and the European Union (EU). The agency's briefing slides provided for example prove that the government surveilled and spied on Brazil's national oil company (Petrobras) and political leadership. The Petrobras revelation urged accusations against the U.S government's engagement in economic espionage which it had long denied doing. Snowden also revealed information about the U.S surveillance activities on international institutions and their meetings, such as the International Atomic Energy Agency, Summit of the Americas, the European Union, UN, World Bank, Organization of Petroleum Exporting countries and the Climate Change Conference.

An article published in October 2013 by the German newspaper Der Spiegel based on the Snowden provided files, showed evidence that the NSA had been tapping and monitoring German Chancellor Angel Merkel's phone since 2002. The documents proved what seemed to

be a targeting record of Merkel from an NSA database generated from a program named SYNAPSE that analyzes communications of foreign intelligence targets. A previous leaked file also disclosed that the NSA had engaged in surveillance of mass German's communications.

By looking at the list of individuals whom were targeted by extremely intrusive surveillance, the Snowden leaked documents shed light on the overall goals and strategy of the NSA. The list of targets found in the files ranged from criminal suspects and terrorists to elected leaders of friendly democratic nations and allies. Even ordinary American citizens were on that list with no apparent reason.

While only little parts of the surveillance strategy exposed in the Snowden files were targeted at eliminating terrorism and safeguarding national security, a closer examination at the files shows that the government had indeed used these surveillance programs for matters beyond national security, such as suspicion-less surveillance aimed at entire population, economic and diplomatic espionage (Greenwald, 2014).

While the NSA and President Obama have responded to the Snowden leaks by indicating that the surveillance policies and activities are only keen on promoting national security, there is mass justification of the collection of information for other reasons. It is already quite apparent that many of the agency's operations have had very little to do with any anti-terrorism efforts or even national security concerns. The leaked files shed light on the presence of economic espionage, eavesdropping and e-mail surveillance directed at Petrobras, the Brazilian oil giant, espionage on energy firms in Mexico and Venezuela and economic conventions in Latin America. Also, the Snowden files proved that the NSA allies-such as Canada, Norway and Sweden- also conducted surveillance on the Brazilian Ministry of Mines and Energy, and several energy companies around the world. One specific file showed

information gathered on SWIFT banking system, Petrobras, OPEC and AZPROM (a Russian oil company) (Poitras & Stark, 2013).

Additional evidence of the NSA's economic interests can be found in the PRISM document that shows a sample of the “Reporting Topics for week 2-8 February 2013”. The list of types of information collected from different countries certainly includes financial and economic categories, such as energy, trade and oil. As per reported by The New York Times, “financial institutions, heads of international aid groups, foreign energy firms and a European Union official engaged in anti-trust battles with American technology companies" were all targets listed in the NSA surveillance documents (Greenwald, 2014). The New York Times added that British and US agencies have also surveilled the communication of EU senior officials, world leaders (such as African heads of state and their family members), United Nations directors, and officials in charge of managing finance and oil ministries.

The reasoning behind economic espionage is obvious enough according to Glenn. Technically, the United States will gain a competitive advantage for its industries when it uses the NSA surveillance tools to figure out the planned strategies by other countries ahead of an economic or trade negotiation summit. One of the leaked documents stated that in 2009, the Assistant Secretary of State Thomas Shannon sent Keith Alexander, the NSA director a gratitude letter, thanking him for the amazing intelligence that was provided to the State Department before the 5th American Summit (a conference to discuss economic agreements). In his letter, Shannon bluntly states that it was thanks to the intelligence provided by the NSA that the USA was able to bargain benefits over other countries: “The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.” (Greenwald, 2014).

In another leaked document named “political affairs” published in year 2011, there is evidence that the NSA had also monitored Dilma Roussef which is the Brazilian President and Enrique Nieto which was at that time the leading presidential candidate in Mexico. The document shows how very personal information was collected on these two Latin America leaders.

There is no question as to the reasons why Brazil and Mexico were targets of the U.S, since they are the leading countries in the oil industry and they have a strong presence in the neighborhood of the U.S. While they might not be the “enemies”, they are definitely not friends of the U.S. Indeed, one NSA document, named "Identifying Challenges: Geopolitical Developments for 2014-2019", both Brazil and Mexico showed under the heading "Friends, Enemies or Problems?" (Greenwald, 2014). Others listed in that document are India, Somalia, Sudan, Yemen and Turkey as well.

The go-to argument for the supporters of mass surveillance is that this kind of surveillance is the only way to ensure the prevention of terrorist attacks on American soil and globally. However, history shows that using an external threat to validate the government’s powers ahead of the public is a strategy used. For more than a decade, the US government has “hailed the risk of terrorism to justify a number of radical activities, from torture to assassinations and even the invasion of Iraq” (Greenwald, 2014). To put it in a more fashionable way, the US policymakers have created the term “war on terror” post the 9/11 attacks as argued by Glenn. This term is more of a slogan that sells easily rather than a viable argument or reason. By taking a look at what was revealed in the Snowden files, it is easy to conclude that most of the collected data had little to do with terrorist activities and national security. Thus, gathering this huge amount of data becomes questionable. Why has the U.S.

surveilled the Brazilian Petrobras company? What did it have to do with national security and terrorist attacks? What about the World Economic summit?

In addition, documents show the extent to which “normal” American citizens were also subject to unjustified surveillance and the same goes for leaders of friendly allied nations. This then suggests that monitoring and collecting metadata activities exhibited by intelligence agencies had nothing to do with preventing and stopping terrorism. It becomes easy then to conclude that the NSA had used the “war on terrorism” as a pretext for conducting extensive unjustified surveillance (Greenwald, 2014).

Furthermore, the claim that mass surveillance stopped terror attacks – a claim made by President Obama and a number of national security officers – has proven to be inaccurate. As *The Washington Post* reported in December 2013 in an article titled "Officials Defenses of No Phone Program may be Unraveling?", the federal judge ruled that the telephone metadata collection program is certainly unconstitutional and claimed that the Department of Justice has not been able to provide on example of an incident in which analysis of the mass data produced by the NSA was able to successfully stop a possible terrorist attack in the country (Nakashima & Miller, 2013).

In addition, Democratic Senators Martin Heinrich, Ron Wyden and Mark Udaal who are all members of the Intelligence Committee, have bluntly confessed through The New York Times that indeed mass surveillance has not enhanced the government’s capacity in fighting terrorism. The argument that mass surveillance would be the answer to the issue of terrorism showed to be exaggerated. There was no apparent proof whatsoever that mass data collection has indeed been an unmatched, unique tool in safeguarding national security. The NSA failed to come forward with any cases that detail a time when mass surveillance was successfully used in stopping a terrorist attack, despite being asked many times by some Congressmen.

There was no convincing instance where warrantless mass surveillance solved a problem that a normal court authorized order couldn't have.

The centrist New American Foundation think tank has conducted a research to examine the credibility of statements made by officials who argue that mass data collection was efficient in safeguarding national security. The research however determined that the program "has had little noticeable impact on the prevention of terrorist attacks" (Nakashima, 2014). As an article published by *The Washington Post* states, it was instead the traditional conventional investigation methods that proved to be the most efficient in providing tips to help stopping an attempted terrorist attack.

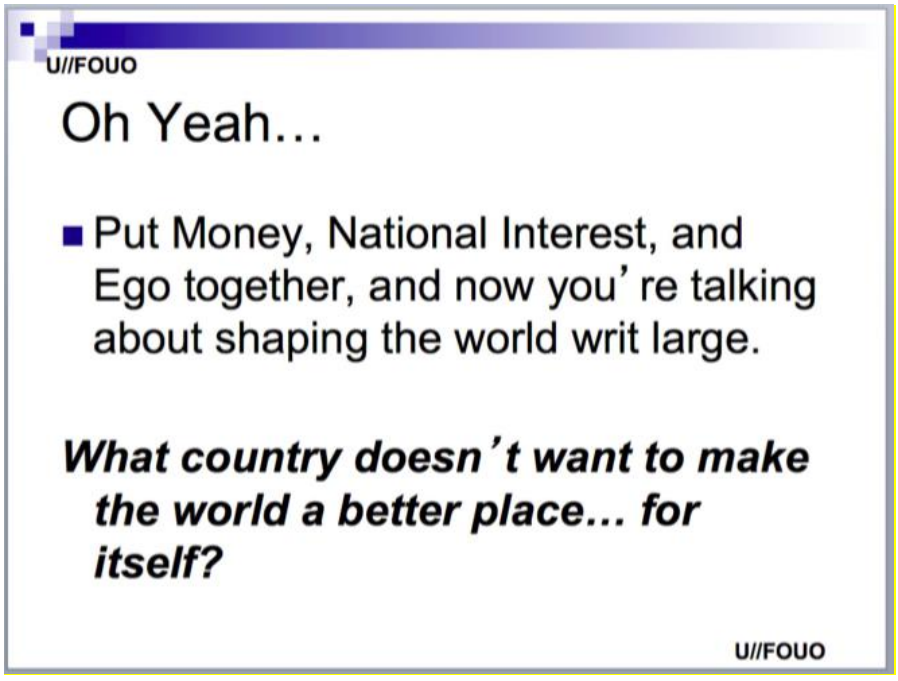
The research states that the "collect-it all" approach has in fact failed to prevent many terrorist incidents such as the Boston Marathon in 2012 bombing, and it had also no input in stopping the planned attempted attacks such as the Time Square Explosion or the Christmas-day bombing of a jet. Both these incidents were prevented due to traditional police operations and warnings made by the public.

An Al Qaeda analyst in the New Yorker, Lawrence Wrigth argues that it is not accurate that the reason 9/11 wasn't stopped is because of the lack of information and that a mass data collection system could have prevented it. Instead, he claims that the CIA had retained crucial information from the FBI and this lack of communication hindered the FBI from taking the right actions to stop the attacks as being the sole authority to address threats on American soil and overseas.

Wright claimed that has the CIA coordinated with the FBI, the latter might have stopped 9/11. The NSA had a warrant to track all Al Qaeda members with a tie to America: It could track them, access their phones, hack their computers, read their e-mails, and get hand on their bank, medical and credit cards data. The NSA had the right to ask the telecom companies for detailed records of any calls Al Qaeda members have made. Hence, there was no need for a

mass-data collection system, collaboration between government agencies was required instead. The government had the requisite information on its hands but had failed to grasp or act on it.

There is surprising frankness within the NSA about the actual intent of constructing such a huge secret surveillance system. A PowerPoint presentation prepared by an NSA/SIGNIT National Intelligence Officer in the department of Science and Technology designed to be used in a meeting to discuss the future of International Internet Standards has a very straightforward title: "The Role of National Interests, Money, and Egos". The Officer who prepared this presentation claims that when you put these three elements together, you get the secret of the success of the U.S. ability to maintain its global surveillance dominance status (Greenwald, 2014).



Source: No Place to hide (page 166)

Since its establishment, the Internet has been declared an unparalleled platform for liberalization and democratization. Yet, in the view of the US, this global network and other forms of communication infrastructure pose a threat on American influence and power over

the world. Greenwald claims that when you look at the matter from this point of view (as shown in the above slide), the mass data collection programs used by the NSA begin to make sense. For the purpose of controlling all aspects of the Internet and communication channels, the U.S had to make sure all is captured and assessed by its agencies.

Undoubtedly, beyond economic gain and diplomatic manipulation, a structure of systematic surveillance enables the United States to keep its hold on the globe. Whenever the United States is capable of knowing what everybody is saying, doing, planning or thinking, its control and power over all factions is amplified. This is twice as valid when the government works at a high level of confidentiality. Secrecy builds a one-way mirror: the US government knows what others in the world are doing, including their own citizens, while no one knows its actions. It is the supreme inequality, allowing the most destructive of all human conditions: the exercise of absolute power without oversight or responsibility (Greenwald, 2014 & Fidler, 2015).

Chapter Five

The Snowden Effect

This chapter presents the US government's reaction and defense against the accusations pointed towards its alleged overreach on its soil and globally. It will discuss the political implications of the Snowden files on domestic U.S. politics and how the Obama Administration reacted following the disclosures. This chapter will also discuss the international response to the actions leaked by Snowden, especially from Germany and Brazil, states that are considered allies of the US.

5.1 Implications on domestic U.S. policies and political order

The documents leaked by Snowden have indeed revealed that the U.S. has been exhibiting some elements of a surveillance state, that are not only targeted at safeguarding national security. These practices have undermined the democratic liberal principles and have threatened the liberal state in the U.S. Given the emphasis on Western liberal legal traditions, it is not shocking that public debate usually begins on the topic of privacy as it is a fundamental element in liberal democracies. Understood as a civil right, it encompasses elements of democratic politics, such as freedom of speech. The Snowden disclosures can be interpreted as an attempt to control communication which is clearly a threat against values upon which the United Stated was formed. Hence, given the aforementioned statement, it is important to establish the ethics of mass data activities that resolve the growing distance between data and individual privacy (Amoore, 2014). Provided that privacy is still the prevailing mobilizing principle of resistance to excessive, unreasonable or unlawful surveillance, the actions of those

advocating technological restrictions, such as encryption, or who can re-infuse the concept with material suitable to the world of mass data are definitely welcome (Stoddart, 2014).

The solution to mass surveillance is not to fully remove it, but instead, to go back to targeted surveillance that's directed only to those which hold significant evidence that they are engaged in something that could harm national security. It is more efficient to use targeted surveillance, as it proved to be more effective in preventing terrorist attacks than the "gather it all" strategy that overwhelms security agencies in so much evidence that it cannot be quickly sifted by investigators. Indeed, after the surveillance abuses revelations exposed in 1970s by the Church Committee, it was exactly this concept that the government had to present some proof of suspected wrong-doing before it could listen to an individual's conversations-which is what initially contributed to the creation of the FISA court. Needless to say, the court was turned into a rubber stamp, and did not provide any substantive judicial review of the government's surveillance demands. Yet, its basic idea is still valid and shows a way ahead: to turn the FISA court into a genuine judicial structure, rather than a one-sided set-up would be a good reform. By making the watchers watched as well, responsibility and accountability take place.

The controversies that arose post the Snowden revelations, led President Obama to launch a detailed investigation to examine the impact of secret mass surveillance practices on the liberal democratic state. In 2014, after reviewing the proposed reforms made by the “Review Group on Intelligence and Communication Technologies”, President Obama recommended that Congress retain the mass storage of metadata, but place ownership of its large databases in the possession of non-government groups such as telecommunications companies. The government can access these private databases only for national security purposes and upon providing reasonable suspicions based on facts. The Congress addressed his propositions and some members voted in favor of it, while others called for its elimination.

Another recommendation made by the review committee is to restrict the FISA court's ability to force private companies to disclose data to intelligence agencies.

In June 2015, Congress passed the US Freedom Act, an agreement that President Obama immediately adopted, and which addressed crucial amendments. Under this new law, the NSA could no longer gather meta-data, but could obtain access to the records held by telecommunication firms by an order of the FISA Court only if it could prove that it had a reasonable suspicion that a suspect is linked to terrorism. Every 18 months, telecom companies must destroy the metadata stored. Officials with security clearances can bring questions of civil liberties or privacy before the FISA Court, and important decisions of the FISA Court will be made public.

On 14 June 2013, U.S. federal prosecutors filed a criminal lawsuit against Snowden, charging him with three felony convictions: theft of government property, and two counts of violation under the Espionage Act, by unlawful dissemination of national security information and the deliberate communication of confidential intelligence documents to an unauthorized individual. His passport was retracted from him as he was trying to flee Hong Kong. Snowden has been in Russia under political asylum since 2013.

The intense debate about Snowden's revelations had since 2013 been in the back and forth arguments about why the NSA did what it did. While Snowden's supporters, international leaders and NSA critics, emphasized that there is clearly abuses of power and violations of laws and human rights, defenders of the NSA kept on insisting that the oversight exercised was only in favor of safeguarding the nation's security interests while ensuring privacy rights.

For it to be able to provide unquestionable safety to its citizens and its soil, the US government believes that expanding surveillance tools is crucial to reach the goal and it confirms that over the years the data gathered by in the intelligence community was indeed

vital in preventing terrorist attacks. The US government argues that for the purpose maintaining the efficiency and effectiveness of these surveillance programs in dealing with threats, they must be kept a secret because any leaks would benefit adversaries and cause harm. This point is however debatable according to Glen Greenwald, the journalist whom Snowden handed the documents to, as no proof in the files show that the U.S. government did indeed use the data generated from these programs to stop a terrorist act.

Although the US government has not cited a single case in which the NSA's mass data archive has helped prevent a terrorist attack, Snowden's disclosures reversed the risky dynamic by throwing light on the system and how it works (Greenwald, 2014). After these revelations, the world realized, for the first time, the extent to which the surveillance programs have developed and are being used to intrude on their private lives. Because the topic of surveillance is always contradictory to what a democratic liberal government stands for, the NSA leakages have started a controversial extreme debate worldwide. They have also sparked calls for change and a global debate on the value of Internet rights and privacy concerns in the digital world and have shed the light on a critical question: what does unrestricted surveillance mean for us as people, inside our own lives?

These revelations have also increased the lack of trust people have for any statement released by a U.S. governmental official and has reshaped friendly relations between nations. It didn’t take too long until someone from within the executive branch took action. Two weeks after the news, two Congressmen have jointly presented a bill asking to defund the surveillance programs under the NSA. The two Congressmen were Justin Amash, conservative Tea party member and John Conyers, a Democrat from Detroit. Amash and Conyesrs were very different as in their backgrounds, but they found common ground in their stand against the NSA's surveillance techniques, especially the domestic aspect of it. Their initiative immediately received tens of co-sponsors across the social spectrum, from the most conservative to the most

liberal, and all in between – a very unique case in Washington. One House member after another took a stand to strongly oppose the NSA program, rejecting the concept that to prevent terrorist attacks, the NSA needs to monitor calls on all American citizens. It was perhaps the most powerful challenge for the state of national security to arise from Congress ever since the 9/11 attacks (Greenwald, 2014).

In response to the NSA's spying on Germany revelations, a friend of the USA, President Obama claimed that he wasn't aware of the latter and explained that either the agency was out of control or that the activity of spying on a top leader from Germany was not that much of an important case to rise to the president.

Regarding the Petrobas disclose, James Clapper, the director of the NSA back then, acknowledged that the NSA did indeed collect financial and economic intelligence, but only for national security purposes. He claimed that the U.S. does not steal foreign companies' secrets to benefit American companies, which was hard to believe given that one of the Snowden files showed that the U.S intelligence community needed to engage in "technology acquisition by all means", including cyber operations against foreign researchers and companies, in order to maintain U.S. leadership in technology and innovation. (Cate. 2015)
Yet, in a press release, on September 8, 2013, James Clapper tackled the allegations of Economic Espionage by stating that:

"It is not a secret that the Intelligence Community collects information about economic and financial matters, and terrorist financing. We collect this information for many important reasons: for one, it could provide the United States and our allies early warning of international financial crises which could negatively impact the global economy. It also could provide insight into other countries' economic policy or behavior which could affect global markets. Our collection of information regarding terrorist financing saves lives.
What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of-or give intelligence we collect to-US companies to enhance their international competitiveness or increase their bottom line."[2]

[2] Source: Office of the Director of National Intelligence, http://www.dni.gov/index.php/newsroomIpress-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations -of-economic-espionage

5.2 International response and U.S. international relations

The revelations that the NSA spied on friendly nations, proved very embarrassing to the U.S government and damaging to its foreign policy and joint relations with the involved countries. Germany and Brazil reacted angrily to what showed in the leakages about spying on their leaders, German chancellor Merkel and Brazilian President Rousseff.

The disclosures about German Federal Chancellor Angela Merkel's phone prompted Germany to engage in the efforts to strengthen the rights to privacy in the international law and terminated a Cold War-era agreement with the U.S intelligence community. This deteriorated the US-German relation in general and on intelligence specifically (NSA: New Reports in German Media Deepen US-Merkel spy row-BBC News, n.d.). As a consequence, the German government did not renew the contract with Verizon and expelled CIA's station chief in Berlin (Fidler, 2015).

The UN General Assembly collectively voted in favor of the resolution – proposed by Germany and Brazil – that acknowledges the online privacy as a fundamental human right, which an analyst explained that this was a message to be sent to the United States that it's time to end this NSA's mass surveillance. On the same day, the government of Brazil declared as well that it will not grant the long-awaited $4.5 billion contract for fighter jets to Boeing (the US based company), but instead would award it to Saab, the Swedish company. Brazil's frustration at the NSA spying against its leaders, corporations, and its people was obviously a crucial factor in this sudden decision. "The NSA issue has destroyed the chance for the Americans," a Brazilian source informed Reuters (Reuters, 2013).

The main change to the national security policy in Europe came in post the Snowden revelations. Upon discovering that the US did not only spy on the unfriendly or possible terrorist nations in the world, but also collected intelligence from its allies. This greatly impeded trust between Europe and the US, which has prompted several improvements to the

law of national security in the EU. Anna Cecilia Malmstrom, a Swedish politician whom had served as European Trader Commissioner until 2014, said at the beginning of June 2013 that the mutual confidence and trust between the EU and the US have been badly compromised, and she expects the US to do whatever it takes to restore it ("EU threatens to stop sharing data with U.S. over spying reports," 2013).

When PRISM revealed how major internet giants were enabling the NSA to access their databases and how they were intercepting the communication of ordinary people from all over the world, European leaders realized that they needed more than ever to secure their servers and data. As European intelligence is very much reliant on the intelligence services of the US-UK, this event has caused considerable harm to that relationship. President François Hollande said, "We cannot tolerate this kind of action between partners and allies. We ask that this end immediately" (Bowcott, 2015b; "France warns US spying claims threaten trade talks," n.d.).

Members from various European countries have voiced their concern regarding the strategy of transferring individuals' data from European countries to the US and called for more security and protection from the law to safeguard personal data from major US servers and social media. Leaders acknowledged these issues and quickly began to work on them. Philipp Albrecht, MEP of the German Greens, said, "As parliamentarians, as leaders, as governments, we have lost control of our security services, we've got to get it back again" (Traynor, 2013).

Snowden's revelations have also triggered a major controversy that has led to a tension between American and European business partners. A surge of mistrust has conquered Europe, which negatively affected American companies, whereas other European companies have benefited from the crisis. The following two examples demonstrate the effect of Snowden's disclosures on business between Europe and the U.S.

1) Brazil, Saab and Boeing: The Snowden disclosures have had a very positive effect on Saab, the aerospace company based in Sweden. Brazil had a tender requesting 36 new Gripen

fighters to be delivered by 2020 to the Brazilian government. Boeing, the American company was trying hard to get the deal.

However, Brazil shocked the world when it chose Saab for this contract. The leakages of the U.S. surveillance outreach caused Boeing to lose the chance of winning this contract. On requested anonymity, a Brazilian government source told Reuters: "The NSA issue wrecked it for the Americans" (Reuters Editorial, 2013).

2) Germany: Verizon vs. Deutsche Telekom: In June 2013, *The Guardian* released the first Snowden file under the name "NSA collecting phone records for millions of Verizon customers daily." The NSA classified paper was a court order that exposed that the agency had stored the call records of millions of U.S citizen who use Verizon. Verizon is an American internet and telephone corporation and one of the biggest suppliers of cellular networking networks in the world. Under a contract from 2010 till 2015, Verizon was the network provider in Germany. As a result of the leaks, the German Government decided to withdraw from the deal and replace Verizon with a German provider. The German government has concluded that Verizon would allow American intelligence agencies to access German government communications via the Verizon network, despite it being more stable, quicker and cheaper than local network service providers. Tobias Plate, spokesperson for the Interior Ministry, said on June 2014 in a press conference covered by Bloomberg: "The federal government needs to recover more technological sovereignty and thus chooses to work with German companies" (Brian Parkin, n.d.). Tobias did not confirm if they had any evidence that Verizon was participating with any American surveillance within Germany. However, an article published later this year, proved that the NSA did indeed tap Chancellor Merkel's phone. The German Government has thus agreed to replace Verizon's contract with Deutsche Telekom, a company already responsible for the

processing of confidential communications between German government officials or intelligence departments.

Chapter Six

Conclusion

The tendency for intelligence agencies to abuse power is not a new phenomenon in general, and specifically in the U.S. As a matter of fact, in 1976 the Church investigation committee has found that intelligence agencies have expanded their operations beyond their initials mandate and have shown inclinations to increase power and reach in all aspects of their activities.

The main enabler that allowed this overreach to take place was mainly the lack of legislation related to intelligence gathering that would serve as a guideline for checks and balances to be used by the judicial body in supervising the activities of intelligence agencies. Another factor was the tendency for these agencies to always try to bypass the checks and balances and to avoid reporting, or underreporting, a secret operational case to the executive branch. As shown in the Senate Select Committee on Intelligence published in 1976, many cases showed that the intelligence community have padlocked some top-secret operations. Under the argument that the US government and US citizens' main priority should be ensuring their safety from potential terrorist threats, the intelligence community claims that there is then an obligation to conduct intelligence operations in secrecy, even if this means that the public and the legislative body are not necessarily aware of such operations. The ultimate purpose is safeguarding their safety and thus it is acceptable to conduct surveillance without their knowledge.

While as some may argue that in exceptional times the President must be granted exceptional powers, it is clear that examining abuse of powers in the field of intelligence remains limited, mainly because most of the intelligence practices are done in total secrecy.

However, the NSA files made available by Snowden can be argued to have demonstrated that the U.S has increased surveillance as well as abused its security tools, undermining by this practice the faith in the political system and liberal principles. Mainly in the post 9/11 era, the Bush administrations has used the argument of "fight against terror" to justify its expansion of surveillance domestically and globally. These surveillance activities manifested elements of a surveillance state which is contradictory to the liberal democratic principles on which the U.S was founded, and they had undermined the imagine that the U.S represents globally as the liberal state. Snowden's revelations have indeed complicated the US international relations, especially with countries that were allied democracies but were not exempted from the NSA surveillance.

The files that Snowden has leaked to the public launched an unprecedent global debate regarding the mass surveillance in the digital world and its legitimacy and ethical framework. Exercising mass surveillance at a wide extent in a democratic western state will always challenge the foundations of the liberal state and the privacy and rights of citizens. In the past, many people have had challenges in pointing out the issues surrounding privacy in the digital platforms on matters of national surveillance, but Snowden managed to ignite the conversation. The NSA through the leaked files has been disputed as for its past actions and the concern of the future since it will always have a responsibility to maintaining national security, however, protecting privacy rights and adhering to the constitutional limitations shouldn't be left aside.

Snowden's actions transformed the way the world viewed the panoptic architecture, precisely because he brought it back into focus. Under the Benthamite panopticon concept, the watchtower was a very real object, and its gaze was continually felt. In the modern era, however the panopticon's tangibility was diminished, and the emphasis was on diverting attention from the monitoring apparatus to the point that the participants could forget that they were under

scrutiny at all. By shattering this illusion, Snowden reminded us that indeed, there were systems in place that grant certain important people access to whatever kind of personal information they needed on everyone in the world. His whistle blowing brought back the panoptic setting. What is important to note is that despite the actions of Snowden, the laws and regulations that allow mass data gathering possible have little changed, but the way the public deals with the surveillance they are subject to, has changed now that they are aware of it. For the best or for the worst, humanity is now well conscious of the level of surveillance they are under and is able to deal with it in a manner that allows a bit more control and power to the subjects.

The ability to spy on people's lives and communications grants tremendous influence and power to those who do it. Unless such power is governed by strict monitoring and transparency, it is certain to be abused. Expecting the US government to run a vast surveillance machine in total secrecy without succumbing to its temptations is contrary to any historical example and to all available evidence of human existence.

When you handle great power to a government, it is nearly impossible for that government to give away that power, and when power is exercised in secret under the umbrella of national security, dangers increase. Power is not simply in the hands of those existing in office at the moment but to those who will be in charge in the future as well. The NSA programs revealed do not only impact the present but also the future. Even if we consider that the current US government's justifications are on point and that it had the rights to exercise those power in fear of terrorism, there is an inevitable slippery slope. The temptation is undeniable for a government who owns a capacity as such to overreach it and abuse it in all sorts of areas- economic dominance, oppression of citizens, diplomatic play foul. Who guards the watchers? Who guarantees that no abuse is put in place?

As any other government, the US government has every legitimate right to oversee cyberspace to safeguard its national security and foreign policies. Democracies need intelligence agencies capable of operatizing in a certain amount of secrecy. However, the revelations made by Snowden, showed that the NSA had no checks and balances on the programs it uses for surveillance that it should have had and must have in the must. The surveillance programs used by NSA should not be totally abolished; they are vital to ensuring national security. Yet, it is no question that the programs need to amend and made subject to oversight and supervision by courts and by Congress to ensure that such surveillance serves national security interests and not illegitimate spying on nationals and foreigners for other purposes such as diplomatic or economic advancement.

After numerous attempts to introduce laws and rules to manage national surveillance in the architecture of the political system in the US and to minimize its harmful effects on some of the core value that make up the United State a democratic liberal state as it is, the government endured another scandal in 2017. WikiLeaks released 8761 documents, code-named Vault 7, just weeks after Trump's administration entered the White House, exposing surveillance projects under the Obama administration. These documents indicate that the surveillance technologies, policy, techniques, implementation and capabilities of the U.S. intelligence community have been further developed and strengthened. The leaked documents clearly show that the new techniques and tools put in place do not aim to increase transparency, but rather to increase confidentiality. They seek to minimize the use of footprints in order to destroy the possibility to detect their application, to self-destruct in timely manner to remain undetected, and, most importantly, to function in a discreet layer of governmental practice that aims not to comply but to avoid challenging legal norms rooted in the concept and foundation of the U.S. political system.

BIBLIOGRAPHY

Administration White Paper., Bulk Collection of Telephony Metadata Under Section 215 of USA PATRIOT ACT., 9 August 2013

Al Jazeera. (2013). NSA says Obama didn't know Merkel's phone was being bugged.

Al Jazeera. (2013). NSA chief defends spy program in face of protest from allies.

Al Jazeera. (2013). Merkel send intelligence delegation to US over NSA spying

Albanese, J.S. (1980). Wiretapping and the Crime Control Ideology

Alden, E. (2006). How Bush is testing the limits of surveillance on American soil. Financial Times, London

Allen, J. (2008). Expanding Law Enforcement Discretion: How the Supreme Court's Post-September 11th Decisions Reflect Necessary Prudence. *Suffolk University Law Review, 41*(3).

Amoore, L (2014) Security and the claim to privacy. International Political Sociology 8(1): 108–112

Arthur, C. (2013, September 21). Major US security company warns over NSA link to encryption formula. Retrieved from HTTP://WWW.THEGUARDIAN.COM/WORLD/2013/SEP/21/RSA-EMC-WARNING-ENCRYPTION-SYSTEM-NSA

Austin, L. (2015). Lawfully illegality: What Snowden has taught us about the legal infrastructure of the surveillance state. Law, Privacy and surveillance in Canada in the Post-Snowden Era

Balkin, J. (2006). The Constitution in the National Surveillance State

Ball, J. (2013, October 25). Leaked memos reveal GCHQ efforts to keep mass surveillance secret. Retrieved from HTTP://WWW.THEGUARDIAN.COM/UK-NEWS/2013/OCT/25/LEAKED-MEMOS-GCHQ-MASS-SURVEILLANCE-SECRET-SNOWDEN

Ball, J. (2014, January 16). NSA collects millions. Of text messages daily in "untargeted" global sweep. Retrieved from HTTP://WWW.THEGUARDIAN.COM/WORLD/2014/JAN/16/NSA-COLLECTS-MILLIONS-TEXT-MESSAGES-DAILY-UNTARGETED-GLOBAL-SWEEP

Bamford, J. (2008). The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America. New York: Doubleday.

Bauman Z. & Lyon D. (2013), Liquid Surveillance, Polity Press

Bennett, D. (1988). The party of fear: From nativist movements to the new right in American History

Bentham, J. (2010). The panopticon writings. London: Verso Books

Bigo, D. and Tsoukala, A. (2008), Terror, Insecurity and Liberty, Illiberal practices of liberal regimes after 9/11. New York, Routledge

Bigo, D., 2002. Security and Immigration: Toward a Critique of the Governmentality of Unease. Alternatives: Global, Local, Political

Bigo, D., 2010, Delivering Liberty and Security? The Reframing of Freedom When Associated with Security

Blankley, T. (2009). American grit: What it will take to survive and win in the 21st century. Ashland, OR: Blackstone Audio.

Boghosian, H. (2013). Spying on democracy: Government surveillance, corporate power, and public resistance.

Borger, J., Ball, J., & Greenwald, G. (2013, September 6). Revealed: How US and UK spy agencies defeat internet privacy and security. The Guardian. Retrieved from HTTP://WWW.THEGUARDIAN.COM/WORLD/2013/SEP/05/NSAGCHQ-ENCRYPTION-CODES-SECURITY

Bowcott, O. (2015). Facebook case may force European firms to change data storage Practices

Brunon-Ernst. A. (2012). Beyond Foucault: New Perspectives on Bentham's Panopticon.

Buzan, B. (1997) 'Rethinking Security After the Cold War,' Cooperation and Conflict, Vol. 32, No. 5, pp. 5-28.

Cassidy, J. (2013) Why Edward Snowden Is a Hero. The New Yorker. Retrieved from http://www.newyorker.com/rational-irrationality/why-edward-snowden-is-a-hero

Ceyhan A. (2008), Technologizing of Security: Management of Uncertainty and Risk in the Age of Biometrics", Surveillance and Society 5(2): 102-123

Cohn, C. (2013, June 7). In Response to the NSA, We Need A New Church Committee and We Need It Now. Retrieved from https://www.eff.org/deeplinks/2013/06/response-nsa-we-need-new-church- commission-and-we-need-it-now

Conniry, K. (2016). National Security, Mass Surveillance, and Citizen Rights under Conditions of Pr Rights under Conditions of Protracted W acted Warfare. *Portland State University- Dissertations and Theses*, *3204*. https://doi.org/10.15760/etd.3195

Corporation, A. B. (2013). Explained: Australia's involvement with the NSA. Retrieved from HTTP://WWW.ABC.NET.AU/NEWS/2013-11-08/AUSTRALIAN-NSA-INVOLVEMENT-EXPLAINED/5079786

Dan, H. (2013). Brazil snubs Boeing in fighter jet deal. The New York Times. Retrieved from HTTP://WWW.NYTIMES.COM/2013/12/19/BUSINESS/INTERNATIONAL/BRAZILSNUBSBOEINGINJETDEAL.HTML

Deleuze, G. (1992). Postscript on the societies of control.

Deleuze, G., & Guattari, F. (1987). A thousand plateaus: capitalism and schizophrenia. Minneapolis: University of Minnesota Press.

DeRosa M., (2004), CTR. For strategic and international studies, Data mining and data analysis for counterterrorism. Retrieved from http://www.cdt.org/security/usapatriot/20040300csis.pdf

Donohue L., (2006). Anglo-American Privacy and Surveillance, 96 J. Criminal Law & Criminology

Etzioni, A. (2015) NSA: National Security vs. Individual Rights. Intelligence and National. Security. 30 (1) 100-136.

EU Threaten to stop sharing data with U.S over spying reports. (July 2013)

Fidler D. (2015). The Snowden Reader. Indiana University Press

Foucault, M. (1991). The Foucault effect: studies in governmentality. Chicago: University of Chicago Press

Foucault, M. (1977). Discipline and Punish: The Birth of the Prison. New York: Pantheon
Fourth Amendment. (2017). Legal Information Institute. Retrieved from https://www.law.cornell.edu/wex/fourth_amendment

Friedman, G. (2014, April 22). Keeping the NSA in Perspective. Retrieved. Geopolitical Weekly. Retrieved form https://www.stratfor.com/weekly/keeping-nsa-perspective

Frontline, (2014, May 13 & May 20). United States of Secrets. Part one and Part two. OPB. Retrieved from http://www.pbs.org/wgbh/pages/frontline/united-states-of- secrets/

Fuchs, C. (2012). Political economy and surveillance theory. Critical Sociology

Gallagher, S. (2013, July 22). JURIST - A Short History of the NSA. Retrieved from http://jurist.org/feature/2013/07/nsa-overview-2.php

Gandy, O. (1989), „The Surveillance Society: Information Technology and Bureaucratic Social Control", Journal of Communications, 39(3), pp. 61-76

Gellman, B., & Poitras, L. (2013, June 7). NSA slide explains the Prism data-collection. Washington Post. Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from- nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf- 11e2-8845-d970ccb04497_story.html

Gellman, B. (2013, June 9). Code name "Verax": Snowden, in exchanges with Post reporter,

made clear he knew risks. The Washington Post. Retrieved from HTTPS://WWW.WASHINGTONPOST.COM/WORLD/NATIONAL-SECURITY/CODE-NAME-VERAX-SNOWDEN-IN-EXCHANGES-WITH-POST-REPORTER-MADE-CLEAR-HE-KNEW-RISKS/2013/06/09/C9A25B54-D14C-11E2-9F1A-1A7CDEE20287_STORY.HTML

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/nsa- infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Germany, S. O. H. (N.D.). Greenwald: "Explosive" NSA spying reports are imminent. Spiegel online. Retrieved from HTTP://WWW.SPIEGEL.DE/INTERNATIONAL/WORLD/JOURNALISTSAYS-EXPLOSIVEREPORTSCOMINGFROMSNOWDENDATAA912034.HTML

Gilbert N. (2007), Dilemmas of Privacy and Surveillance: Challenges of Technological Change., The Royal academy of Engineering

Goldsmith J., Katyal N., (2017). The Terrorists' Court, N.Y. TIMES

Gorman, S. (2013, August 23). NSA Officers spy on love interests. Retrieved from HTTP://BLOGS.WSJ.COM/WASHWIRE/2013/08/23/NSA-OFFICERS-SOMETIMES-SPY-ON-LOVE-INTERESTS/

Greenslade, R. (2013, August 19). How Edward Snowden led journalist and filmmaker to reveal his secrets. The Guardian. Retrieved from HTTP://WWW.THEGUARDIAN.COM/WORLD/2013/AUG/19/EDWARD-SNOWDENNSASECRETSGLENNGREENWALDLAURAPOITRAS

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

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. New York, NY: Metropolitan Books, Henry Holt.

Greenwald, G. & Ackerman, S. (June 2013). How the NSA is still harvesting your online data: Files show vast scale of current NSA metadata programs, with one steam alone celebrating 'one trillion records processes'. The Guardian

Greenwald, G. & Ackerman, S. (June 2013). NSA collected US emails records in bulk for more than two years under Obama. The Guardian

Greenwald, G., Grim, R., & Gallagher, R. (2013). Top-secret document reveals NSA spied on porn habits as part of plan to discredit "Radicalizers". The Guardian

Greenwald, G., & Macaskill, E. (2013, June). NSA PRISM program taps into user data of Apple, Google and others. The Guardian. Retrieved from

HTTP://WWW.THEGUARDIAN.COM/WORLD/2013/JUN/06/USTECH-GIANTS-NSA-DATA

Greenwald, G., Macaskill, E. & Poitras, L. (June 2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian

Greenwald, G. & Saxena, S. (2013). India among top targets of spying by NSA. The Guardian

Haines, D. (2017). Ethical considerations in qualitative case study research recruiting participants with profound intellectual disabilities. *Research Ethics*, *13*(3-4), 219-232.

Hakim, P. (2014). The future of US-Brazil relations: Confrontation, cooperation or detachment? International Affairs, 90(5), 1161-1180. Retrieved September 30, 2014.

Harrison, H., Birks, M., Mills, J., & Franklin, R. (2017). Case Study Research: Foundations and Methodological Orientations. *Forum: Qualitative Social Research*, *18*(1).

Hayes B., State of Surveillance: The NSA Files and the Global Fightback., State of Power

Heale, R., & Twycross, A. (2017). What is a case study? *Evidence Based Nursing*, *21*(1), 7-8

HM Government. (2008) The National Security Strategy of the United Kingdom: Security in an Interdependent World, Joint Committee on the National Security Strategy, March 2008.

Inkster, N. (2014). The Snowden revelations: Myths and Misapprehensions. Survival: Global Politics and Strategy, 56(1), 57-60.

James, R. (2013, November 22). N.S.A. Report outlined goals for more power. The New York Times. Retrieved from HTTP://WWW.NYTIMES.COM/2013/11/23/US/POLITICS/NSA-REPORT-OUTLINED-GOALS-FOR-MORE-POWER.HTML

Kirschbaum, E. (2014, January 26). Snowden says NSA engages in industrial espionage: TV. Retrieved from HTTP://WWW.REUTERS.COM/ARTICLE/2014/01/26/US-SECURITY-SNOWDEN-GERMANY-IDUSBREA0P0DE20140126

Kitrosser H. (2007), Macro-Transparency as Structural Directive: A Look at the NSA Surveillance Controversy, Minnesota Law Review

Klein, E. (2013, August 9). Edward Snowden, patriot - The Washington Post. The Washington Post. Retrieved from http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward- snowden-patriot/

Kreimer S. F. (2004), Watching the Watchers: Surveillance, Transparency and Political Freedom in the War on Terror., Journal of Constitutional Law, Vol. 7:1, pp. 133- 181

Levi, M., & Wall, D. (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*, *31*(2), 194-220. Retrieved November 29, 2020, from http://www.jstor.org/stable/1410524

Levine, B. (N.D.). Who is putting up "interceptor" cell towers? Retrieved from HTTP://VENTUREBEAT.COM/2014/09/02/WHO-IS-PUTTING-UP-INTERCEPTOR-CELL-TOWERS-THE-MYSTERY-DEEPENS/

Lewis, P. (2013). NSA denies discussing Merkel phone surveillance with Obama. The Guardian

Lichtblau, E. (2007). *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES

Lomas, N. (2014, November 4). U.K. Spy Agency Chief Goes Public with Anti- Encryption Appeal to U.S. Tech Companies | TechCrunch. TechCrunch. Retrieved from http://techcrunch.com/2014/11/04/privacy-not-an-absolute-right/

Lyon, D. (2001), Surveillance Society: Monitoring Everyday Life, Oxford: Open University

Lyon, D. (2006). The search for surveillance theories. In D. Lyon (Ed.), Theorising surveillance: The panopticon and beyond (pp. 3–20). Portland: Willam Publishing.

Lyon D. (2007), Surveillance Studies: An Overview., Polity Press

Lyon, D. (2012), Introducing Surveillance Studies, Cambridge, Polity Press

Maass, P. (2013, August 13). How Laura Poitras helped Snowden spill his secrets. The New York Times. Retrieved from HTTP://WWW.NYTIMES.COM/2013/08/18/MAGAZINE/LAURA-POITRAS-SNOWDEN.HTML-PAGEWANTED-ALL

MacAskill, E. (2013, June 30). New NSA leaks show how US is bugging its European allies. The Guardian, Retrieved from https://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies

MacAskill, E. (2013, September 9). Yahoo files lawsuit against NSA over user data requests. The Guardian. Retrieved from http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests

Macaskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fiber optic cables for secret access to world's communications. Retrieved from HTTP://WWW.THEGUARDIAN.COM/UK/2013/JUN/21/GCHQ-CABLES-SECRET-WORLD-COMMUNICATIONS-NSA

Margulies, P. (2014). The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism. Fordham Law Review (Volume 82, Issue 5)

Marx G., Reichman N. (1984), Routinizing the Discovery of Secrets: Computers as Informants, in American Behavioral Scientist, Vol. 27, no. 4, pp.423-452

Mearsheimer, J.J. (2001) The Tragedy of Great Power Politics. New York: W.W. Norton

McNiff, C. Timeline: U.S. Spying and Surveillance. Infoplease. Retrieved from

http://www.infoplease.com/us/government/spying-surveillance-timeline.html

Military Order No.222. (2001). Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism. 66 Federal Register. Retrieved from https://fas.org/irp/offdocs/eo/mo-111301.htm

Miller, G., Nakashima, E., (December 2013). Officials' defenses of NSA phone program may be unraveling. The Washington Post

Mitchell, T. (1988). Colonizing Egypt. Cambridge: Cambridge UP.

Monohan T. (2010), Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance. In Surveillance and Democracy., Edited by K. D. Haggerty and M. Samatas. New York: Routledge 2010, 91-110

Moschella W., (2005). Letter to the Senate Select Comm. on Intelligence and House Permanent Select Comm. on Intelligence

Moyers, B. (2013). Bruce Fein and John Nichols on George W. Bush and Presidential Overreach.

Nakashima, E. (December 2013). Panel urges new curbs on surveillance by U.S. The Washington Post

Nakashima, E. (January 2014). NSA phone record collection does little to prevent terrorist attacks, group says. The Washington Post

NSA: New reports in German media deepen US Merkel Spy row. (n.d.). BBC News. Retrieved from HTTP://WWW.BBC.COM/NEWS/WORLDEUROPE24692908

Parkin, B., (N.D.). Germany favors Deutsche Telecom to replace ousted Verizon. Retrieved from HTTP://WWW.BLOOMBERG.COM/NEWS/ARTICLES/201406-26/GERMANGOVERNMENTTOENDVERIZONCONTRACTCITINGNSA-CONCERN

Peissl, W. (2003). Surveillance and Security: A Dodgy Relationship. Journal of Contingencies & Crisis Management, 11(1), 19-24

Poitras, L. Rosenbach, M. & Stark, H. (September 2013). NSA Monitors Financial World

Rahman, M. (2017). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review. Journal of Education and Learning

Reeves, T. (1982). The life and times of Joe McCarthy: A Biography

Report and Recommendations of The Presidents Review Group on Intelligence and Communication Technologies (December 2013), Security and Liberty in Changing World

Reuters Editorial. (2013). Update 4: Saab wins Brazil jet deal after NSA spying sours Boeing bid. Retrieved from HTTP://WWW.REUTERS.COM/ARTICLE/2013/12/19/BRAZIL-JETS-IDUSL2N0JX17W20131219

Rogerson K. Milton D. (2013), A Policymaking Process "Tug of War": National Information Security Policies in Comparative Perspective., Journal of Information Technology & Politics. 10:462-476

Rushe, D., Ackerman, S., & Ball, J. (2013, October 31). Reports that NSA taps into Google and Yahoo data hubs infuriate tech giants. Retrieved from HTTP://WWW.THEGUARDIAN.COM/TECHNOLOGY/2013/OCT/30/GOOGLE-REPORTS-NSA-SECRETLY-INTERCEPTS-DATA-LINKS

Savage, C. (2013). Secret Court Rebuked N.S.A. on Surveillance. New York Times. Retrieved from http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?pagewanted=all&_r=2&

Schofield, P. (2009). Bentham: a guide for the perplexed. London: Continuum.

Schulte, J., 2006. Preemptive Media - Surveillance Creep! New Manifestations of Data Surveillance at the Beginning of the Twenty-First Century. Radical History Review. 95, Spring, pp.70–88.

Scott, J. (2017). Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space. *Journal of Business & Technology Law*, *12*(2). Retrieved 29 November 2020.

Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (1976), US Senate., U.S. Government Printing Officer., Washington

Smith, C., & Hung, L. (2010). The PATRIOT Act issues and controversies. Springfield, Ill.: Charles C. Thomas Publisher

Spiegel staff. (November 2013). How the NSA and GCHQ spied on OPEC

Stevens G. M. (Legislative Attorney, American Law Division), Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws, Report for Congress, Congressional Research Service 2003

Stoddart, E (2014) (In)visibility before privacy: A theological ethics of surveillance as social sorting. Studies in Christian Ethics 27(1): 33–49.

Stout D., (2002). Rumsfeld Defends Plan to Hold War Detainees, N.Y. TIMES.

Strohm, C., & Wilber, D. Q. (2014). Pentagon says Snowden took most U.S. secrets ever. Retrieved from HTTP://WWW.BLOOMBERG.COM/NEWS/ARTICLES/2014¬01¬09/PENTAGON-FINDS-SNOWDEN-TOOK-1-7-MILLION-FILES-ROGERS-SAYS

Strizel, H. (2007) 'Towards a Theory of Securization: Copenhagen and Beyond,' European Journal of International Relations, Vol. 13, No. 3, pp. 357-383.

Sulmasy, G., & Yoo, J. Katz and the War on Terrorism. *University of California, Davis*, *41*.

Teegavarapu, S., Summers, J., & Mocko, G. (2008). Case Study Method for Design Research

The USA PATRIOT Act: Preserving Life and Liberty (2001). The Department of Justice. Retrieved from http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

Toxen, B. (2014, May 1). The NSA and Snowden: Securing the All-Seeing Eye. Retrieved from http://cacm.acm.org/magazines/2014/5/174340-the-nsa-and-snowden/abstract

Traynor, I. (2013, November 26). NSA surveillance: Europe threatens to freeze US data-sharing arrangements. The Guardian. Retrieved from http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing

United States White House, (2006) The National Security Strategy of the United States of America, March 2006.

Vicens, A., Gilson, D., & Park, A. (2013, September 11). Timeline: Here's how we got from 9/11 to massive NSA spying on Americans today. Retrieved from http://www.motherjones.com/politics/2013/09/nsa-timeline-surveillance

Walpin, G. (2013, August 16). We need NSA surveillance. *National Review.* Retrieved from http://www.nationalreview.com/article/355959/we-need-nsa-surveillance-gerald-walpin

Watts, J. (2013, September 9). NSA accused of spying on Brazilian oil company Petrobras. The Guardian. Retrieved from HTTP://WWW.THEGUARDIAN.COM/WORLD/2013/SEP/09/NSA-SPYING-BRAZIL-OIL-PETROBRAS

White, W. (1956). Citadel: The Story of the U.S. Senate

XKeyscore: NSA'S Google for the world's private communications. (N.D.). Retrieved from HTTPS://THEINTERCEPT.COM/2015/07/01/NSAS-GOOGLE-WORLDS-PRIVATE-COMMUNICA TIONS/

"You're being watched": Edward Snowden emerges as source behind explosive revelations of NSA Spying. (n.d.). Retrieved from HTTP://WWW.DEMOCRACYNOW.ORG/2013/6/10/YOURE_BEING_WATCHED_EDWARD_SNOWDEN_EMERGES

Appendices

Appendix A

Key U.S. Laws in the Snowden Disclosures

Fidler D. (2015). *The Snowden Reader.* Indiana University Press

Fourth Amendment to the U.S. Constitution	"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."
Section 215 of the USA PATRIOT Act	The 215 Section authorizes the Federal Bureau of Investigation (FBI) to "make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Any such application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) ...to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities[.]"

Section 702 of the Foreign Intelligence Surveillance Act	"Notwithstanding any other provision of law... the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." Before implementing any such authorization, the Attorney General and Director of National Intelligence must submit to the Foreign Intelligence Surveillance Court for its review and approval a "written certification" that includes (1) targeting procedures to "ensure that any acquisition...is limited to targeting persons reasonably believed to be located outside the United States and... prevent the intentional acquisition of any communication to which the sender and all intended recipients are known at the time of acquisition to be located in the United States"; and (2) minimization procedures that, among other things, "minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning un-consenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information [.]"

Appendix B

Summary of major surveillance programs and tools

Codename	**Purpose**	**Scope**	**Type**
XKeyscore	Store and query data based on specific filters	Global	Bulk
Tempora (GCHQ)	Store internet traffic	Global	Bulk
BULLRUN (NSA) Edgehill (GCHQ)	Break encryption used in networked communication	Global	Bulk
FAIRVIEW	Capture phone metadata, internet traffic and SMS from foreign countries (through AT&T)	Global	Bulk
DishFire	Capture SMS	Global	Bulk
STORMBREW	Capture data from top-level communications infrastructure and fiber-optic cables	Global	Bulk
MUSCULAR (GCHQ and NSA)	Capture all traffic between data centers of Google and Yahoo	Yahoo and Google data centers	Bulk

Stellar Wind	Store call metadata	USA	Bulk
PRISM	Capture any data from tech companies that is defined by the FISA court authorized orders	US based service providers	Bulk
MYSTIC (SOMALGET)	Store call metadata and also phone calls for some countries	All calls from: Bahamas, Kenya, Afghanistan	Bulk
Turbulence	Injecting malware into remote computers	Global	Targeted