



University of Piraeus  
School of Economics, Business and International Studies  
Department of International and European Studies  
in coordination with  
New York University's Centre for Global Affairs  
M.Sc. in American Studies: Politics, Strategy and Economics

## **Intelligence and Democracy: Snowden Revelations and Reforms.**

*by*

*Charalampos (Bobby) O. Paraskevopoulos (mas21016)*

**Supervisor:** Dr. Konstantopoulos Ioannis, Assistant Professor in International Relations & Economic Diplomacy at the Department of International and European Studies, School of Economic, Business and International Studies, University of Piraeus.

University of Piraeus in coordination with New York University's Centre for Global Affairs  
Piraeus (Greece/Attiki), September 2023

The intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

Copyright © 2023 by Charalampos (Bobby) O. Paraskevopoulos  
All rights reserved

# Table of Contents

<b>Dedication</b> .....	5
<b>Abstract</b> .....	6
<b>Abbreviations</b> .....	8
<b>List of Figures</b> .....	10
<b>Chapter I: Introduction</b> .....	12
<b>Chapter II: Intelligence and Democracy.</b> .....	16
<b>II.1 Democracy.</b> .....	16
<i>Definition of Democracy, the United States' political system and its Principles.</i> .....	16
<i>The 4th Amendment, the reasonable Expectation of Privacy, National Security, Freedom of Information and Human Rights after 9/11.</i> .....	17
<b>II.2 Intelligence.</b> .....	21
<i>Definition of Intelligence and the Intelligence Cycle.</i> .....	21
<i>Intelligence Community (IC).</i> .....	23
<i>Ethics of Intelligence.</i> .....	25
<i>Espionage Act of 1917.</i> .....	26
<i>FISA History, Acts and Amendments.</i> .....	27
<i>Executive Order 12333.</i> .....	31
<i>Executive Order 12333, Section 215 of the Patriot Act, FISA Amendments Act: A Comparison.</i> .....	33
<i>The role of ACLU.</i> .....	34
<b>II.3 Intelligence and American Democracy.</b> .....	35
<i>Intelligence vs Democracy?</i> .....	35
<i>The act of Whistleblowing.</i> .....	36
<i>Metadata and Mass Surveillance</i> .....	37
<i>Oversight and Accountability.</i> .....	38
<b>II.4 Research Methodology.</b> .....	43
<i>Structure.</i> .....	43
<i>Research Questions:</i> .....	45
<b>Chapter III: The Snowden case – Timeline of Events</b> .....	47
<i>Introduction.</i> .....	47
<b>III.1 The Planning: Chronicles of the spy story.</b> .....	49
<b>III.2 The fight for asylum: How Mr. Snowden avoided U.S prosecution?</b> .....	51
<b>III.3 The Revelations.</b> .....	53

<b>III.4. What we discovered regarding the US and UK operations for mass surveillance of phone and internet interactions?</b> .....	59
<i>Accessing transnational communication systems.</i> .....	59
<i>Getting into the cloud services and electronic operations of corporates.</i> .....	59
<i>Monitoring the position of smart phone devices.</i> .....	61
<i>Monitoring international phone conversations and calls of many nations.</i> .....	61
<i>US surveillance authorities put pressure on European nations to weaken their privacy legislation.</i> .....	61
<i>Enhancing widespread surveillance.</i> .....	62
<i>Unauthorized access to mobile devices and applications.</i> .....	63
<i>Lowering levels of encryption.</i> .....	64
<i>Directing key communication systems.</i> .....	65
<i>Encryption keys theft.</i> .....	66
<i>Summary of the significant spying programs and instruments.</i> .....	66
<b>III.5 Obama’s limited and ineffective response.</b> .....	68
<b>III.6 Reactions to Obama’s reforms.</b> .....	73
<b>Chapter IV: Edward Snowden Disclosures: Discussion and Reflections.</b> .....	76
<i>IV.1 Snowden’s motives: A Whistleblower or a Traitor?</i> .....	77
<i>IV.2 The consequences of the Snowden revelations.</i> .....	81
<i>IV.3 The institutions as counterweights and overseers of the security state: Changes after the Snowden revelations and proposals for the protection of classified information.</i> .....	85
<i>IV.4 Intelligence vs Democracy: How to achieve harmony between security and privacy and shape the pathway to reform?</i> .....	89
<b>Chapter V: Conclusions</b> .....	94
<b>Bibliography:</b> .....	96

## **Dedication**

I can't thank the Almighty God enough for giving me the chance to get an education, improve my skills, and help move my society forward. I also extend my deepest gratitude to my mom for raising me and providing me financial assistance so that I may seek further education and training and then grow into a greater version of myself.

I want to convey my very special and honest thankfulness and appreciation to my job manager, Hellenic Police Spokesperson Konstantia Dimoglidou, since I would not have been able to finish this thesis without her essential assistance. In particular, she has been by my side from the very beginning and throughout every stage of my academic experience and research preparation and completion. From attending the lectures and conducting the required projects to successfully completing the academic exams, Mrs. Dimoglidou has been there for me at every step of this journey, and her high passion, motivation, empathy, and facilitation have encouraged me to go ahead and strive to accomplish this project, which at first seemed quite challenging.

Additionally, I want to thank my research supervisor, Dr. Ioannis Konstantopoulos, who is an Assistant Professor in International Relations and Economic Diplomacy at the Department of International and European Studies, School of Economic, Business, and International Studies, University of Piraeus. He gave me permission to do this study and gave me important advice throughout my educational journey. I have been greatly impressed by his energy, passion, genuineness, and determination. He has taught me how to do the research and deliver the results in the most understandable way. Being able to work and learn under his direction was a huge honor and a source of satisfaction and pleasure. Additionally, I want to praise him for his kindness, sensitivity, and tolerance throughout our conversations we had about the research and thesis production and completion.

Last but not least, along with my supervisor professor, I would also like to express my deepest thanks and admiration to the other members of my dissertation committee: Professors Athanasios Platias and Pano Yannakogeorgos, for their support and encouragement, their enlightening remarks, and their significant contribution in deploying my skills and awareness in American Studies and the US intelligence sector. I also want to offer my sincere thanks to all the professors at Piraeus University and New York University for their help, support, and guidance throughout this astonishing educational journey.

## **Abstract**

In June 2013, Edward Snowden leaked secret documents that showed the U.S. government was spying on its own people. This made him a popular phenomenon. The material revealed that the NSA (National Security Agency) coerced many telecom service companies to cooperate in the acquisition of millions of U.S. people's "metadata." Data about an individual's life that is private and confidential is included in "metadata." So, if "metadata" is gathered and examined, it can paint a picture of a person's private actions, which is a breach of that person's right to privacy. Because metadata can give so much information, it is invasive and violates the 4th Amendment. Nevertheless, collecting and examining information may be an effective weapon in the war on terrorism and in defending U.S. civilians from further assaults. To effectively manage privacy concerns while achieving national security goals, the standard must be raised to probable cause delineation. These revelations exposed the NSA's massive PRISM mass surveillance data system (program) as well as evidence of covert agreements between nations exchanging intelligence information. Edward Snowden, a Hawaii-based NSA contractor, served as the originator of the leak in cooperation with two of the biggest daily newspapers in the world, "The Guardian" and "The Washington Post." After originally escaping to Hong Kong and subsequently Russia, Edward Snowden is still evading capture. The disclosures had a severe impact on US ties with other countries, such as Brazil, setting aside commercial advantages and disrupting US relations with many nations across the globe. Also, some of the large US-based IT corporations, particularly those specializing in cloud services, suffered great loss of money as a result of the "whistleblowing."

Meanwhile, before the revelations, the National Security Agency's monitoring operations, the White House, and the Department of Justice's statutory avoidance were largely unknown to the public sphere and a substantial part of Congress. After Edward Snowden's leaks to certain reporters, the dishonesty of Intelligence Community (IC) attorneys and officials, the breaking of the law, and the Executive Branch and the Justice Department's control of the FISA Court, it became clearer and clearer how much the 4th Amendment rights of US Persons (USPs) were being abused.

After that, this thesis tries to show the timeline of Snowden's leaks and his reasons for them, as well as the responses to the revelations and the immediate, short-term, and long-term effects of these leaks, including the chaotic effects on US national security, such as the weakening of US ties with other countries and the exposure of US surveillance programs and techniques to

terrorist groups. Second, this study looks at the reforms that were put in place and the new ideas for possible future reforms. It also looks at what these reforms mean for the government's responsibilities and duties to the American people, as well as the role that society and its institutions, which could act as a check on the security state and make it more open, played in pushing for and using more openness. So, the Edward Snowden case study will be used to look at how the government and mass surveillance and monitoring work in the democratic United States of America. In particular, the former NSA worker who got millions of top-secret and classified files from NSA computers and gave them to the press in June 2013 revealed the existence of the NSA's intelligence operations, surveillance systems, and programs, as well as the lack of oversight from the FISC and Congress. Some of these programs, like the Prism program, will be looked at in this study, along with information about how they work. After the 9/11 bombings of the World Trade Towers and the Pentagon, the American government had to rethink how to stop future terrorist attacks. The USA PATRIOT Act of 2001 gave the government the power to do extra-wide surveillance to protect its public and national virtues and reaffirm its fundamental thesis in the world. But in order to protect public safety and national security, in some cases, people's rights to privacy and even their freedom may be sacrificed for the sake of greater prosperity. Last but not least, this paper gives a modern perspective on Edward Snowden and rejects the idea that he was a hero and an ethical whistleblower but a hazardous traitor who put the whole nation in an unprecedentedly perilous situation.

## Abbreviations

9/11 11 September 2001 suicide attacks on New York, Washington, DC	DO Directorate of Operations (CIA)
ABI activity-based intelligence	DOD Department of Defense
ACLU American Civil Liberties Union	DOE Department of Energy
ADDNI assistant deputy director of national intelligence	DS&T Directorate of Science and Technology (CIA)
AI artificial intelligence	DSRP Defense Space Reconnaissance Program
AOR area of responsibility	EA1917 Espionage Act of 1917
ASAT anti-satellite weapon	ELINT electronic intelligence
BDA battle damage assessment	EO electro-optical; executive order
CDA congressionally directed action	EU European Union
CEO chief executive officer	FAA FISA Amendments Act of 2008
CI counterintelligence	FARA FISA Amendments Reauthorization Act of 2017
CIA Central Intelligence Agency	FBI Federal Bureau of Investigation
CIC Counterintelligence Center	FBIS Foreign Broadcast Information Service
CIG Central Intelligence Group	FIA Future Imagery Architecture
CMA Community Management Account	FININT financial intelligence
CMR civil-military relations	FISA Foreign Intelligence Surveillance Act
CNA computer network attack	FISC Foreign Intelligence Surveillance Court
CNE computer network exploitation	FISINT foreign instrumentation intelligence
COI Coordinator of Information	GAO Government Accountability Office
COIN counterinsurgency	GCHQ Government Communications Headquarters (Britain)
COMINT communications intelligence	GDIP General Defense Intelligence Program
COO chief operating officer	GEOINT geospatial intelligence
COS chief of station	HPSCI House Permanent Select Committee on Intelligence
CRS Congressional Research Service	HSINT homeland security intelligence
CT counterterrorism	HSIP Homeland Security Intelligence Program
CTC Counterterrorism Center	HUMINT human intelligence
DC Deputies Committee (NSC)	I&A intelligence and analysis
DCI director of central intelligence	I&W indications and warnings
DCIA director of the Central Intelligence Agency	IC intelligence community
DCS Defense Clandestine Service	IG inspector general
DEA Drug Enforcement Administration	IMINT imagery (or photo) intelligence
DGIAP Defense General Intelligence Applications Program	INF intermediate nuclear forces
DHS Department of Homeland Security	INR Bureau of Intelligence and Research (Department of State)
DI Directorate of Intelligence	INTs collection disciplines (HUMINT, GEOINT, MASINT, OSINT, SIGINT)
DIA Defense Intelligence Agency	IR infrared imagery
DICP Defense Intelligence Counterdrug Program	IRTPA Intelligence Reform and Terrorism Prevention Act
DISTP Defense Intelligence Special Technologies Program	ISR intelligence, surveillance, and reconnaissance
DITP Defense Intelligence Tactical Program	
DNI director of national intelligence	



<p>IT information technology  JICC Joint Intelligence Community Council  JIOC Joint Intelligence Operations Center  JMIP Joint Military Intelligence Program  JTTF Joint Terrorism Task Force  MASINT measurement and signatures intelligence  MIP Military Intelligence Program  NATO North Atlantic Treaty Organization  NCPC National Counterproliferation Center  NCS National Clandestine Service  NCSC National Counterintelligence and Security Center  NFIP National Foreign Intelligence Program  NGA National Geospatial-Intelligence Agency  NIC National Intelligence Council  NIE national intelligence estimate  NIM national intelligence manager  NIMA National Imagery and Mapping Agency  NIO national intelligence officer  NIP National Intelligence Program  NIPF National Intelligence Priorities Framework  NOC nonofficial cover  NRO National Reconnaissance Office  NRP National Reconnaissance Program  NSA National Security Agency  NSC National Security Council  NSL national security letters  NTM national technical means  OCO overseas contingency operations  ODNI Office of the Director of National Intelligence  OSD Office of the Secretary of Defense  OSE Open Source Enterprise  OSINT open-source intelligence  OSS Office of Strategic Services  PC Principals Committee (NSC)  PCLOB Privacy and Civil Liberties Oversight Board  PDB President's Daily Brief  PFIAB President's Foreign Intelligence Advisory Board  PIAB President's Intelligence Advisory Board  PIOB President's Intelligence Oversight Board  PIPs Presidential Intelligence Priorities  PSP President's Surveillance Program</p>	<p>SDI Strategic Defense Initiative  SIGINT signals intelligence  SOCMINT social media intelligence  SSCI Senate Select Committee on Intelligence  TECHINT technical intelligence  TPEDs tasking, processing, exploitation, and dissemination  UN United Nations  UNSCOM United Nations Special Commission  USDI under secretary of defense for intelligence  USA PATRIOT ACT Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism  USA FREEDOM ACT Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015  VoIP Voice-over-Internet Protocol  WIRe Worldwide Intelligence Review  WMD weapons of mass destruction</p>
--	---

(Lowenthal, 2020)

## List of Figures

<b>Figure 1 - The U.S. Intelligence Cycle .....</b>	<b>23</b>
<b>Figure 2 - The U.S. Intelligence Community.....</b>	<b>24</b>
<b>Figure 3 - Overview of NSA Privacy Protections Under FAA 702.....</b>	<b>31</b>
<b>Figure 4 - Avenues for Whistle-blowers in the Intelligence Community.....</b>	<b>37</b>
<b>Figure 5 - US Intelligence: Multiple Layers of Rules and Oversight .....</b>	<b>40</b>
<b>Figure 6 - Accountability legislation affecting the U.S. intelligence agencies, 1947–2006.....</b>	<b>41</b>
<b>Figure 7 - Research Methodology.....</b>	<b>46</b>
<b>Figure 8 - Following Snowden’s Tracks. How he got the secret N.S.A. files and passed them on - Summary.....</b>	<b>51</b>
<b>Figure 9 - Call Event Hop Scenario and Method of Counting.....</b>	<b>54</b>
<b>Figure 10 - Slide showing companies participating in the PRISM program and the types of data they provide. ....</b>	<b>56</b>
<b>Figure 11 - Google Cloud Exploitation.....</b>	<b>60</b>
<b>Figure 12 - A list of countries that might be part of the RAMPART-A program is included in the Snowden’s archives. A 2013 classified presentation showed that the NSA has top-secret surveillance treaties with 33 third-party governments, including Denmark, Germany, and 15 other EU members (Gallagher, 2014).....</b>	<b>63</b>
<b>Figure 13 – A brief representation of the 12 basic NSA surveillance reforms.....</b>	<b>71</b>
<b>Figure 14 – Domestic Internet Backbone Surveillance. ....</b>	<b>74</b>

*This page is intentionally blank.*

## Chapter I: Introduction

“I would say the best part of the Obama administration would be his continuance of the protections of the homeland using the big metadata programs, the NSA being enhanced.”

—Jeb Bush, April 21, 2015

“We have it back. The statue is free.”

—Snowden bust activists, May 7, 2015

James Madison wrote in *The Federalist*, with his signature grace and insight: "If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this; you must first enable the government to control the governed, and in the next place, oblige it to control itself" (Madison, 1788; Casto, n.d.). From the time of Thucydides, Sun Tzu, Machiavelli, and Jomini to the present, knowledge has always been a prerequisite for using power effectively. Because there is a lack of confidence in the international system, intelligence organizations exist. This is the reason for their existence. To start, they are the most effective tools for avoiding a strategic surprise. Secondly, to advance national interests and make the best choices possible in the political, economic, and military spheres, they assist the decision-making process by gathering, evaluating, and disseminating information to decision makers (both civilian and military). Thirdly, they use counterintelligence to safeguard national security. And last, as a unique component of a state's bureaucracy, they include an institutional memory system that provides decision-makers with long-term experience. In order to carry out their duties, intelligence services gather and analyze intelligence as well as engage in secret operations (Konstantopoulos, 2017). But is secrecy necessary? Secrecy is often regarded as the key element that sets intelligence apart from other types of information utilized by national security decision-makers. Even if this definition of intelligence is overly limited, it serves as a good place to start when talking about the special role that intelligence plays in American democracy. However, the United States has had to count on covert intelligence since its declaration of independence, with Gen. George Washington reigning as the country's first spymaster. Yet, throughout US history, there has been dissatisfaction with espionage, monitoring, and dependence on secret intelligence. When the nation was at war, secret intelligence

and surveillance were grudgingly considered necessary but were renounced when peace was declared (George, 2020).

Undoubtedly, the "War on Terror" has been waged since 9/11, and after some degree of democratization of intelligence in the 1990s, it seems that this has made the conflict between secret intelligence and respect for human rights even more pronounced. The main cause of this is the altered understanding of security dangers in light of the "new" terrorism. Informants, interrogation, intelligence sharing, performance, and covert action are some of the most controversial intelligence operations that are examined in relation to the responsibilities of law, rights, and ethics in intelligence. In order to safeguard human rights without interfering with agencies' capacity to uphold public safety, supervision must be revitalized (Gill, 2009).

Following this, on June 5, 2013, Edward Snowden stunned the entire world when he gave highly secret documents from the National Security Agency (NSA) to a British daily newspaper called "The Guardian." These documents revealed that the Foreign Intelligence Surveillance Court (FISC) had given Verizon a secret order to collect data about all phone calls made in the US and abroad. Snowden said that the NSA was spying on American citizens by collecting a lot of "telephony metadata." This was done with permission from Congress and the President. Right away, President Obama and Senator Diane Feinstein tried to downplay how Orwellian the program was. They did this by saying things like, "It's just metadata." (Atkins, 2014). Also, the impact that the United States' collection of data and metadata from millions of individuals had on Americans has been a major topic of discussion about NSA spying activities. It is crucial to note that the NSA affects people worldwide; in fact, as was previously established, it primarily monitors calls and other forms of contact between the United States and other nations. The European Union's decision to put pressure on the US is one example of how Europe and other US allies have attempted to distance themselves from the NSA's surveillance techniques. Although the NSA denied collecting data from millions of Americans in a statement issued months before Snowden's papers were leaked, there is no guarantee that other governments or mass surveillance programs are not being carried out by nations that have denied involvement in monitoring (Olesen, n.d.).

Snowden's leaks did not happen in a vacuum; they have their own cultural and historical background (Wood, 2009). From J. Edgar Hoover to Watergate to the Bush Administration's warrantless wiretapping, the US has a long history of government spying. After 9/11, a climate of dread and danger, coupled with the well-known inability of the CIA to recognize the threat, made

intelligence overreach possible. Simultaneously, the ever-expanding usage of the Internet, and especially platforms like Google, Facebook, and Skype, had normalized the commercialization of personal data (Bauman, et al., 2014; Richardson, 2016). As national security became an increasingly dominant element in political discourse, the Western public either thought about or was dimly aware that monitoring programs had significantly grown. At the heart of this discourse about national security and public consensus is the often-discussed relationship between secrecy and a democratic, open state. The academic emphasis on the Intelligence Community's post-9/11 internet discourse has brought to light important national security issues. According to scholars, the growth of the US intelligence community in the twenty-first century is based on the idea of the "state of exception," which allows for increased political power based on the maintenance of a state of constant emergency. The agencies' behavior is secretive in the name of national security, and it also serves as a weapon to maintain their "legitimacy of power" (Richardson, 2016; Mirfattahi, 2019).

According to information stolen from NSA rogue contractor Edward Snowden, ongoing disclosures about US communications-intercept activities have sparked strong feelings in a number of communities. Concerned with problems of personal freedom and data privacy, civil liberties organizations have raised anxiety about the widespread nature of the NSA's bulk data gathering. States that were found to have participated in such a collection with the organization have been humiliated. Countries that thought themselves to have favorable ties with the United States but were vulnerable to its clandestine intelligence collection responded with varying degrees of fury. Some of this fury was genuine, but the majority was created for domestic and political purposes or with the aim of gaining a policy benefit from the embarrassment caused by the United States and its allies. Customers' faith in the main US technology businesses and service providers that have willingly or in response to legal orders worked with the NSA has declined, with undetermined but possibly substantial ramifications for their future commercial prospects (Inkster, 2014).

Additionally, when considering Snowden's motivations, one may ask whether he believes he has accomplished his goals (Lands, 2017). *"They're excusing themselves from accountability to us at the same time they're trying to exert greater power over us,"* Snowden said in an interview. This statement perfectly expresses Snowden's thoughts about the US government and its practices of mass data collection (Snowden, 2016). According to him, his primary motivation for releasing the materials was his belief that collecting data on Americans is unethical. In contrast, another can

conclude from this that Snowden was motivated by a desire for pure recognition. These discoveries had a favorable effect on policy, but in return, many different capabilities had to be destroyed in order for them to be made public, hurting national security (Johnson, et al., 2014; Johnson, 2015).

Therefore, this thesis addresses the issues raised by the 2013 disclosures of two National Security Agency (NSA) surveillance programs. One is known as "Bulk Collection of Telephone Metadata," which involved gathering, maintaining, and analyzing records of a substantial portion of phone conversations that had been made and received in the United States ("phone surveillance"). The second program, called "PRISM" which involved targeting non-Americans and gathering private electronic communications from a number of big web providers, including Google and Facebook. Also, this project concentrates on the particular concerns generated by these two initiatives, despite the fact that their characteristics and concerns are equally applicable to other national security programs (Etzioni, 2014).

In short, this paper evaluates the pertinent topics using a realistic approach. To be more exact, Chapter II of the project will examine the Intelligence and Democracy theories. In Chapter III, the "Snowden's Timeline of Events" that took place back in 2013 will be analyzed. Therefore, in chapter IV the below four (4) questions will be discussed and probed:

- 1: Snowden's motives: A Whistleblower or a Traitor?
- 2: What are the consequences of the Snowden revelations?
- 3: How the institutions which might act as counterweights and overseers to the security state have been changed after the Snowden revelations? What are the proposals for protection of classified information? and
- 4: Intelligence vs Democracy: How to achieve harmony between security and privacy and shape the pathway to reform?

## Chapter II: Intelligence and Democracy.

“The important thing about foreign policy is this: There are a lot of important objectives: democracy is one of these, security is another, prosperity is another one, environment is another one. So you have to see how you give emphasis to these objectives at any moment in time.”

- “Henry A. Kissinger, interviewed by Suchichai Yoon, Nation, Bangkok newspaper, March 8, 1999, A5.”

### II.1 Democracy.

*Definition of Democracy, the United States' political system and its Principles.*

Democracy is a complex phenomenon that has a wide range of interpretations and applications (Haggerty & Samatas, 2010). There is not a single democracy, but rather a number of distinct and rival democracies (Guitar, 2018). The concepts of liberty, democracy, equality, individual responsibility, and civic duty, while they have different implementations, are still shared by all democratic philosophies. Democracy, when it transitions from theory to practice, is fundamentally a method of making decisions (Cohen, 2012). By their very nature, democracies must be pledged to government by the people, in which the needs of the public are managed jointly. Democracy may be enforced by permitting unrestricted debate on public problems (Guitar, 2018). A democratic government is one in which all members of the population are considered equal (Mill, 1861). In general, democracy is a system of governance in which the people have the power to make decisions (Guitar, 2018).

The US political system is somewhat unique compared to other democracies. The nation is a federal constitutional republic. Along with the Congress and the courts, the President of the United States has some authority. The national government is reserved with this authority. The federal government has control over the state governments. The U.S. regime is based on a set of ideas that argue for a constitutional republic (Čirjak, 2020). The rationale behind this claim is shown below. Notwithstanding, the catalog is not complete, but it serves as a starting point for researching the American experience in self-government (Bill of Rights Institute, 2022):

(a) Natural Rights & Foundations (the fundamental concepts that serve as the cornerstone of



American government): Natural/Inalienable Rights, Liberty, Equality, Justice.

(b) Consent & Republican Government (the republican principles that are the foundations for keeping the sovereignty of the people in government): Majority Rule/Minority Rights, Consent of the Governed/Popular Sovereignty, Democracy, Republic.

(c) Limited Government (to maintain governing authority within its legitimate extent, the government must be restrained and offer individuals options to defend themselves against arbitrary power): Rule of Law, Due Process.

(d) Constitutional/Auxiliary Precautions (there must be laws that constrain both the actions of the government and the people in order to maintain them within these constrained parameters): Separation of Powers, Checks and Balances, Federalism.

(e) Bill of Rights (as a last line of defense against government misuse, the Founding Fathers enshrined a list of rights they deemed crucial to the preservation of their constitutional system): Freedom of Religion, Freedom of Speech, Press, and Assembly and Private Property, which means individuals' inherent right to produce, acquire, and manage their own property, beliefs, talents, and views, as well as the rewards of their work, (Bill of Rights Institute, 2022).

*The 4th Amendment, the reasonable Expectation of Privacy, National Security, Freedom of Information and Human Rights after 9/11.*

The concept of privacy has proven difficult to articulate clearly. Initially, privacy is a legitimate right that an individual has in relation to other people when it comes to (a) other people having information about him or her or (b) other people observing or perceiving him or her, including a person's activities, interactions, and so on. Secondly, the right to privacy is tightly correlated with one of the most important moral values, which is the right to be independent. Thirdly, some privacy is merely required for an individual to accomplish his or her goals, whatever they may be (Dover, et al., 2017). Because of its inherent and practical value, privacy is often seen as a crucial concern. It is important because violating someone's privacy can lead to serious physical, financial, or social consequences. Our demand for privacy will continue to exist as long as we live in a culture where individuals are typically intolerant of living styles, habits, and ways of thinking, and where human weaknesses tend to become the objects of disrespect or disapproval. For instance, blackmail derives much of its impact from the material consequences that individuals

would suffer if specific behaviors were revealed (Bellaby, 2012).

To illustrate, in 1791, the American people adopted the Fourth Amendment as part of the Bill of Rights to forbid the newly constituted federal government from committing breaches into their lives. It reads (Thompson II, 2014): *"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 of affirmation, and particularly describing the place to be searched and the person or things to be seized"*, (Congress.gov, 2020).

Admittedly, the 4th Amendment protects against unreasonable seizures and searches. In most cases, a warrant is required for police to conduct a search. Similarly, intelligence officers are not permitted to look wherever they choose in quest of information. The due process clause of the Constitution says that the government can't take away a person's life, freedom, or property in an unfair or unreasonable way. For instance, a fair trial must be conducted before the court may deny a person's right to freedom by imprisoning him or her. Then, the Foreign Intelligence Surveillance Act of 1978 (FISA) was passed by Congress to safeguard the personal freedoms of American people. It forbids government organizations, including the Federal Bureau of Investigation (FBI) and National Security Agency (NSA), from wiretapping and eavesdropping on US residents and those who are deemed to be "US persons" without first meeting a number of conditions. FISA lets agencies get authorization to wiretap and search people who are not US citizens but who work for foreign forces or agencies of foreign forces in the US. FISA lets the government spy on people who are U.S. citizens only when they are acting for a foreign power (Jensen III, et al., 2018).

The first clause of the Amendment, which mandates that all searches and seizures must be lawful, and the second clause, which demands that all warrants satisfy certain minimum requirements, including specifically describing the location to be searched and the items to be seized, have been difficult for the federal courts to reconcile over the years (Sundby, 1988). In every case, the Court must first decide whether the Fourth Amendment's limitations are even applicable. This is accomplished by determining whether the government has undertaken a "search", a constitutional term that cannot be defined by a simple dictionary meaning but rather requires the application of the complex, sometimes conflicting Fourth Amendment case law of the Supreme Court (Thompson II, 2014).

Liberal democracies, by definition, uphold citizens' right to privacy while requiring open

governance. In a limited sense, covert collection of information on its population is opposed to democracy. Governments should not be authorized to monitor people's ideas or opinions as long as they do not lead to illegal behavior. However, much like governmental secrecy, privacy has its bounds. There is a common misconception that Americans must decide between their individual freedom and public security. Public safety and individual privacy may be reasonably compromised. If the federal government has a good basis to suspect that someone is collaborating with a foreign power or is a member of a terrorist group with the intention of attacking innocent Americans, listening in on that person's phone calls is scarcely a serious overreach. So, it is critical to differentiate between a person's civil freedoms and his or her right to privacy (George, 2020).

However, prior to the 1978 enactment of FISA (Foreign Intelligence Surveillance Act) by Congress, a number of lower federal courts supported warrantless electronic monitoring carried out for national security reasons. These courts interpreted the Fourth Amendment to exclude searches performed for foreign intelligence reasons from the warrant requirement. After 9/11, the government focused on these precedents to claim that President Bush's NSA program of domestic monitoring did not violate the Fourth Amendment, despite the fact that surveillance happened without a warrant or reasonable cause to think it would disclose criminal intent. FISA modifies the legal environment in which the 4<sup>th</sup> Amendment reasonableness of NSA programs will be evaluated. To determine whether warrantless NSA surveillance is justified, it is necessary to evaluate options. FISA has established an option that, according to past experience, simplifies the process of obtaining court permission for monitoring related to national security. The Fourth Amendment is presumed to be violated by monitoring conducted outside of FISA unless it is necessary to protect national security. Even though it violates FISA, surveillance that is authorized outside of FISA and supported by a real emergency, fulfills Fourth Amendment requirements and is within the President's authority. This is due to the fact that FISA violates the idea of separation of powers to the degree that it prohibits the President from taking steps that he or she reasonably thinks are required to react to real national security crises. Hence, President Bush's NSA surveillance program violated the Constitution because it exceeded the President's congressionally granted authority to react to actual national security situations (Seamon, 2008).

Since 9/11, stopping terrorism and maintaining high levels of national security have appeared to be top priorities everywhere, but especially in the United States. After 9/11, the US and some of its partners started the "War on Terror," which, according to people who work for

human rights, has hurt international human rights laws (Roy, 2018) (Freeman, 2011). Additionally, it highlighted the tensions between security and freedom, whereas the effectiveness of executive and legislative oversight has been called into question in light of the use of more invasive monitoring and interrogation methods, as well as intelligence-driven targeted murders (George, 2020). The implementation of a number of anti-terrorism laws and military operations were the two main components of the "War on Terror." According to a number of studies, US political rhetoric and foreign policy-making procedures are naturally characterized by the conflict between upholding human rights and preserving national security. Some considered it's possible that US officials did not see national security and human rights as inherently linked and connected but rather they gave national security priority at the cost of human rights. The fight against terrorism projects difficulties for the human rights system because of the growth of the anti-terrorism counter-norm that was embraced by a sizable portion of US people as well as certain US allies overseas after the events of 9/11. Through political discussion and judicial rulings, the "War on Terror" has also reinforced some principles. Courts and legislatures disagreed with some of the executive's proposed limits on human rights; thus, they rejected such restrictions. Although there is widespread agreement that terrorism must be tackled in light of human rights, there is less agreement on how to achieve it (Roy, 2018; Freeman, 2011; Addicott, et al., 2012).

Later, the concept of security is fairly ambiguous. It is often used to refer to many types of collective security, such as national security (in the face of foreign military aggression), community security (in the face of law and order disturbances), and organizational security (in the face of fraud, breaches of confidentiality, and other forms of misconduct and criminality). In other instances, it refers to a person's physical safety. In this context, physical security refers to the absence of dangers to one's life, liberty, or personal property, the last of which is a fundamental human right. However, apart from discussions about the size of security, there are also concerns about the kind of security. There is a distinction between informational and non-informational security (Dover, et al., 2017). Namely, nearly every government has regulations concerning the safeguarding of national security-information. Information freedom laws usually have an exception for information related to national security, which is a concept that is defined differently in different countries. In addition, several nations have State Secrets or Official Secrets Acts or sections in their penal laws that restrict the disclosure of information and make its unauthorized disclosure a crime. Furthermore, a more recent phenomenon is the adoption of rules on the

protection of classified information that are more specific about the kinds of information that must be safeguarded, as well as the nature and length of such protection. This is notably common in Central Europe and Asia. Many countries have also passed legislation allowing access to the secret police records of former communist regimes. These laws often collide with the freedom of information. An assumption that information should be publicly disclosed is often created by FOI (Freedom of Information) laws. These extensive access exemptions usually cause severe worries about the function of intelligence services, even in some of the oldest democracies. In short, National security is crucial for every country, but the balance is often biased (Born & Caparini, 2007).

## **II.2 Intelligence.**

### *Definition of Intelligence and the Intelligence Cycle.*

What is intelligence? Intelligence consists mostly of clandestine actions—targeting, collecting, analyzing, distributing, and taking action—designed to increase security and/or preserve dominance compared to rivals by notifying them in advance of dangers, risks, threats, and opportunities. According to Sherman Kent, "intelligence" may also refer to the institutions that conduct these actions and their "product." To differentiate intelligence from a plethora of other "knowledge management" approaches, keep in mind that its objective is security, a portion of it will be undertaken secretly, and since it is constantly relevant to others, it will elicit criticism (Gill, 2012). Other intelligence-related actions, such as counterintelligence and covert action, are now seen as instances. The National Security Act of 1947, which established the CIA, demonstrates the difference between strict definitions and reality. It entrusted the following duties to the CIA (Hastedt, 1991):

- a) To provide advice to the National Security Council on intelligence-related national security problems.
- b) To offer suggestions to the National Security Council about how government departments and agencies can work together on intelligence.
- c) To connect and assess intelligence and ensure its proper distribution across the government.
- d) To help existing intelligence agencies by giving them more tasks that the NSC thinks could be

done more efficiently by a central body.

e) Conduct other duties and tasks related to national security intelligence as directed by the National Security Council (Hastedt, 1991).

Yet, many individuals don't perceive any difference between intelligence and information other than the likelihood that it is hidden. However, it is crucial to make a distinction between the two aforementioned definitions. Information is everything that can be known, regardless of how it was found. Information that has been gathered, analyzed, and focused to fulfill policymakers' declared or recognized goals is referred to as "intelligence." Among the many different types of information, intelligence is one of them. The identification, acquisition, and analysis of intelligence are in response to the demands of policymakers. All intelligence is information, but not all information is intelligence (Lowenthal, 2020).

The following are a few brief explanations of intelligence that are considered to be differentiated either by their origin or by their clarity (Andrew, et al., 2020):

a) *"The term 'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons."* - the National Security Act of 1947,

b) *"Intelligence deals with all the things which should be known in advance of initiating a course of action."* - The Clark Task Force of the Hoover Commission in 1955,

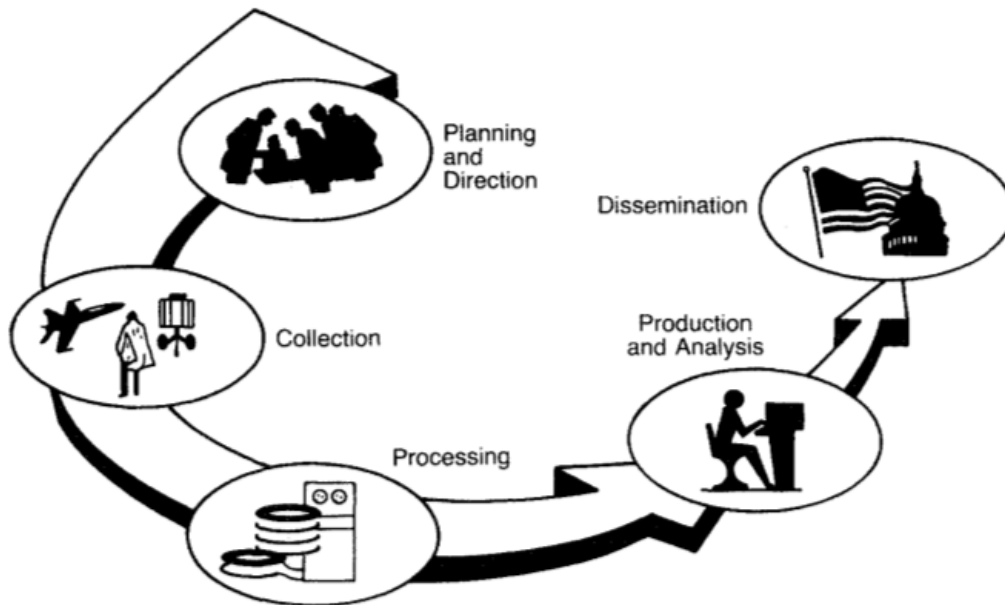
c) *"The Commission believes it preferable to define 'intelligence' simply and broadly as information about 'things foreign' – people, places, things, and events – needed by the Government for the conduct of its functions."* - A report from 1990s produced by the Brown-Aspin Commission,

d) *"Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us – the prelude to decision and action by US policymakers"* – the CIA (Andrew, et al., 2020).

Moreover, the term "intelligence cycle" is used to describe how states manage their intelligence communities, which are made up of a large number of knowledge-intensive industries. The typical cycle starts with the targeting of assets used for collecting, such as human spies, hackers, or satellites. After being gathered, raw intelligence is processed, verified, analyzed, and debated. Then, a condensed amount of information is given to the policymakers to help them make decisions. Either in the aftermath of a significant crisis or as part of a normal assessment, the target

list is reevaluated, and the cycle begins again. This traditional idea of an intelligence cycle was the basis for the early policy-oriented writings on intelligence, which tried to describe how the cycle worked. The process remains essential since it includes and links the vast majority of intelligence agencies' activities and highlights how they inform the government's broader operations. (Andrew, et al., 2020).

**Figure 1 - The U.S. Intelligence Cycle**



[Source: From *Fact Book on Intelligence*, Office of Public Affairs, Central Intelligence Agency, April 1983, p. 16., (Johnson, 1989)]

### *Intelligence Community (IC).*

The Intelligence Community is an integrated enterprise made up of 17 Executive Branch agencies and organizations (often referred to as "IC elements") that collaborate to advance national security and carry out a range of intelligence-related operations. The DNI, who serves as the IC's head, establishes the organization's strategic goals via the National Intelligence Strategy. Each IC member makes a contribution by carrying out the organizational mission in line with its statutory obligations (Coats, 2019). These organizations are in charge of three main tasks: gathering and analyzing data from all over the world (a process known as "analysis"); safeguarding American government secrets from foreign intelligence services and other spy agencies (a process known as "counterintelligence"); and covertly influencing events abroad to advance American interests

through political interference, paramilitary activity, economic disruption, and other means. Intelligence is gathered through technical means (like satellites and reconnaissance planes, or "technical intelligence," or "TECHINT"), human means (classic espionage, or "human intelligence," or "HUMINT"), and Open-Source intelligence means (OSINT) which is the process of gathering data from sources that are published or otherwise made accessible to the public, including broadcast TV and radio, social media, and websites (Johnson, 2002; Sharma, et al., 2021; microfocus, n.d.).

**Figure 2 - The U.S. Intelligence Community**



Source: (Jensen, III, et al., 2018)



### *Ethics of Intelligence.*

Next, "Ethics" is a social, religious, or civil code of behavior considered correct, especially that of a particular group, profession, or individual. In terms of history, the ethics of intelligence services have relatively recently been the focus of public debate (Omand & Phythian, 2018; Collins, n.d.). Ethical questions surrounding the use of intelligence have long been controversial. By its very nature, intelligence entails the collection of information that other players would want to keep hidden; hence, intelligence depends on intelligence officers to deceive, incite, and coerce in ways not acceptable for members of the general public. On the one hand, stating that intelligence is an essentially immoral activity disregards both the significant role that ethics serves in the lives of individuals and political society, as well as the ethical function that intelligence may play. On the other hand, as Allen Dulles stated in 1963, while he was the director of the Central Intelligence Agency (CIA) of the United States and the chief intelligence adviser to the President and the National Security Council, *"the last thing we can afford to do today is to put our intelligence in chains"*, means that the ability to gather relevant information at the appropriate time is critical to intelligence collection, and there are concerns that limiting this – either by limiting the tools available or by delaying decision-making – creates a window of opportunity for the next terrorist strike to be successful (Bellaby, 2017; Bellaby, 2018). In short, based on the following points, it is possible to take a morally valid position (Omand & Phythian, 2012):

- a) Public safety is the obligation of security and intelligence agencies. They have to find and then use covert information to help deal with national security-related threats.
- b) Because getting secret intelligence requires overcoming the efforts of others to stop you from getting it, it always involves a moral hazard.
- c) Intelligence actions may be regulated by an ethical code that incorporates "Just War" ideals and respect for human rights, including the ban on torture and harsh treatment.
- d) Intelligence relies on secret sources and procedures to safeguard the lives of the individuals involved. Senior judges and legislators who can be trusted to enter the "ring of secrecy" and provide people with assurance that ethical norms are being followed must act as proxies for oversight (Omand & Phythian, 2012).

At the same time, the US is dedicated to protecting privacy and civil rights, but excessive intelligence gathering may weaken these ideals. To illustrate, it is substantial to pay close attention to the following principles: Firstly, national security and individual privacy are two distinct types

of protection that the US government must simultaneously safeguard. Secondly, risk management is the key responsibility; there are many dangers involved, and each one has to be taken into account (risks to privacy, freedom, civil liberties, U.S. relations with other countries, and trade and business, particularly international commerce). Thirdly, the government should consider its advantages and costs while making choices (to the extent feasible) (Clarke, et al., 2014).

Following this, it is crucial to construct a two-part ethical framework that defines the features of intelligence collection that may be unethical while also including intelligence's function in defending the political community. Initially, the ethical framework will argue that intelligence collection may be considered "unethical" since it may provoke "harm" to individuals. By recognizing the bad side of intelligence, it's possible to discern whether it's justified. The second part of the ethical framework will argue for just intelligence principles. These principles are a series of parameters based on the "Just War" tradition that, by citing just cause, legitimate authority, right intention, last resort, proportionality, and discrimination, explain the conditions under which the damage produced is justifiable. In particular, and in order to fully understand the role of these principles and their connection with intelligence collection, it is essential to be explained below (Bellaby, 2012):

a) Just cause: intelligence collection and the damage it might cause must be justified by a significant threat. b) Authority: There must be a legitimate authority representing the political community's interests that approves the activity. c) Intention: The methods should be used to achieve the specified objectives as well as other goals (political, economic, and social); d) Proportion: Benefits should outweigh costs. e) Last resort: less dangerous actions should be tried first; and f) Discrimination: targets should be legitimate or illegitimate (Bellaby, 2012).

### *Espionage Act of 1917.*

Initially, the Espionage Act, one of the federal government's most potent laws, was also regarded as one of its most controversial pieces of legislation. It was enacted during WWI to curb espionage and public criticism of the government's war operations (Bomboy, 2022). In 1917, Woodrow Wilson urged Congress to establish the Act. In fact, to block public opposition against U.S. involvement in WWI, the legislation banned gathering or publishing national security information that may be used against the U.S. In 1918, a set of amendments banned speech that

was seen as unpatriotic or hurtful to the United States. How has it been used? The statute criminalizes the unlawful retention or publication of national defense information that might damage the U.S. It was passed decades before the executive branch created the present national security classification system. Similarly, Espionage Act-protected documents are usually classified. The Espionage Act and executive branch classification function in parallel, so a document doesn't need to be classified to be protected by the law (Barnes, 2022).

In addition, recent disputes over the Espionage Act have focused on the First Amendment and people's freedom to disclose classified information to the press if they think the government has behaved inappropriately. Particularly, opponents have cited Justice Reed's remarks in the "*Gorin*" ruling about the act's broader meaning of the term "national defense." (Bomboy, 2022).

Since 1917, the Espionage Act has been used to prosecute numerous notable individuals. For example, both New York-born Julius and Ethel Rosenberg were prosecuted under the Espionage Act in 1951, convicted of being Soviet spies, and killed in 1953. The Espionage Act remains in force to this day. Most notably, former National Security Agency contractor Edward Snowden was charged with espionage crimes in 2013 for leaking U.S.-classified information about government surveillance activities (Kratz, 2017). Because of the nature of the evidence related to national security and the activities that need to be revealed to prove the illegal disclosure of classified information, prosecutions under the Espionage Act are hard to carry out. Vital evidence could be deemed classified and kept secret from the defendant, hindering the ability to have a fair trial. The Act is problematic when applied to the exposure of classified material since it ignores intent, a common factor necessary for the conviction of criminal activities. As a result, whistleblowers who provide information to the media to expose unlawful government conduct rather than to assist foreign nations in harming the United States sometimes are not protected. Due to the fact that national security is at stake, the standard is low (Marks, 2021).

### *FISA History, Acts and Amendments.*

In 1976, the Church Committee reviewed intelligence activities that had been performed over the previous years. The Committee ruled that government officials violated Title III and the Fourth Amendment by spying on U.S. residents without any valid suspicion of criminal behavior, much less affiliation with foreign forces. The committee's ultimate decision rejected the President's

or IC's inherent right to conduct unlawful and warrantless electronic surveillance. As political pressure mounted, the Ford Administration agreed to endorse legislation requiring judicial review of foreign intelligence surveillance in 1976. The FISA Act was signed into law by President Jimmy Carter in 1978 (Jensen, III, et al., 2018). Special intelligence courts must authorize national security wiretaps under FISA. The Church Committee recommended this law to reconcile national security with the U.S. Constitution. Consequently, FISA created special courts with specially authorized judges to issue warrants for searches, seizures, and wiretaps when national security is at risk. FISA warrants may have been rapidly approved in a case of major danger, which sometimes necessitates finding out immediately what someone is doing or who they are talking to. Bush has disregarded FISA because he has found it inconvenient (Miller, 2008). Currently, eleven federal district court judges comprise the Foreign Intelligence Surveillance Court (FISC). Then, the Foreign Intelligence Surveillance Court of Review (FISCR) was established by FISA to review judgments issued by the FISC. The U.S. Supreme Court has the final decision-making power in FISA-related disputes. FISC hearings are closed-door and confidential; even defense lawyers can't review FISA applications. Also, the court does a weaker analysis of probable cause. The government must show that the person being spied on is a threat to national security and that one of the main goals of the investigation is to collect foreign intelligence. If the government has enough proof, the court will issue an order letting the government's application go forward (Jensen, III, et al., 2018).

On the contrary, the Foreign Intelligence Surveillance Act (FISA), passed after the Watergate scandal, allowed the government to covertly eavesdrop on Americans in their own nation. Originally, it was enacted to let the government gather foreign intelligence material regarding conversations with "agents of foreign countries." (American Civil Liberties Union, n.d.) However, today, the government uses this once-narrow provision to overcome the Constitution. Namely, as part of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", also known as the USA PATRIOT Act, Congress passed two amendments to the Foreign Intelligence Surveillance Act (FISA). (Congressional Research Service, 2021).

In particular, Section 206 of the PATRIOT Act authorizes investigators to trace suspects with the same FISA warrant even if they change devices. Federal officers no longer need a separate warrant for each suspect's phone, email, apartment, or other facility (Rosenbach & Peritz, 2009).

Then, Section 215 expanded the scope of documents that might be sought under FISA to also include "any tangible thing." Thus, Section 215 of the Act changed the rules about how federal officials can get business data and other "tangible records." Business data, phone service provider data, apartment rental data, driver's license archives, library documents, book sale files, gun purchase records, tax return data, educational records, and health records are examples of "tangible records." Additionally, it reduced the standard for a judge to order warrant production (Congressional Research Service, 2021). Also, under this clause, federal investigators may force third-party record holders, such as telecom providers, banks, or others, to reveal these documents. The U.S. must prove that the documents are pertinent to a terrorist or counterintelligence investigation to invoke this clause. Applications for orders including libraries, book sales, guns, taxes, educational records, or other sensitive information must be personally approved by the FBI Director or the FBI Deputy Director. Annually, Congress must be updated on these orders. In contrast, Section 215 critics say the "relevancy" criteria may be used to get nearly anything and that Congress should set a higher standard. Some say library and other record restrictions aren't strong enough to preserve privacy and First Amendment rights (Rosenbach & Peritz, 2009). Thirdly, Section 505 of the USA PATRIOT Act enabled the use of National Security Letters (NSLs) when seeking information "relevant" to recognized national security inquiries to safeguard against global terrorism or underground intelligence operations. A National Security Letter is a type of administrative subpoena (McDermott, 2018).

Next, the Intelligence Reform and Terrorism Prevention Act of 2004 included a third FISA amendment (IRTPA). IRTPA Section 6001(a), also known as the "lone wolf" provision, modified the requirements for FISA-authorized searches. It allows surveillance of non-U.S. persons involved in international terrorism without proof tying them to a foreign state or terrorist group (Congressional Research Service, 2021). Later, in 2008, Congress replaced Section 702 of FISA with Public Law 110-261, the 2008 FISA Amendments Act. This version codifies the PSP: It allows bulk collection, from American corporations, of Americans' international communications (telephone calls and emails, including metadata), as long as the government is targeting foreigners abroad. According to this section, surveillance may be permitted by the Attorney General and Director of National Intelligence without prior permission from the FISC, as long as minimization standards and general procedures approved by the court are maintained. The court merely accepts yearly "certifications" permitting the targeting of large groups of persons rather than approving






each target separately. Agents from the NSA decide which phone lines and email accounts will be tapped, and there is no rule that says these phones and email accounts must be foreign. Only the program's overall target must be foreign (McDermott, 2018)

However, in summer 2013, media reported on National Security Agency (NSA) foreign intelligence operations, including the bulk collection of telephone metadata under Section 215 of the USA PATRIOT Act. After a one-day gap, Congress passed the USA FREEDOM Act, which limited the government's foreign intelligence operations and extended the no longer-valid guidelines until March 15, 2020. Notwithstanding the fact that these clauses expired on March 15, 2020, grandfather clauses allow them to continue to apply to investigations initiated or possible violations that occurred prior to that date (Congressional Research Service, 2021).

Eventually, after months of hearings and significant public debate, Congress authorized a six-year renewal of the FISA Amendments Act of 2008 in January 2018. FISA Section 702 enables warrantless NSA searches of foreigners' communications. The procedure gathers American data. Section 702 of the FISA makes intelligence-collection operations targeting non-Americans abroad subject to its jurisdiction. These foreigners make contact with Americans; thus, the latter are intercepted. The FISA Amendments Reauthorization Act of 2017 extends Section 702 for six years, to December 31, 2023, and includes new restrictions on querying surveillance databases, prohibiting the continuation of certain forms of collection about a target that were not directly addressed to or from that target unless Congress approves such collection within 30 days of being notified of the resumption, and requiring additional reporting by the Executive Branch (American Civil Liberties Union, n.d.; Wikipedia, n.d.).

Beside this, 2018 legislation that had been passed by former President Trump made the unlawful withdrawal and preservation of classified documents, information, and archives a felony crime indictable by 5 years in jail and/or a fine (Bump, 2022).

**Figure 3 - Overview of NSA Privacy Protections Under FAA 702**

 <p><b>TARGETING</b></p>	<ul style="list-style-type: none"> <li>• Targeting must be for a valid foreign intelligence purpose in response to National Intelligence Priorities.</li> <li>• Targeting must be under a Foreign Intelligence Surveillance Court (FISC)-approved FAA 702 Certification and limited to non-US Persons located overseas.</li> <li>• All targeting is governed by FISC-approved targeting procedures.</li> </ul>	<ul style="list-style-type: none"> <li>• Targeting of US Persons or any persons located inside the United States is strictly prohibited.</li> <li>• Reverse-targeting of US Persons is prohibited.</li> </ul>
 <p><b>COLLECTION</b></p>	<ul style="list-style-type: none"> <li>• Specific communications identifiers (for example, phone numbers or e-mail addresses) are used to limit collection only to communications to, from, or about a valid foreign intelligence target.</li> </ul>	<ul style="list-style-type: none"> <li>• Intentional collection of wholly domestic communications (that is, all communicants are in the US) is prohibited.</li> </ul>
 <p><b>ANALYSIS/ EXPLORATION</b></p>	<ul style="list-style-type: none"> <li>• Queries into collected data must be designed to return valid foreign intelligence.</li> <li>• Overly broad queries are prohibited.</li> </ul>	<ul style="list-style-type: none"> <li>• Upon additional authorization and oversight, queries using US Person identifiers are permitted for foreign intelligence purposes.</li> <li>• Any wholly domestic communications (that is, all communicants are in the United States) must be destroyed upon recognition.</li> </ul>
 <p><b>DISSEMINATION</b></p>	<ul style="list-style-type: none"> <li>• Disseminations to external entities, including Executive Branch agencies and select foreign partners, are made for valid foreign intelligence purposes.</li> </ul>	<ul style="list-style-type: none"> <li>• US Person information is protected in reporting unless necessary to understand and assess the foreign intelligence, evidence of a crime, or other exception applies.</li> </ul>
 <p><b>RETENTION</b></p>	<ul style="list-style-type: none"> <li>• Raw data is destroyed after two years or five years (depending on the collection source) after the expiration of the certification under which it was acquired.</li> </ul>	

**CLAIMER:** This overview is a quick reference guide and is not intended as substitute for the minimization procedures and their implementation.

[Source: (CLARKE, et al., 2014)]

*Executive Order 12333.*

The Executive Order 12333 issued by U.S. President Ronald Reagan on December 4, 1981, was designed to increase the powers and duties of U.S. intelligence organizations and to instruct the heads of U.S. government agencies to fully cooperate with CIA requests for information. “United States Intelligence Activities” was the name given to this executive order. On July 30,

2008, President George W. Bush amended Executive Order 12333 to enhance the role of the DNI (Wikipedia, 2022; Office of the Press Secretary, 2008). It was developed in the aftermath of Watergate and the Foreign Intelligence Surveillance Act, a law approved by Congress that controls espionage done on persons based inside the United States. Since FISA only covers certain types of espionage, the President states that the executive branch is still free to spy on foreigners without much or any oversight from Congress (Jaycox, 2014).

The Executive Order accomplishes 3 goals: (a) it defines what it covers; (b) when and how agencies may conduct surveillance; and (c) under what circumstances they can conduct surveillance. The E.O. establishes guidelines for surveillance on United States citizens and on anyone within the country. Additionally, it instructs the Attorney General and others to develop new laws and guidelines for what data may be gathered, stored, and shared (Jaycox, 2014). However, according to Snowden's revelations, the American government runs several expansive programs in accordance with EO 12333, many of which seem to entail mass data collection from Americans. These programs included, for instance, the NSA's gathering of billions of cellphone location records every day, its recording of each and every conversation made from, to, and within at least two nations, and its covert interception of information from Google and Yahoo user accounts (ACLU, 2022) .

In a 2007 internal surveillance manual, the NSA itself provides the following description of EO 12333 (Abdo, 2014):

~~(U//FOUO)~~ Executive Order 12333 was issued by the President of the United States to provide for the effective conduct of US intelligence activities and the protection of the rights of US persons. **It is the primary source of NSA's foreign intelligence-gathering authority.**

(Source: <https://www.aclu.org/news/national-security/new-documents-shed-light-one-nsas-most-powerful-tools> , <https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf#page=4>)

The following is a parallel definition from a "Legal Fact Sheet" on the Executive order, which the NSA issued precisely one week after Snowden's initial disclosure (Abdo, 2014):

**(U) NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO) 12333.**

(Source: <https://www.aclu.org/news/national-security/new-documents-shed-light-one-nsas-most-powerful-tools>)



*Executive Order 12333, Section 215 of the Patriot Act, FISA Amendments Act: A Comparison.*

Executive Order 12333 gives the government the power to perform surveillance outside the US, even though FISA mostly conducts surveillance inside the US. In general, EO 12333 gives US intelligence services the fundamental legal basis for gathering foreign "signals intelligence" information which is data gathered via communications and other material passed or accessed by radio, wire, and other electromagnetic methods. Next, in contrast to FISA, EO 12333 does not require digital communications service providers to help with surveillance. The technical details are still secret and hard to understand, but the NSA has clarified that they include exploiting vulnerabilities in telecommunications infrastructure (Lawne, n.d.).

Many articles have concentrated on Section 215 of the Patriot Act (used to gather all Americans' phone records) and Section 702 of the Foreign Intelligence Surveillance Amendments Act (FAA) (used to gather phone calls, emails, and other Internet content) as the legal bases for most of the NSA's surveillance system. These two laws were enacted by Congress, and the Foreign Intelligence Surveillance Court supervises them (FISA court). However, it is highly possible that the NSA remarkably conducts more of its espionage under the President's claimed powers and is entirely regulated by E.O. 12333, which was first authorized by President Reagan (Jaycox, 2014).

EO 12333 significantly differs from the two major legal Acts that have been the subject of public discussion for years, Section 215 of the Patriot Act and the FISA Amendments Act, which the government uses to support the bulk collection of American citizens' phone data and the PRISM project, respectively. Due to the fact that the executive branch authorized and put into effect the executive order by itself, the programs running under the order are subject to almost no supervision from Congress or the courts. That's why decoding the government's secret orders is crucial. We've already seen the NSA adopt a "collect it all" approach, even when dealing with agencies supervised by Congress and the courts (Abdo, 2014).

*The role of ACLU.*

Through legislative campaigning and lawsuits, the American Civil Liberties Union is aggressively resisting the extension of FISA. They are opposed to legislative initiatives that would enhance the government's ability to spy on law-abiding citizens who are not engaging in espionage, and they are in favor of measures that would strengthen judicial and congressional oversight of FISA surveillance and reestablish much-needed checks and balances (American Civil Liberties Union, n.d.).

## II.3 Intelligence and American Democracy.

### *Intelligence vs Democracy?*

All nations have a capable intelligence infrastructure. But what type of intelligence infrastructure do they demand, and how could it be managed (Bruneau & Dombroski, n.d.)? Emerging democracies seek to ensure the democratic transition of political power, achieve legitimacy with authorities and democratic society, revise and reorganize their legal and economic systems, and, perhaps most importantly, build democratic civil-military relations (CMR)—that create new security institutions (including intelligence agencies) that are democratically civilian controlled, effective, and efficient. Effectiveness and efficiency need secrecy, while democratic governance requires transparency, honesty, and accountability (bruneau & florina matei, 2010). Similarly, intelligence and security operations are crucial to every state's internal and external security and the preservation of critical national interests. Securing public permission for governmental activity is a core democratic principle (Caparini, 2007). However, democratic management of intelligence is a hot topic globally, particularly in developing democracies, for four reasons. First, as Pat Holt says, "Secrecy is the enemy of democracy" because it fosters violation. How can there be accountability, the operating mechanism of democracy, if there is secrecy, particularly when both providers and end-users of classified information gain from the absence of oversight? Because intelligence agencies are secret, they bypass democracy's checks and balances. Second, information is power, and intelligence organizations gather and analyze information. Information solely goes to intelligence agencies, not to society or the state. Intelligence organizations may be independent from official oversight and, using secret knowledge, shape state policy. As a result, intelligence personnel and organizations could violate laws overseas. Third, although espionage is prohibited worldwide, intelligence officials often pay foreigners to pose as spies and demagogues, tap phones, and steal data. Therefore, intelligence personnel may always self-justify that their activity is important to national security. To illustrate, as Peter Wright has stated, "[Intelligence] is a constant war, and you face a constantly shifting target." (Bruneau & Dombroski, n.d.; Born & Jensen, 2007) Thus, the complexity of intelligence oversight and control is also characterized by the community's common necessity for security vs. individual liberties and rights (Caparini, 2007).

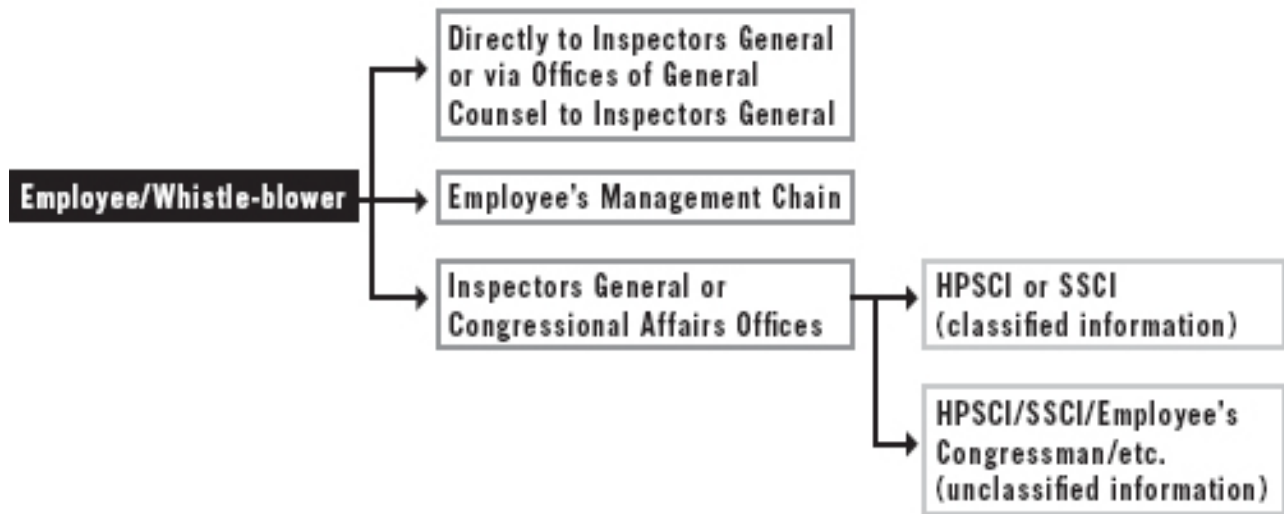
### *The act of Whistleblowing.*

There is a plethora of ways in which an employee might share information without permission from their employer (Miller, 2017). Disclosure of such information is often illegal and unethical, like when a dishonest intelligence official gives vital information about a terrorism investigation to the suspects in exchange for money. In other situations, revelation of such information, even though it is apparently illegal, may be legitimate and ethically needed, for instance, when a police officer discloses a corrupt police chief's criminal action to an oversight authority. In some circumstances, the legality and particularly the morality of the revelation may be uncertain, such as when an intelligence officer discloses to the media what he believes to be illegal and unethical monitoring action by his employer. As a result, in many cases, whistleblowing is a violation. Many acts of whistleblowing frequently violate an organization's trust, laws, or structure. It raises questions about ethical conduct. It reveals misconduct. It argues that something is wrong and that things must be improved (Marcon, 2015).

Likewise, Miceli and Near (1992) outline the following stages of a whistleblower's choice. First, a person identifies malpractice, which leads to an evaluation of whether to respond. Next, a whistleblower must decide whether they can take action and what type of action to take—whistleblowing or even another action. Maybe this sequence of whistleblower steps is too logical and reasonable. Perhaps there is more spontaneity and feeling in practice (Marcon, 2015).

Later, in 1998, Congress and the executive branch passed the Intelligence Community Whistleblower Protection Act. The statute created complaint and urgent concern procedures for intelligence community personnel. They must initially go via the intelligence community, but they may alert intelligence committees if the community hasn't acted by a certain period. This legislation raises concerns regarding the behavior of individuals such as Edward Snowden's behavior. Concerns such as how serious a problem must be for someone to become a whistleblower or how persistent someone must be before becoming a whistleblower are some of the issues that are rising. The greatest cure may be a mechanism in which objections are considered and handled with the purpose of finding an intermediate solution before the ultimate step. For most individuals and minor situations, that should be sufficient. But for the uncontaminated and pure whistleblowing system itself to properly operate, it must be honest, open-minded, and depending on the case, punishment-free (Lowenthal, 2020).

**Figure 4 - Avenues for Whistle-blowers in the Intelligence Community.**



**EMPLOYEE PROTECTIONS FOR DISCLOSURES:**

- National Security Act of 1947, CIA Act of 1949, Inspector General Act of 1978
- Presidential Policy Directive No. 19
- Agencies' Internal Policies

*(Source: (CLARKE, et al., 2014)*

Eventually, once a whistleblower's acts are exposed to the public, a cognitive fight usually follows. On one side of the divide, the whistleblower may be welcomed, applauded for their efforts, and called a "hero" or, if the matter refers to the country level, a "patriot." In another direction, they may be humiliated and called "traitors." These phrases have been used frequently in the Edward Snowden whistleblower case (Marcon, 2015).

*Metadata and Mass Surveillance*

The value of metadata has often been minimized by those in command of intelligence since the Snowden leaks (Keefe, 2013). Voice material might be challenging to interpret and gather on a large scale, but metadata is great for computer analysis. Metadata may reveal a person's hobbies, views, social positions, a person's identity, whereabouts, and social network. Cross-checking information with public records may disclose a person's identity, address, credit history, and more. Although the metadata gathering program helps prevent terrorism, it might violate personal

expectations of privacy (Atkins, 2014). Additionally, metadata is so rich in hints that Google, eBay, and the NSA are collecting and mining it: e-mail addresses to and from, times of e-mails, phone numbers called and received, call durations, and particular device serial numbers (The Washington Post, 2013).

The mass surveillance system has been dubbed "Orwellian" because it bears a striking resemblance to the scenarios and tactics detailed by George Orwell in "1984," in which all people are constantly monitored and manipulated by "Big Brother." After 9/11, spy services could better acquire information. The likelihood that some present procedures may have prevented the attacks was enough to warrant additional mass surveillance activities. Authorities were able to virtually track a person's movements anywhere in the world and share this information more quickly thanks to innovative capabilities. Although proof that expanded capabilities have hindered assaults and protected civilian lives is weak, the chances are high, according to recent studies (Monteiro, 2014). In the pursuit of security, however, essential rights may be threatened or abused, a practice that should be evaluated (U.S. DoJ, 2014). Yet, there is no proof that anybody in the US has experienced unfairness or prejudice because their emails were read (Inkster, 2014).

The term "mass surveillance" is an inappropriate name. Mass surveillance means that nations are routinely monitoring their people's communications and taking action based on the information collected. In reality, the NSA and its partners have processed large amounts of communications information through computer programs intended to determine very restricted target groups based on specific criteria (Inkster, 2014).

### *Oversight and Accountability.*

James Madison remarked in Federalist Paper No. 51, "*If men were angels, no government would be necessary.*" In the absence of angels, he said that "*ambition must be made to counteract ambition.*" In a democratic society, the most essential defense against misuse is elections: the people's oversight. Madison also emphasized "auxiliary precautions" in governance. This term encompasses checks and balances exerted by the three governmental branches in the US, from impeachment proceedings against the president and judicial review through investigations, commissions, hearings, and budget reviews. Madison predicted the need for consistent supervision of government activities, a characteristic of modern governance known as accountability, or, in

the less elegant word used by political scientists, "oversight" (Born, et al., 2005). Aside from that, intelligence and security oversight frequently examine one of two things: Firstly, supervision may evaluate the intelligence service's ability to fulfill its mission. Executive-level oversight focuses on functional problems, such as how well the service is executing its objectives and functions, such as detecting key threats, to see if the intelligence community is reacting properly to policymakers' demands and whether it has enough capabilities. And secondly, oversight might aim to determine the intelligence service's legitimacy, i.e., if it has performed appropriately and applied legal and ethical standards in its actions and goals (Born & Caparini, 2007).

Directors of agencies are responsible for incorporating legal and ethical principles into training and working procedures. Legal and ethical criteria must be seriously considered in order to emerge as an integral part of an organization's culture and not only a formality. It is more difficult to alter the culture that prevails inside intelligence organizations than to give them a more democratic constitutional framework, generally (Grill & Phythian, 2018). If pressure to change the culture only comes from outside watchdogs, there is a chance that representatives and people inside the group will see it as foreign interference and mostly about public relations. Therefore, an internal supervision system is needed to enforce operational norms and improve training (Grill & Phythian, 2018; Barak, 1991).

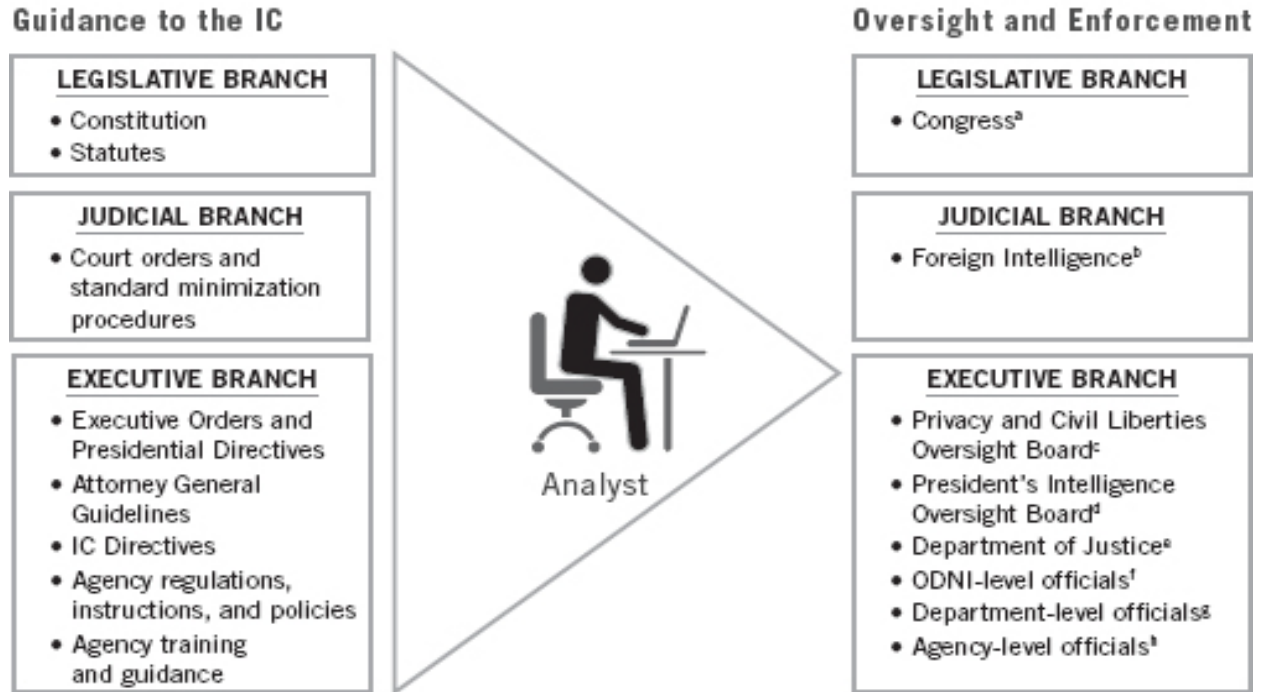
Obviously, IC is under executive, legislative, judicial, internal, and external oversight. For instance, on the one hand, Congress created two special committees to examine abuses in the IC: the Senate Church Committee and the House Pike Committee, while on the other hand, the media and other watchdog organizations play a crucial role in regulating intelligence (Boraz, 2007; Ott, 2003).

In short, separate organs in U.S. democratic organizations supervise intelligence, but executive authority is the most prominent and crucial in ensuring a state uses its intelligence institutions effectively. The executive branch establishes the IC's mission and organizes it to support it. In addition, the executive branch is the major consumer of intelligence and so provides the Intelligence Community with the most daily guidance (Boraz, 2007).

- Executive Privilege -

**Figure 5 - US Intelligence: Multiple Layers of Rules and Oversight**

The graphic below illustrates the role played by each of the three branches of the US Government in governance of a query run by an intelligence analyst. On the left are the laws and guidelines that apply to actions of the analyst, setting forth the parameters within which the search may be conducted. The right side of the graphic highlights the review, oversight, and auditing functions of each of the three branches, once the search has been conducted.



<sup>a</sup>Determines whether and how to authorize/fund intelligence activities and conducts oversight via intelligence and other committees.

<sup>b</sup>Rules on matters under Foreign Intelligence Surveillance Act.

<sup>c</sup>Provides privacy/civil liberties advice and oversight for USG efforts to protect the nation from terrorism.

<sup>d</sup>Reviews reports of potential violations of law and executive order on behalf of President.

<sup>e</sup>Includes DOJ's National Security Division and DOJ's Privacy and Civil Liberties Office.

<sup>f</sup>Includes ODNI's Civil Liberties and Privacy Office, ODNI/OGC, and the IC Inspector General.

<sup>g</sup>At the department level, these can include departmental counterparts to the agency-level organizations, and may also include other offices (for example, DOD's Assistant to the Secretary of Defense for Intelligence oversight).

<sup>h</sup>At the agency level, these can include the following organizations: Offices of General Counsel, Offices of Inspector General, Civil Liberties and Privacy Offices, Intelligence Oversight Offices, Compliance Offices (for example, NSA's new Civil Liberties and Privacy Officer position, and NSA's Office of the Director of Compliance).

[Source: (CLARKE, et al., 2014)]



**Figure 6 - Accountability legislation affecting the U.S. intelligence agencies, 1947–2006.**

<i>Statute</i>	<i>Year of enactment</i>	<i>Core objective</i>
National Security Act <sup>1</sup>	1947	To create the Central Intelligence Agency
Hughes–Ryan Act <sup>2</sup>	1974	To require presidential approval of covert action and their reporting to Congress “in a timely manner” (within two days)
Foreign Intelligence Surveillance Act (FISA) <sup>3</sup>	1978	To prohibit improper intelligence operations through the establishment of a FISA court to review warrant requests for wiretaps and other intrusive surveillance methods
Intelligence Oversight Act <sup>4</sup>	1980	To require prior reporting to Congress of all intelligence activities
Intelligence Identities Act <sup>5</sup>	1982	To prohibit the disclosure of the names of individuals working undercover in the intelligence agencies
CIA Inspector General Act <sup>6</sup>	1989	To establish a CIA Inspector General answerable to Congress
Intelligence Oversight Act <sup>7</sup>	1991	To clarify oversight language by defining covert action more definitively and adjusting the reporting time to “prior” in most cases, but with an opportunity for presidential delay (two days) if exigencies so require
USA PATRIOT Act <sup>8</sup>	2001	To improve intelligence sharing and enhance collection targeted at domestic subversives
Intelligence Reform and Terrorism Prevention Act <sup>9</sup>	2004	To create a Director of National Intelligence to further improve the sharing of information among the intelligence agencies

*[Source: (Johnson, 2008)]*

Attention to congressional intelligence oversight has grown in the 110th Congress, particularly because the House Democratic majority pledged to adopt the remaining 9/11 Commission recommendations. Its 2004 findings set the foundation for rethinking Congress's organization in this area. The commission's consensus report said congressional intelligence oversight was "dysfunctional" and offered two alternatives. These included: (1) the establishment of a joint committee on intelligence (JCI), patterned after the dissolved Joint Committee on Atomic Energy (JCAE), with the ability to review legislation in each house; and (2) increased status and power for the current select committees on intelligence by making them standing committees and awarding them both authorization and appropriations power (Kaiser, 2010).

The intelligence Committees mostly function in secret. Their usual information-gathering tools include open and closed hearings, formal briefings, statutorily mandated reports and informal contacts. Also, legislation plays a crucial role in oversight (DeRosa, 2022). Oversight is separated into two vigorous categories: "police patrols" and "fire alarms" (Kibbe, 2010; McCubbins & Schwartz, 1984). "Patrol" oversight is aggressive, immediate, and unified, while "fire alarm" oversight is roundabout and fragmented (Kibbe, 2010). But what are the main current issues with performing oversight? The congressional intelligence committees have been under criticism in recent years for not investigating key intelligence mistakes (the 9/11 intelligence failure) as well

as being too amenable to the Bush presidency's disputed tactics on investigations and warrantless surveillance. To illustrate, the existing system of oversight is hindered by: (a) gerrymandered jurisdictional lines, called "jurisdictional complexity," (b) the intelligence committees' inability to get the necessary information to perform oversight, and (c) the growing partisanship among intelligence committees (Kibbe, 2010; Ott, 2003).

In conclusion, the U.S. system of congressional intelligence oversight has proven to be effective. But the system, in order to work, demands certain circumstances. These include IC's realization that oversight is not merely a legal necessity but a crucial systemic asset if done well. The Intelligence Community must embrace, not oppose, oversight. On the congressional side, the checklist is even bigger: (1) nonpartisanship; (2) a skilled professional staff; (3) a qualified, trained staff director; (4) a chairman who has handled significant topics and programs; and (5) a solid working partnership among the oversight, military services, and budget committees. Surely, Senate intelligence oversight no longer meets these minimal standards. It is unknown whether it can be revived or whether the damage is permanent (Ott, 2003).

## **II.4 Research Methodology.**

### *Structure.*

Generally, when we define "methodology," we refer to a collection of techniques and methods that a professional might use to conduct a research process. In this research method, reasonable strategies and processes are appropriately used and merged to enlarge an existing issue (Ζαφειρόπουλος, 2015). There are two types of research methods: qualitative and quantitative. Quantitative approach concentrate on numerical data and statistical comparisons, as well as assessment of theoretical ideas using instruments such as the standardized questionnaire, in order to identify causal correlations. However, the study of quantitative data and the formation of new hypotheses need qualitative procedures and techniques, such as interviews and case studies (Κυριαζή, 1998). Qualitative research is an appropriate methodological choice to investigate in depth participants' representations, attitudes, perceptions, and motives, as well as their emotions and symbolic imaginary data. At the same time, the qualitative method, according to Iosifidis (2008), is a basic research tool of the social sciences, as they do not use numbers or mathematical logic but seek to accurately record what participants say and do, to interpret their choices, and to understand the obvious or invisible factors that affect the quality of these choices (Λιαργκόβας, et al., 2018) .

In short, the importance of research methodology is primarily focused on the investigation of scientific sources, which leads to the creation of new knowledge, which is then used to either answer research questions or confirm research hypotheses (Λιαργκόβας, et al., 2018).

To illustrate, the performance of this thesis was based on secondary research in conjunction with bibliographic research (particular types of research that are enlisted in the "genre of collected data" category). To be more specific, secondary research data are collected and evaluated as they emerge from the processing of previous primary research, the results of which have been published in various sources, such as work studies, committee reports, surveys carried out, opinion polls, explanatory reports of bills, etc. The most common form of secondary research is bibliographic research. In bibliographic research, there is a study and a critical analysis of the texts as they are presented in the articles that have been published in scientific journals and books (Λιαργκόβας, et al., 2019).

This research used a qualitative approach since it offered a comprehensive examination of the two topics, "Intelligence vs. Democracy" on the one hand, and the "Edward Snowden case study" on the other. Compared to a quantitative approach, for numerous reasons, it could not be the optimal choice for this project. Due to the hypersensitive nature of the intelligence subject and the significant proportion of secret material included in its content, it is practically difficult to get detailed and reliable statistics based on the Internet and interviews. Furthermore, linguistic and geographical constraints (USA–Greece) would have made survey work and/or interacting with participants practically impossible. Finally, selecting a realistic, representative sample and removing prejudice would have been a very complex and difficult procedure.

Then, the purpose of this qualitative study is to present a comprehensive review of the relationship between the government, secrecy, mass surveillance, and privacy in the democracy of the United States of America, also referred to as "Intelligence vs. Democracy," by using the Edward Snowden case study. Following this, it attempts to represent the Snowden-related leaks' timeline and his motives; discoveries and responses to the revelations; the immediate and long-term effects of these leaks; and the consequences of the disclosures, including deteriorated international ties and awareness of widespread monitoring programs. Also, this study examines the meaning and the role of the intelligence oversight in theory and in practice, as well as its issues and paradoxes; the reforms that were implemented due to Snowden's disclosures, along with the introduction of possible future reforms; what these reforms signify for the government's responsibility and obligations to the American people; and the influence that society and its institutions had in advocating for and employing greater openness. This technique presented in Figure 7 offers a simple description of the framework of this study. The Intelligence and Democracy theory (background information), Snowden's timeline of events, the extent of the revelations, and the findings regarding the US and UK operations for mass surveillance of phone and internet interactions will be conducted mostly through a literature study. Analyzing the Intelligence and Democracy literature, definitions, and interpretations in conjunction with the extent of Snowden's revelations will give the foundation for grasping what was revealed and to what scale. After reviewing what was disclosed, follows examination of the impacts on U.S. government and its people, Snowden's motives, counterweights and overseers to the security state and the reforms, issues which are the core of this research. On the one hand, the usage of this special case study and, on the other, the knowledge stemmed from the literature review will help

us better determine the implications the revelations had on the USA and its political and social systems.

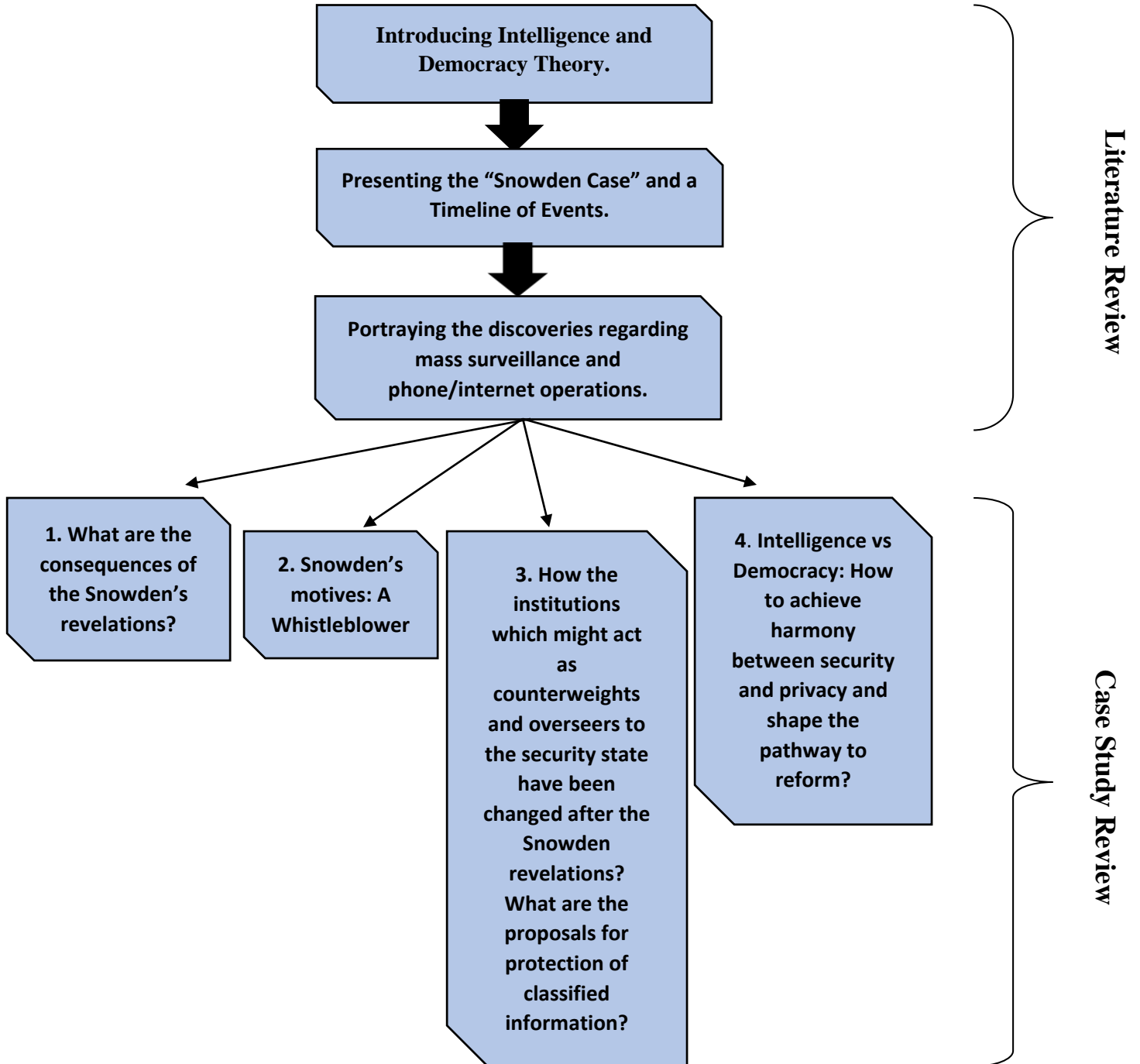
In conclusion, the case study method was chosen as the research instrument because of how extensive and analytical it is. This was done to assess how much the intelligence subject and its operations, and then Snowden's revelations, have influenced the US social and political scene. The idea behind this was to demonstrate the necessity of paving the way for essential reforms in the oversight system and IC in order to not only establish harmony between secrecy and privacy, but also to provide the lessons that can be learned from these experiences until now regarding the accountability of intelligence and security services for human rights (Ybo, 2007).

#### *Research Questions:*

After the aforementioned structure, the research questions are presented as detailed below:

- 1. What are the consequences of the Snowden's revelations?*
- 2. Snowden's motives: A Whistleblower or a Traitor?*
- 3. How the institutions which might act as counterweights and overseers to the security state have been changed after the Snowden revelations? What are the proposals for protection of classified information?*
- 4. Intelligence vs Democracy: How to achieve harmony between security and privacy and shape the pathway to reform?*

**Figure 7 - Research Methodology.**



## Chapter III: The Snowden case – Timeline of Events

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”

— Edward Snowden

“If you are outside of the intelligence community, if you are the ordinary person and you start seeing a bunch of headlines saying, U.S., Big Brother, looking down on you, collecting telephone records, et cetera, well, understandably people would be concerned. I would be too if I wasn't inside the government.”

— Barack Obama, August 9, 2013

### *Introduction.*

Edward Snowden is the most famous and controversial "whistleblower" in the world. No one has ever released so many top-secret files from the world's most powerful spy agencies. He did. He's unmatched. No one realized how feasible it was to steal the digital analog of archives full of multi-locked paper records and security systems until the current generation of computer programmers came around (Harding, 2014).

To illustrate, Edward Snowden, a gifted techie who left his high school in his second year, rose to the top of government intelligence organizations. He was born in 1983 in North Carolina to a family of public servants in the sectors of the Coast Guard, army, law enforcement, and government attorneys. Snowden spent most of his time online, participating in debates on the tech website "Ars Technica." He regularly made references to Newton and Goethe and debated the essence of freedom. "*Confidence in the objective*," he said, "*enables you to be really free.*" Following this, when 9/11 happened, Snowden was heading to work. He was driving to work when he heard the first aircraft strike. Snowden was impacted by the assaults, like many civic-minded Americans. Moreover, in 2004, when the ground conflict in Iraq heated up with the Battle of Fallujah, he joined the Army special forces but was dismissed after injuring both of his legs. "*I was open to the government's explanation—almost propaganda—about Iraq, aluminum tubes, and anthrax*," he says. "*I still felt the government wouldn't lie to us, that it had noble intent, and that the war in Iraq would be a limited, focused endeavor to liberate the oppressed. I wanted to do my*

part" (Marcon, 2015) (Andrews, et al., 2014) (Bamford, 2014). His first job was as an NSA guard. The CIA soon identified Snowden's IT and security skills. Taking advantage of these skills, Snowden revealed to Poitras and Greenwald in the famous interview that during his time with the CIA, it was the first time he saw how far the NSA and CIA could reach. After his experience with the CIA, he was sent to a Hawaii-based NSA facility (Alhinnawi, et al., 2015). His views on Social Security and other liberal ideas had not altered, as he followed Thoreau's passionate individualism in opposing state interference in the economic sector and saw the CIA as an increasing threat to American liberties (Gardner, 2016).

Moreover, for his online postings, he came up with a pseudonym. His username, "The True HOOHA," was exposed in a Reuters story. This was his nickname on an anime website, which matches his Ars handle, TheTrueHOOHA. Under this identity, postings clearly indicate that the person is Snowden. Thus, in February 2010, TheTrueHOOHA stated: *"Society really seems to have developed an unquestioning obedience towards spooky types." "Did we get to where we are today via a slippery slope that was entirely within our control to stop? Or was it a relatively instantaneous sea change that sneaked in undetected because of pervasive government secrecy?"* (Gardner, 2016; Mullin, 2013).

While he was at the NSA station, he planned to release the papers, always citing the common good. He gathered 1.7 million crucial papers (Alhinnawi, et al., 2015; Strohm & Wilber, 2014). When co-workers entrusted him with their private keys, he utilized keyboard capture to steal them and connect directly to classified material. Despite the NSA's prohibition on USB drives, Snowden easily copied all the papers to them. After the copy and the disclosure of the archives, Greenwald persuaded Snowden to reveal his identity. When identifying himself in the 2013 interview, Snowden states that he does not want to be the focus, but rather the disclosures. He also says he won't hurt anybody, not even governments. He said that he examined all papers to ensure they wouldn't expose U.S.-harming material. He rooted for only disclosing materials that were in the public's eye and that posed no immediate harm (Greenslade, 2013).

"The Guardian" published Snowden's disclosures first. His intentions were as audacious as they were disputed. Snowden exposed the NSA and its partners' actual behavior. Snowden's disclosures are crucial. His papers demonstrated that electronic surveillance technologies have escalated out of sight, partly due to the political frenzy after 9/11. The NSA and its British junior partner, GCHQ (which is secretly linked with internet and telecom firms that control the



technology), have employed all their technological talents to "master the internet." That has led to a world of spying (Harding, 2014). Cell phones, computers, Facebook, Skype, and chat rooms are all tools the NSA uses to create what it refers to as "a pattern of life," a thorough profile of a target and everyone connected to them (Macaskill & Dance, 2013).

### **III.1 The Planning: Chronicles of the spy story.**

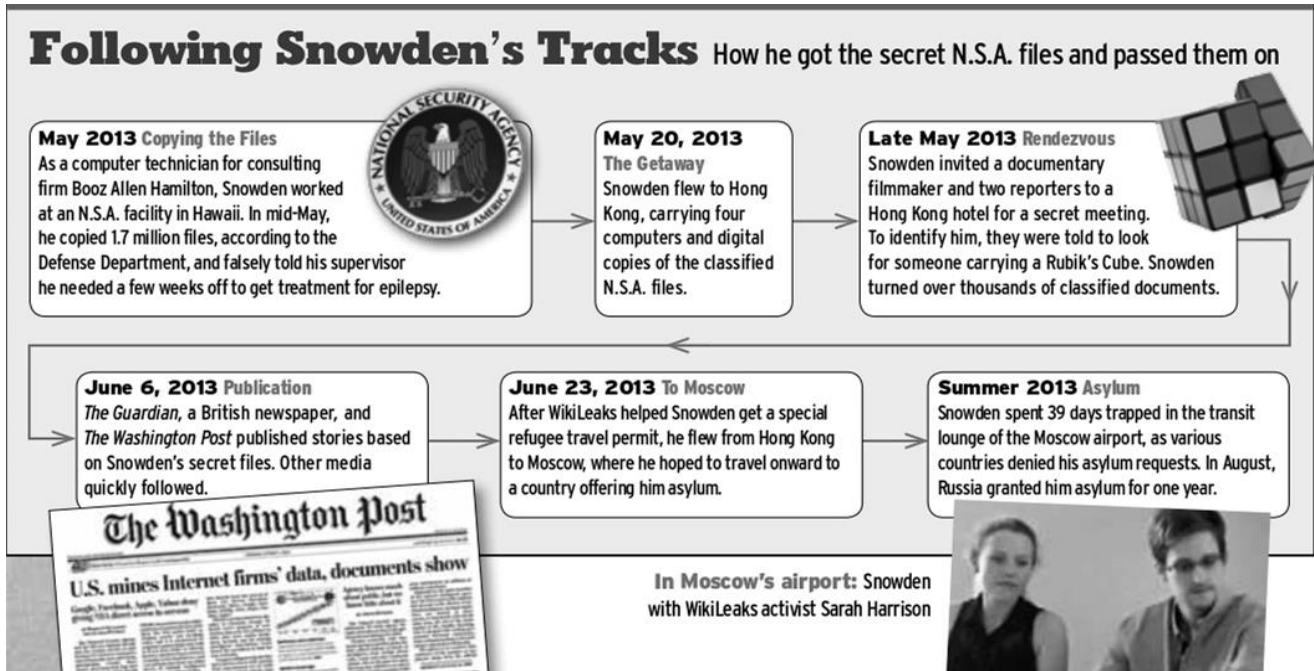
Snowden had been planning to release the documents for a long time. Three months earlier, he told a Hong Kong newspaper, the South China Morning Post, that he had applied for a job at the management consulting firm Booz Allen Hamilton to get as much access as possible so he could find proof of the NSA's spying programs. The oxymoron of this interview was that it exposed American eavesdropping in China while the U.S. administration accused Beijing of hacking U.S. corporations (Gardner, 2016).

Furthermore, it will be explained what has happened to the NSA "whistleblower" who disclosed documents to the Guardian since he chose to go public with his name and started fighting for asylum (Gidda, 2013): Firstly, on May 13, 2013, Snowden started giving papers to Poitras, Greenwald, and "The Washington Post" reporter Barton Gellman (NBC News, 2014). Then, on May 20, 2013, he was hired by the defense firm Booz Allen Hamilton and landed in Hong Kong from Hawaii. He traveled with four laptops that provided him access to some of the most highly classified information held by the US government (Gidda, 2013). On June 5, "The Guardian", a British daily, revealed that the NSA is gathering telephone data on millions of Verizon customers in the United States according to a secret court ruling. According to security experts, other phone providers' data is also included. The Guardian and The Washington Post have published further spying leaks in subsequent articles. On June 9, Edward Snowden, who claimed to have worked at the NSA and CIA, permitted himself to be named as the source of revelations concerning secret U.S. surveillance programs. He informed The Guardian that he wanted to alert the US people about actions taken in their name and against them. Furthermore, on June 10, Snowden left his Hong Kong hotel as his next whereabouts were unclear. Booz Allen Hamilton said it dismissed Snowden for violating the firm's ethics and regulations a day later (Associated Press, 2013). On June 11, the EU wants US guarantees that surveillance programs didn't violate Europeans' rights. On June 12,

Snowden told the South China Morning Post that U.S. intelligence has been hacking networks for years. On June 17, while in an online discussion, the man identified as Snowden by Britain's Guardian newspaper said U.S. officials had far-reaching access to phone calls, e-mails, and other data. On June 18, FBI Deputy Director Sean Joyce told the House Intelligence Committee that PRISM had helped avert terrorist attacks (Government Accountability Project, n.d.). On June 23, as extradition pressure had been mounting, Snowden traveled from Hong Kong to Moscow. On June 24, White House spokesman Jay Carney demanded Russia bring back Snowden. He also believed that his escape from Hong Kong would affect US-China ties. On June 25, China declared that the US position helped Snowden leave Hong Kong and that it was *"unjustified and unacceptable."* Putin claimed Snowden was at Moscow's Sheremetyevo airport and was free. Barack Obama promised to extradite Snowden, and US Secretary of State John Kerry asked Russia to send the criminal back to the US (BBC News, 2013). On June 26, Putin said that Snowden would not be sent to the United States. He disputed that Snowden had been approached by his security team. On July 1, a Russian consular officer confirms Snowden's asylum application. Also, WikiLeaks revealed he had been seeking asylum in France, Germany, Ireland, China, and Cuba. On July 10, Glenn Greenwald, a Guardian writer who has published several pieces based on Snowden's material, said Snowden insisted he hadn't sent secret information to China or Russia (Gidda, 2013). On July 12, Snowden met activists and Russian authorities and claimed he'd stop disclosing U.S. surveillance secrets if Russia granted him asylum. Lastly, on July 16, Snowden demanded his attorney submit an application for emergency asylum in Russia, arguing that he was risking persecution from the U.S. government as well as the possibility that they might torture or even kill him (Associated Press, 2013).

In conclusion, in 2013, Edward Snowden was a National Security Agency contractor who worked as an IT systems specialist. He went to Hong Kong to give three reporters huge numbers of top-secret archives about how the NSA was spying on American citizens. Following this, and according to him, the secret material he revealed to the media exposed privacy violations by government spy agencies. He considered himself a whistleblower. However, the American government saw him as a traitor who had violated the Espionage Act (Davies, 2019).

**Figure 8 - Following Snowden's Tracks. How he got the secret N.S.A. files and passed them on - Summary.**



[Source: (SMITH, 2014)]

### III.2 The fight for asylum: How Mr. Snowden avoided U.S prosecution?

According to Vladimir Putin, Snowden was still in the Sheremetyevo airport's international transit zone despite the United States canceling his passport. The former said that Russia would not help send Snowden back to the US, and he went to 20 countries, including Russia, looking for safety. Also, he stated that he didn't want Snowden's presence to hurt ties with the U.S., and if he wanted to stay in Russia, *"he must cease harming our American friends."* Snowden was given temporary refugee status by Russia after more than a month in the Sheremetyevo transit zone. Then he departed the airport with a WikiLeaks worker ( Ray, 2022).

Moreover, the chronicles of Snowden's fight for asylum during his endeavor to avoid US prosecution are provided below: (a) In July 17, Putin clearly indicated he wouldn't damage ties with Washington over Snowden. (b) On July 19, the Kremlin claimed that Snowden has no intentions of obtaining a Russian passport. (c) On July 22, Attorney Kucherena predicted that Snowden would leave the airport transit area by Wednesday. (d) On July 24, an airport source

claimed a Russian federal agency had given Snowden credentials in order to leave the airport, which would be delivered to him by Kucherena. (e) On August 1, Snowden left the airport after getting Russian asylum until July 31, 2014 (Reuters Staff, 2013). (f) On November 3, Der Spiegel, a German magazine, published a letter written by Snowden. Its title was "A Manifesto for the Truth," which implied that *"mass surveillance is a global problem and needs a global solution."* (g) In December 17, Snowden wrote a letter to Brazil, proposing to examine U.S. surveillance of Brazilians. (h) On January 23, 2014, on the one hand, Attorney General Eric Holder supported, *"If Mr. Snowden wanted to come back to the United States and enter a plea, we would engage with his lawyers."* On the other hand, in an online conversation later that day, Snowden announced that returning to the U.S. is *"unfortunately not possible in the face of current whistleblower protection laws"* (Government Accountability Project, 2013).

Afterwards, Obama said he *"would not scramble jets"* or risk diplomatic crises to pursue Snowden. However, Washington was attempting to prevent his escape. The Guardian stated that U.S. authorities *"persuaded Ecuador to withdraw Snowden's asylum request."* Congressional leaders threatened to withdraw trade accords, and vice president Joe Biden continued with a diplomatic phone call that changed Ecuador's president's view. After showing Snowden some support at first, Ecuador took itself out of the running as a possible place of asylum (McParland, 2013).

He is still facing espionage accusations. The United States wants Russia to extradite Snowden. The DoJ has charged him with breaching the Espionage Act for disclosing worldwide mass surveillance programs. If convicted, Snowden risks 30 years in jail. Also, according to many experts, the 1917 Espionage Act seems obsolete and inadequate to deal with Snowden's case. If he's prosecuted for violations under the Espionage Act, he might be blocked from providing a public-interest defense. Senior US authorities have judged Snowden without even a trial, labeling him a criminal and a traitor, as a result raising worries about his fair trial if he comes back. In addition to the prosecutions against him, US authorities have taken away Snowden's passport, which makes it harder for him to move around and seek asylum. He couldn't visit asylum-offering nations. The USA continues to pressure nations throughout the globe to block his passage through their territory or airspace (Amnesty International UK, 2020).

After all, in 2020, Mr. Snowden announced that he was going to seek Russian citizenship, seeing the move as a practical one that would allow his family to travel more freely. Finally, Mr.

Putin granted his request in a ruling that the Kremlin made public in 2022. Numerous immigrants were awarded citizenship as a result of the ruling, including Mr. Snowden (Yuhas, 2022).

### **III.3 The Revelations.**

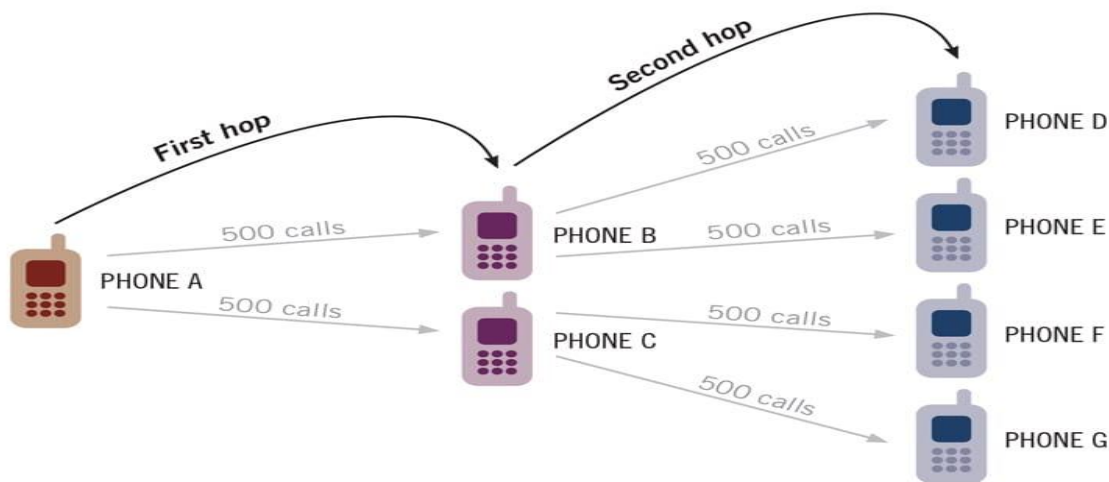
Edward Snowden's June 2013 leak of an estimated 1.7 million highly classified documents shed light on the subject of mass surveillance of American individuals as well as expanded worldwide spying by the Five Eyes organizations (Lashmar, 2018; Mirfattahi, 2019). As an NSA employee, he had previously expressed concerns to authorities about the NSA's surveillance of internal communications but subsequently opted to expose practices that, according to him, the American government had covered and implemented (Mirfattahi, 2019). Furthermore, this section discusses the two (2) NSA surveillance programs revealed in the 2013 revelations. On the one hand, the "Bulk Collection of Telephone Metadata" program gathers, maintains, and examines data for a substantial part of U.S. phone calls (not the whole content), and on the other hand, the "PRISM" program gathers non-Americans' personal digital conversations (the whole content) from Google, Facebook, and other major firms (Etzioni, 2014).

In particular, regarding the "Bulk Collection of Telephone Metadata" program, on June 6, 2013, The Guardian and the Washington Post reported that the NSA had requested and received a court ruling in April 2013 to gather phone data of millions of Verizon customers. The order was supposed to expire on July 19 (Olesen, n.d.; Greenwald, 2013). In the released court decision, the NSA was given "all call detail records" or "telephony metadata" produced by Verizon for communications (a) between the U.S. and overseas or (b) fully inside the United States, such as local phone calls (The Guardian, 2013). The specific court order is greatly aided by Section 215 of the Patriot Act which allows the FBI to request for court orders requiring the production of tangible things (such as books, archives, documents, texts, and many other materials) for an inquiry to gather foreign intelligence information not involving a U.S. person or to guard against terrorist acts or covert intelligence operations (Olesen, n.d.; U.S.C., n.d.). On the contrary, the first amendment of the US constitution, which protects people's right to freedom of speech, press, or other activities, prevents the prior article from being implemented in cases where fundamental human rights are not protected (Beeman, 2010). Essentially, the disclosures have shown and

continue to show that several U.S. government gathering and surveillance operations are outside the boundaries of Section 215 of the USA PATRIOT Act and Section 702 of the FAA. The first piece revealed an NSA effort to obtain millions of Verizon customers' phone data, whether or not they are suspected. This program involves the ongoing collection of "telephony metadata" (who, when, and what types of phone calls – but not call content) by the government under the terms of the aforementioned court order issued in accordance with Section 215 of the USA PATRIOT Act (Rubinstein & Hoboken, 2014).

Then, the Third-Party Doctrine was used to legitimize the acquisition of telephone records. According to the Third-Party Doctrine, which was implemented in *Smith v. Maryland*, personal data that is willingly given to a third-party has no reasonable expectation of privacy and, hence, is not protected by the Fourth Amendment (U.S. Supreme Court, 1979). In other words, a person who uses a mobile phone knowingly transmits metadata to his or her cell provider, a third party, thus endangering his or her expectation of privacy (Etzioni, 2014). Following this, FISC was focusing on the *Smith* ruling to justify telephone providers' provision of metadata to the NSA (Atkins, 2014; Etzioni, 2014).

**Figure 9 - Call Event Hop Scenario and Method of Counting.**



*Target uses **Phone Number A** which is the FISC-approved selector in the FISC order. This would be counted as **1 order, 1 target, 7 unique identifiers (phone numbers A, B, C, D, E, F, G)** and, assuming 500 calls between each party (1,000 records), **6000 CDRs**. CDRs may include records for both sides of a call (for example, one call from **Phone Number A** to **Phone Number B** could result in 2 records).*

*[Source: Office of the Director of National Intelligence Statistical Transparency Report Regarding the Use of National Security Authorities, Calendar Year 2018, (Laperrugue, 2019)]*

After it was found out that the NSA was collecting a lot of people's phone metadata, more papers were made public. The Guardian was able to find out that the NSA had been getting user information from a number of large technology companies as well as looking at people's call records. For instance, the NSA had direct access to Google, Facebook, Apple, and other US internet companies, according to a top-secret document that the Guardian acquired. The NSA's accessibility is a component of an earlier revealed system/program named PRISM, which collects browsing history information, emails, data transfers, and live conversations. The program permits substantial, in-depth surveillance of live conversations and chats and archived data. The legislation facilitates the targeting of clients of participating corporations who reside outside the US or Americans whose communications involve individuals outside the US. Additionally, it allows the collection of communications made solely inside the United States without a warrant. The exposure of the PRISM project comes after the aforementioned leak of a top-secret court order requiring Verizon to hand over the phone data of millions of US customers. Aside from acquiring telephone data, this type of surveillance could record the entire content of conversations as well as their metadata (Greenwald & MacAskill, 2013). Similarly, the program was enabled by Section 702 of the FISA Amendments Act (FAA) of 2008. It prohibits the US government from obtaining foreign target information from US ISPs unilaterally. All counterterrorism information is collected with the ISP's knowledge. These measures are authorized by the US Attorney General and the Director of National Intelligence in written guidelines, which the FISC approves for one year and may renew. Thus, the NSA doesn't require a court warrant to collect information on suspected foreign targets (Etzioni, 2014). However, even when the process worked as claimed, with no Americans targeted, the NSA consistently captured American information. This is "incidental" to contact sequencing, a fundamental trading technique. To get information on a person who is thought to be a spy or foreign terrorist, at least everyone in the suspect's inbox or outbox needs to be scanned (Gellman & Poitras, 2013). Meanwhile, Senator Ron Wyden, one of the PRISM opponents, claimed that a gap in Section 702 permitted the government to perform warrantless or, in other words, "backdoor" inquiries of Americans' communication activities (Ball & Ackerman, 2013).

Figure 10 - Slide showing companies participating in the PRISM program and the types of data they provide.

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF)

## PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PaTTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection  
(Surveillance and Stored Comms)?  
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:  
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

[Source: (N.S.A., 2013)]

Besides these, Snowden has disclosed that, at least since 2009, the NSA has been hacking computers in Hong Kong and mainland China. According to the records, US hackers targeted governmental officials, a university, corporations, and students in Hong Kong. They include the dates and IP addresses of systems hacked in Hong Kong and mainland China over the previous four years. They also indicate if an assault is underway or finished, as well as other operational details. The records show a 75% hacking achievement against Hong Kong systems (Chan, 2013). Edward Snowden isn't done releasing revelations, telling the Guardian that the NSA has a more remarkable British collaborator, the spy agency G.C.H.Q. Documents exposing how American and British intelligence services had eavesdropped on global leaders during conferences in London in 2009 were one of the many documents concerning governmental monitoring that he had obtained and revealed. The Guardian newspaper reported that G.C.H.Q., the British eavesdropping organization that operates directly with the N.S.A., monitored the e-mail and phones of other nations' delegates at two London conferences by constructing a surveilled Internet café. The US also intercepted Medvedev's (the former Russian President's) conversations, according to the newspaper. Documents showed that e-mail interception and primary software were placed on



machines in the ersatz Internet café, that foreign diplomats' BlackBerry communications and conversations were intercepted, and that 45 analysts watched who was calling whom during the conference (Shane & Somaiya, 2013). Moreover, he claimed that Great Britain may have had greater access to its citizens' data. *"It's not just a US problem. The UK has a huge dog in this fight,"* Snowden added to the Guardian. *"They [GCHQ] are worse than the US."* According to Snowden, the GCHQ has access to fiber-optic cables, can read emails, Facebook posts, record phone conversations, scan emails, and analyze website traffic. Namely, Tempora, an 18-month GCHQ program, taps cables that transport worldwide communications with the capacity to carry 600 million daily "telephone events." In contrast, proponents of the program supported the idea that all GCHQ operations are lawful. For example, as Big Brother Watch director Nick Pickles stated, *"If GCHQ has been intercepting huge numbers of innocent people's communications as part of a massive sweeping exercise, then I struggle to see how that squares with a process that requires a warrant for each individual intercept"* (Trifunov, 2013).

During the debate about the NSA's role in domestic monitoring, secret intelligence agency papers showed that the US spied on Europe, the UN, and other countries (Poitras, et al., 2013). The NSA describes its "intelligence priorities" in a document that was released, ranking them from "1" (highest interest) through "5" (lowest interest). It should come as no surprise that China, Russia, Iran, Pakistan, and Afghanistan are the main targets. Among the spying carried out against US friends, it was discovered that the NSA had bugged many embassies in New York and Washington and that the NSA possessed the construction drawings of the European Union base in New York (Poitras, et al., 2013). Also, 35 foreign leaders' communications were reportedly being monitored by the NSA in October 2013, but their names were excluded from the list. This information came to light after claims that the NSA had been monitoring Angela Merkel's phone. As a result of allegations that the NSA spied on countries perceived to be US allies, the US faced a harsh backlash from its allies (Ball, 2013).

Edward Snowden leaked secret governmental materials with the purpose of exposing the NSA's systemic gathering of US people's personal data and protesting against this phenomenon. He believed that more information was being gathered than US law permitted, and he stated that *"NSA and intelligence community in general, is focused on getting intelligence wherever it can by any means possible. It believes, on the grounds of sort of a self-certification, that they serve the national interest. Originally we saw that focus very narrowly tailored as foreign intelligence*

*gathered overseas. Now increasingly we see that it's happening domestically and to do that they, the NSA specifically, targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyses them and it measures them and it stores them for periods of time simply because that's the easiest, most efficient, and most valuable way to achieve these ends"* (Landau, 2013). Snowden's actions had huge ramifications, and the US authorities responded quickly and brutally. In an appearance on ABC's "This Week," National Security Agency director Gen. Keith B. Alexander accused Mr. Snowden of causing "irreversible damage" to American intelligence operations against terrorism and other challenges. "This is not an individual who in my opinion was acting with noble intent," General Alexander said in an interview with George Stephanopoulos (Schwartz & Preston, 2013). Moreover, the head of the Senate Intelligence Committee, Sen. Dianne Feinstein (D-Calif.) calls Snowden's NSA disclosures an "act of treason" (Herb & Sink, 2013). Snowden was charged with espionage, which was rather unexpected given that "leaks of classified information to the press have relatively infrequently been punished as crimes," according to a study by the Congressional Research Service. A warrant for Snowden's arrest has been issued. Alternatively, other officials of the US administration have a different perspective on the matter. Former Vice President Al Gore stated, "[The NSA surveillance] in my view violates the Constitution. The Fourth Amendment language is crystal clear. It isn't acceptable to have a secret interpretation of a law that goes far beyond any reasonable reading of either the law or the Constitution and then classify as top secret what the actual law is." Later, Senator Ron Wyden questioned Director of National Intelligence James Clapper in March 2013 at hearings on national security matters whether the NSA gathered "any type of data at all on millions or hundreds of millions of Americans." Then, Clapper responded, "No; not wittingly." Following the release of the NSA documents, Senator Rand Paul declared, "Clapper lied in Congress, in defiance of the law, in the name of security." Mr. Snowden told the truth in the name of privacy" (Landau, 2013).

The security ramifications of Mr. Snowden's disclosures are uncertain and may remain unknown. We will never be able to fully understand the devastation that he caused with his acts. Undoubtedly, inconsistency within the NSA itself is evidence of the agency's failure to quantify the actual harm. Even though it wasn't the first time that someone was disclosing U.S. intelligence-sensitive information, the political consequences have been significant and are still ongoing (Konstantopoulos, 2017).

### **III.4. What we discovered regarding the US and UK operations for mass surveillance of phone and internet interactions?**

#### *Accessing transnational communication systems.*

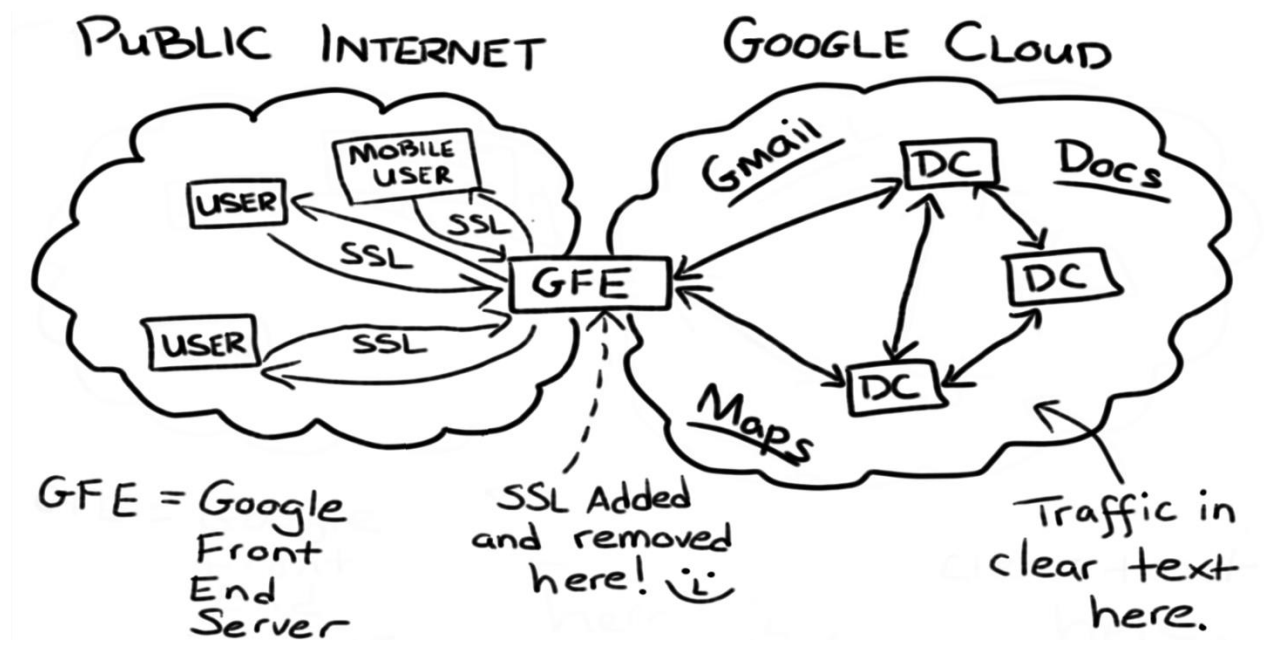
In Upstream and TEMPORA, the NSA and GCHQ intercepted transnational internet cables. These programs examined and filtered every message travelling across the internet's wires. Undersea cable hacking provides new spying tools to spies in the United Kingdom and the United States (Timberg, 2013; MacAskill, et al., 2013). Secret documents revealed that the British spy agency GCHQ, with assistance from the US National Security Agency, collected and stored webcam images of millions of internet users. GCHQ papers from 2008 to 2010 revealed that a surveillance software called Optic Nerve recorded still photographs of Yahoo webcam conversations in bulk, regardless of whether individuals were intelligence targets. In one six-month period in 2008, the organization acquired webcam footage from 1.8 million Yahoo user profiles internationally (Ackerman & Ball, 2014). Moreover, according to top-secret papers, Canada's top spy agency monitors millions of Web users' file downloads to detect extremists (Gallagher & Greenwald, 2015). The secret program penetrates Internet cables and analyzes up to 15 million daily downloads from websites used to exchange films, photos, music, and other material. CSE (Communications Security Establishment) captures millions of Canadians' emails and retains them for "days to months" to detect malicious files and other threats on government computer systems. According to a 2010 paper, it monitored visits to government websites and gathered 400,000 emails daily, retaining some material for years (Seglins, 2015).

#### *Getting into the cloud services and electronic operations of corporates.*

According to the Snowden records, PRISM is the single largest source of information for the NSA's intelligence reports. As "downstream" software, it gathers information from Google, Facebook, Apple, and other companies. They have all disclosed numbers indicating the overall number of applications they have received from law enforcement authorities over time. That being said, they are unable to disclose a number for FISA-related inquiries alone since this information remains secret (The Guardian, 2013; Kelion, 2013). The NSA has quietly hacked into the primary

communications lines that link Yahoo and Google data centers throughout the globe. By exploiting these connections, the CIA has positioned itself to gather data from millions and millions of user profiles, the majority of which belong to U.S. citizens. The NSA does not maintain all the information it obtains, but it does maintain a substantial amount. Namely, the NSA's primary instrument for exploiting data connections was the "MUSCULAR" program, which was run cooperatively with its British equivalent, Government Communications Headquarters. In that case, the British government hacked Belgacom, Belgium's biggest telecommunications provider, with some of the most powerful malware ever seen. The Belgacom hack, as Snowden stated, is the *"first documented example to show one EU member state mounting a cyberattack on another... a breathtaking example of the scale of the state-sponsored hacking problem."* Belgacom's global clients were alarmed by the hacking findings. The firm manages a vast number of data connections globally, and it serves millions of individuals throughout Europe as well as officials from important organizations such as the European Commission, the European Parliament, and the European Council (Gellman & Soltani, 2013; Gallagher, 2014).

Figure 11 - Google Cloud Exploitation.



[In an NSA presentation slide on "Google Cloud Exploitation," however, a sketch shows where the "Public Internet" meets the internal "Google Cloud" where their data resides. In hand-printed letters, the drawing notes that encryption is "added and removed here!" The artist adds a smiley face, a cheeky celebration of victory over Google security (Szoldra & Kelley, 2013)] Image: (Anon., 2016).

*Monitoring the position of smart phone devices.*

According to top-secret papers leaked by Snowden and conversations with U.S. intelligence sources, the National Security Agency was collecting about 5 billion pieces of data each day on the locations of smartphones throughout the globe. This allowed the agency to record the activities of people and map their connections in previously unprecedented ways. Many people who were against it thought that the NSA had no reason to think that the movements of most smartphone users were important to national security. Instead, they backed the idea that it was gathering location data in bulk because its most powerful and analytical tool, CO-TRAVELER, should look for unknown people whose movements intersect with those connected to known intelligence targets (Gellman & Soltani, 2013).

*Monitoring international phone conversations and calls of many nations.*

People who know about the operation and documents provided by former contractor Edward Snowden say that the National Security Agency has built a surveillance system that can record and analyze "100%" of a foreign country's phone calls up to one month after they happen. In 2009, the "MYSTIC" phone interception program was initiated. Its "retrospective and retrieval" tool, or "RETRO," and similar initiatives achieved their maximum capacity against the first target country in 2011. Two years later, scheduling papers predicted other locations would see similar activity. As President Obama explained it in January, such techniques may collect large data flows "without the use of discriminants." "RETRO" and "MYSTIC" programs were conducted under Executive Order 12333, which provides intelligence agencies the conventional power to conduct activities outside the United States (Gellman & Soltani, 2014).

*US surveillance authorities put pressure on European nations to weaken their privacy legislation.*

According to Edward Snowden, US intelligence agencies were successful in pressuring EU countries to undermine regulations securing their communications infrastructure, allowing American spies to access massive amounts of data on EU residents with impunity. For example, the National Security Agency's sector, which is called Foreign Affairs Division and is responsible

for communicating with allied nations, launched these "legal guidance operations" to undermine privacy laws and detect weaknesses in protections provided by the constitutions of Sweden, Germany, and the Netherlands. *"Each of these countries received instruction from the NSA, sometimes under the guise of the US department of defense and other bodies, on how to degrade the legal protections of their countries' communications,"* Mr. Snowden further said in a written statement submitted to the European parliament and seen by the Financial Times (FT.COM, 2014). Additionally, GCHQ played a significant role in similarly instructing its counterparts. The Guardian said that Snowden-leaked GCHQ papers revealed that the British agency has taken credit for instructing European counterparts on how to avoid national legislation designed to limit their monitoring capabilities (Shirbon, 2013).

#### *Enhancing widespread surveillance.*

The papers that were made public showed how the NSA's monitoring of communications around the world has grown under the secret RAMPART-A program, which used the help of a growing network of intelligence organizations. Undoubtedly, the NSA is a key player in the so-called "Five Eyes" surveillance partnership, which also includes spying organizations in the UK, Canada, New Zealand, and Australia. However, the most recent Snowden revelations revealed that a number of other nations, which the NSA was calling "third-party partners," were playing an increasingly significant role by permitting the NSA to covertly place espionage equipment on their fiber-optic connections. Allowing the NSA to intercept private conversations is politically toxic for any foreign nation. States that participate in RAMPART-A, on the other hand, receive access to the NSA's advanced monitoring equipment, allowing them to spy on data flowing into and out of their regions. According to the classified papers, the NSA has established at least 13 RAMPART-A sites, nine of which were operational in 2013. Three of the biggest, with the codenames AZUREPHOENIX, SPINNERET, and MOONLIGHTPATH, collect data from around 70 different cables or networks (Gallagher, 2014). In particular, the German foreign intelligence service called Bundesnachrichtendienst (BND) was gathering and transmitting vast quantities of metadata—220 million telephone records—to the NSA every day (Biermann, 2015).

**Figure 12 - A list of countries that might be part of the RAMPART-A program is included in the Snowden's archives. A 2013 classified presentation showed that the NSA has top-secret surveillance treaties with 33 third-party governments, including Denmark, Germany, and 15 other EU members (Gallagher, 2014).**



[Source: (Gallagher, 2014)]

*Unauthorized access to mobile devices and applications.*

In the past, the US government has paid nearly £100 million to the British spy agency GCHQ to get access to and impact on Britain's intelligence collection programs. The top-secret payments detailed in papers show that the United States expects a return on their investment, and that GCHQ must work hard to meet those expectations. "GCHQ must pull its weight and be seen to pull its weight," according to a GCHQ strategy briefing. Snowden issued a warning about the collaboration of the NSA and GCHQ, stating that both organizations were responsible for the

development of systems that enable widespread collection and analysis of internet and mobile data. In addition to the returns, the papers obtained by the Guardian showed that GCHQ was investing money in attempts to collect personal information from mobile phones and applications and that it sought the possibility to "exploit any phone, anywhere" (Hopkins, 2013). The documents also direct agency personnel in "intercepting Google Maps queries made on smartphones, and using them to collect large volumes of location information." Also, a document from 2010 revealed that Android phones transmit GPS data "in the clear" (without encryption), providing the NSA with the user's position each time he or she opens Google Maps. Advanced features of the agency's targeted malware program were also revealed. One slide contains a list of plugins designed to allow "hot mic" recording, high-precision geo-tracking, and file retrieval that would obtain any locally stored material on the mobile device. This includes text messages, emails, and entries in a calendar (Brandom, 2014). In another classified GCHQ document, the spies claimed, "[If] its [sic] on the phone, we can get it," describing the targeting of an iPhone (Scahill & Begley, 2015). Even Canada, as part of the "Five Eyes" alliance, has developed a vast arsenal of cyberwarfare tools alongside its U.S. and British counterparts to hack into computers and phones in many parts of the world, including friendly trade countries like Mexico and hotspots like the Middle East (Seglins, 2015).

#### *Lowering levels of encryption.*

According to top-secret documents that were leaked by Edward Snowden, US and British intelligence services have broken a big part of the internet encryption that hundreds of millions of people use to keep their personal information, online transactions, and communications private. The authorities have developed a plethora of methods that promote "the use of ubiquitous encryption across the internet." These processes include secretive efforts to guarantee NSA dominance over global encryption standards, the use of supercomputers to smash encryption with "brute force," and—the most heavily protected secret—cooperation with technology firms and internet service providers. Through these secret collaborations, the agencies have installed into the commercial encryption software hidden weaknesses known as "backdoors" or "trapdoors" (Ball, et al., 2013). Likewise, a leaked document indicates that for at least three years, GCHQ, in partnership with the NSA, has been searching for methods to access the encrypted communications



of famous Internet corporations such as Google, Yahoo, Facebook, and Microsoft's Hotmail. According to that document, by 2012, GCHQ had created "new access opportunities" in Google's systems. Yet, Google disputed any government access and stated there was no proof its systems had been hacked (Perlroth, et al., 2013). Moreover, the papers exposed that the NSA had spent more than \$250 million a year on its Sigint Enabling Project, which "engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" to make them "exploitable" (The New York Times, 2013).

*Directing key communication systems.*

The leaked documents showed the leading NSA hacking unit, which is none other than the TAO (Tailored Access Operations). The Office of Tailored Access Operations (TAO), now called Computer Network Operations and written as S32, is a part of the National Security Agency that gathers information and intelligence on cyberwarfare (Von Spiegel Staff, 2013). It is thought to be the most secret tool of the intelligence agency. It is made up of more than 1,000 military and civilian computer hackers, intelligence analysts, targeting experts, computer hardware and software designers, and electrical engineers. TAO is equipped with software blueprints that enable it to penetrate widely used hardware, such as "routers, switches, and firewalls from numerous product sellers." Its experts prefer to tap networks over isolated PCs since a network often contains several devices. It keeps its own secret network, breaks into computers all over the world, and intercepts shipments in order to put "back doors" in hardware that its targets have ordered. "QUANTUMINSERT" is a popular hacking tool for intelligence services. GCHQ used it to target Belgacom employees' PCs in order to gain access to the company's networks. Specifically, the NSA targeted OPEC (Organization of the Petroleum Exporting Countries) leaders in Vienna using the same technique. In both situations, these methods let the trans-Atlantic surveillance alliance get unhindered access to vital economic data. QUANTUM's insert technique and its versions are related to the NSA's shadow network, which uses "covert" routers and servers. It is believed that the NSA, by using its capabilities, infects routers and servers from non-NSA networks with "implants" to direct them remotely (Wikipedia, 2023; Von Spiegel Staff, 2013) .

*Encryption keys theft.*

Snowden gave top-secret papers to The Intercept that said that American and British agents broke into the computer network of the biggest SIM card maker in the world and stole the encryption keys that keep mobile conversations around the world private. "Gemalto," a global firm based in the Netherlands, develops chips for mobile phones and next-generation payment cards. AT&T, T-Mobile, Verizon, Sprint, and 450 cellular network providers worldwide are its customers. It acts in 85 countries and has over 40 production bases. "Gemalto" develops around 2 billion SIM cards annually. Its slogan is "Security to Be Free." With these obtained encryption keys, spy organizations may monitor mobile conversations without the permission of telecom firms or foreign governments. Having the keys also negates the need for a warrant or wiretap, while leaving no trace on the wifi provider's network that data was intercepted. Furthermore, mass key theft gives intelligence services access to any previously collected encrypted communications that they were unable to decode (Begley & Scahill, 2015) .

However, by obtaining the keys to target the communications of specific customers, intelligence agencies may have made the security of billions of other customers less safe. Snowden wrote in a "Reddit Ask Me Anything" session that *"Our governments ... should never be weighing the equities in an intelligence gathering operation such that a temporary benefit to surveillance regarding a few key targets is seen as more desirable than protecting the communications of a global system..."* (Zetter, 2015).

*Summary of the significant spying programs and instruments.*

<b>Codename</b>	<b>Purpose</b>	<b>Type</b>	<b>Scope</b>
Stellar Wind	Store call metadata	Bulk	USA
PRISM	Capture any data that match court-approved search terms	Bulk	US-based service providers
XKeyscore	Store and query data based on specific filters (aka. selectors)	Bulk	Global
Tempora (GCHQ)	Store internet traffic	Bulk	Global

MYSTIC (SOMALGET)	Store call metadata and also phone calls for some countries	Bulk	All calls from: Kenya, Bahamas, Afghanistan (SOMALGET) Metadata from several countries
BULLRUN (NSA) Edgehill (GCHQ)	Break encryption used in networked communication (SSL, VPN)	Bulk	Global
MUSCULAR (GCHQ and NSA)	Capture all traffic between data centers of Yahoo and Google	Bulk	Yahoo and Google data centers
Turbulence	Injecting malware into remote computers	Targeted	Global
FAIRVIEW	Capture internet traffic, phone metadata and SMS from foreign countries (via AT&T)	Bulk	Global
STORMBREW	Capture data from fiber-optic cables and top-level communications infrastructure	Bulk	Global
Dishfire	Capture SMS	Bulk	Global

[Source: (Alhinnawi, et al., 2015)]

### **III.5 Obama's limited and ineffective response.**

Prior to the Snowden events, back in 2011, Obama had strongly supported the Patriot Act's collection of American phone records, but before becoming president, he saw the situation differently. In 2005, Congress debated the first reauthorization of the Patriot Act, which gave the federal government more power to spy. Obama was one of nine senators who signed a letter saying that the bill broke civil rights laws and should be rejected. Finally, Congress reauthorized Patriot Act and Section 215 as well. Obama became president a few years later. And then, under President Obama's command, the NSA conducted surveillance closely, like the expansive "fishing expeditions" about which Sen. Obama warned (Lee, 2013).

In the weeks after Snowden's revelations, the Obama administration faced domestic and worldwide criticism over national security and NSA activities. Snowden became a "hero" and "whistleblower" in regional and global discussions. According to a new Angus Reid Global internet survey, Americans are split on Edward Snowden and concerned about government spying. 51% of Americans called the NSA leaker *"something of a hero who should be commended for letting the public know that our governments are running electronic surveillance programs that threaten people's privacy,"* while 49% called him *"more of a traitor who should be condemned for publicizing security activities and threatening western intelligence operations."* There were no choices for "neither" or "not sure." Even though 54% of Americans decided that *"protection and anti-terrorism initiatives imply that we may occasionally have to violate civil liberties like privacy of personal information,"* few are completely comfortable with this idea. Yet, 60% are opposed to extensive electronic government monitoring, and an equal amount of US people distrust the Obama administration to protect their personal data (Ariel & Freeman, 2013).

If Edward Snowden's leaks led to policy changes, better protections for civil rights, and a national conversation, does that mean he is more of a hero and whistleblower than a traitor? Obama's position is known. At a 2013 press conference, Obama indicated Americans would be better off if they hadn't discovered the government had been collecting enormous quantities of phone and Internet data. Obama denied Snowden's patriotism. Earlier, he had said that his government was already investigating systems that most Americans didn't know about (Wolf, 2013). Later, Obama disagreed with former Attorney General Eric Holder that Edward Snowden performed a "public service" by releasing thousands of sensitive national security papers in 2013. To illustrate, after Holder spoke on a podcast and recognized Snowden's importance in initiating

a public discussion about government monitoring, White House press secretary Josh Earnest said that *"The president has had the opportunity to speak on this a number of times, and I think a careful review of his public comments would indicate that he does not."* Earnest also informed interviewers that Holder himself said that Snowden ought to come back to the US from Russia and address the serious criminal allegations involving him (Gass, 2016). Additional to Obama's disagreement over Snowden's leaks, the former supported the idea that he wouldn't pardon him because he *"hasn't gone before a court,"* but Snowden's supporters disagreed, citing historical precedence. Particularly, he stated, *"I can't pardon somebody who hasn't gone before a court and presented themselves, so that's not something that I would comment on at this point,"* Obama said in an interview with the German newspaper Der Spiegel and public broadcaster ARD. *"I think that Mr. Snowden raised some legitimate concerns. How he did it was something that did not follow the procedures and practices of our intelligence community. If everybody took the approach that I make my own decisions about these issues, then it would be very hard to have an organized government or any kind of national security system"* (Toor, 2016).

Furthermore, President Obama called the National Security Agency's phone and other digital record collection "transparent" to PBS' Charlie Rose. He defended the program in a 2013 prerecorded interview, claiming the NSA had not unjustly targeted Americans. *"What I can say unequivocally is that if you are a U.S. person, the NSA cannot listen to your telephone calls, and the NSA cannot target your emails ... and have not,"* Obama stated. Later in the interview, he declared the project had *"disrupted"* terrorist activities abroad and in the US. The president cited the 2009 arrest of Najibullah Zazi, who planned to blow up the New York City metro (Reilly , 2013).

In order to portray Snowden as the opposite of a hero—a traitor—and eliminate his supporters, President Obama, Press Secretary Carney, and other administration officials created a composite scene (Price, n.d.). In particular, the government portrayed current NSA agents as brave warriors defending the country (Price, n.d.). Obama adopted a subtler approach in disputing the circumstances surrounding the leak and Snowden's own motives, while Carney employed more straightforward and brutal arguments in response to Snowden's claims of bravery. Obama and Carney both sought to dispute the exceptional character of Snowden's "heroic" mission. One of the main heroic components of Snowden's story was eliminated when Carney revealed that the challenge he faced was baseless and Obama criticized the "gift" that Snowden returned to humanity

in a similar manner (Price, n.d.). Also, he said that the administration has already acted to regulate and increase supervision of the operations. Snowden exposed and agreed that there should be enhanced openness and changes in the intelligence operations so that the public may have trust that these programs have robust supervision and clear safeguards against corruption, by introducing numerous measures that will help achieve this goal (The White House - Office of the Press Secretary, 2013).

Except for his theoretical response, in June 2013, President Obama practically responded to the Snowden leaks. In his first public response on the Snowden revelations, he said the phone collection program *"is fully overseen not just by Congress, but by the FISA Court. No one is listening to the content of people's phone calls."* He supports the statement that he had *"a healthy skepticism"* about the monitoring programs, but they stopped terrorist attacks. *"It's important to recognize that you can't have 100% security and also have 100% privacy and zero inconvenience,"* he claims. *"We're going to have to make some choices as a society"* (Breslow, 2014).

In August 2013, he established the President's Review Group, which was a call to the government to increase public trust. P.R.G. provided a detailed plan, composed of 46 recommendations, including Section 215 of the USA PATRIOT Act, for reaffirming privacy and civil rights without jeopardizing national security. It recommended openness and supervision to safeguard U.S. national security and enhance foreign policy. The Review Group also requested that the U.S. prove the need for secrecy (American Library Association, 2014). The culmination of this procedure was Obama's January 17, 2014, public speech on mass surveillance. He promised stricter controls on the collection of data on Americans, including the requirement of judicial approval for inquiries into phone records. Obama also promised stronger oversight and acknowledged that NSA spying created a threat to individual freedoms (Wikipedia, n.d.; Obama, 2005; The Editorial Board, 2014; Obama, 2014). The president's message seemed to target two main audiences: The American public, worried about liberty and privacy, and the foreign public, worried about America's intelligence capabilities. Taking into consideration these two aspects, some of the most meaningful and solid reforms declared by Obama are the following: (a) The NSA would stop storing the collected data according to Section 215 of FISA but keep it accessible. Obama supported this plan, forcing the intelligence agency to propose new metadata storage methods by March 2014. The Attorney General and the Intelligence Community (IC) would create a new initiative that could meet the potential and cover the weaknesses of the Section 215 metadata

program without the administration storing bulk phone metadata archives. (b) The NSA would only search the database with court authorization or in an urgent situation, and it would limit itself to searching data that is only two "hops" away from its aim (Nicoll & Delaney, 2014; The White House, 2014). (c) The passage of the USA FREEDOM Act. On the one hand, the bill controls Patriot Act bulk record collecting: (i) it prevents Section 215 of the Patriot Act from collecting every American's phone number and other information. The government could only seek records on terrorists and spies, those in touch with them, and/or their activities. (ii) It modifies NSL laws, which enable the FBI to obtain communication, financial, and credit data without a warrant. On the other hand, it adds privacy safeguards to the FISA Amendments Act of 2008 (a.k.a. Prism/Upstream): (i) It bans the government from investigating US citizen information obtained under this statute except when there is an emergency or a court ruling, and (ii) The bill restricts this program's data collection. The government may now gather foreign intelligence to, from, or about a "target" as long as it doesn't target Americans overseas or in the U.S. The law would constrain the "about" topic to counterterrorism (ACLU, 2013; 113th Congress, 2013-2014). (d) Instructions to the Director of National Intelligence to evaluate the Foreign Intelligence Surveillance Court's (FISC) rulings on agencies' surveillance warrant requests yearly to declassify as many as feasible. (e) The new presidential order would specify foreign surveillance rules (what may and may not be done). Such collection would only occur in response to specified needs and for national security reasons (Nicoll & Delaney, 2014).

**Figure 13 – A brief representation of the 12 basic NSA surveillance reforms.**

1.	Stop mass surveillance of digital communications.
2.	Protect the privacy rights of foreigners.
3.	No data retention.
4.	Ban no-review National Security Letters.
5.	Stop undermining Internet security (weakening the encryption).
6.	Oppose the FISA Improvement Act (legitimizing the NSA's unlawful collection and storage of US people's' phone data).

7.	Reject the Third-Party Doctrine
8.	Provide public accounting of spying programs.
9.	Embrace meaningful transparency reform.
10.	Reform the FISA court (independent FISA court advocates and a yearly review of FISA court judgments for declassification).
11.	Protect national security whistleblowers.
12.	Give criminal defendants all surveillance evidence (the accused ones should see every evidence against them).

(Source: <https://www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained>)

Consequently, it is essential to know what the government has really changed since Snowden and what is still the same. In particular, (a) personal data now have "Appropriate Safeguards" unless they conflict with national security (Non-U.S. citizens' personal data may only be stored for five years. Unless the DNI finds a national security cause to maintain the material, agents must destroy it after five years), (b) The government may still collect Americans' data without a warrant (when the government gathers foreigners' data, it surely gathers Americans' conversations, too – "incidental" or "backdoor" collection), (c) National Security Letters are now no longer valid until the FBI agrees to extend them (the orders end after 3 years, unless the FBI sends a letter demanding its extension), (d) The bulk gathering of telephone metadata continues (from 3 "hops" to 2 "hops"), (e) The government refuses to reveal how it treats NSA personnel who violate their authority (Sen. Charles Grassley's letter to the Justice Department, but no response yet), (f) The government continues to spy on some foreign leaders (for national security, anyone can be questioned) (Childress, 2015).

In summary, President Obama proposed a number of changes to the country's surveillance system in 2014. One of these changes was to add more privacy protections to a controversial National Security Agency program that collects the phone numbers of many Americans. But the amendments leave open a number of questions that Congress and other government bodies will have to answer. One of the most noticeable and essential responses came from Sen. Rand Paul, who said that he is "encouraged" by Obama's reforms but frustrated by the details (Condon, 2014).



In addition, he stated that *"the Fourth Amendment requires an individualized warrant based on probable cause before the government can search phone records and e-mails. President Obama's announced solution to the NSA spying controversy is the same unconstitutional program with a new configuration. I intend to continue the fight to restore Americans rights through my Fourth Amendment Restoration Act and my legal challenge against the NSA. The American people should not expect the fox to guard the hen house"* (Leary , 2014).

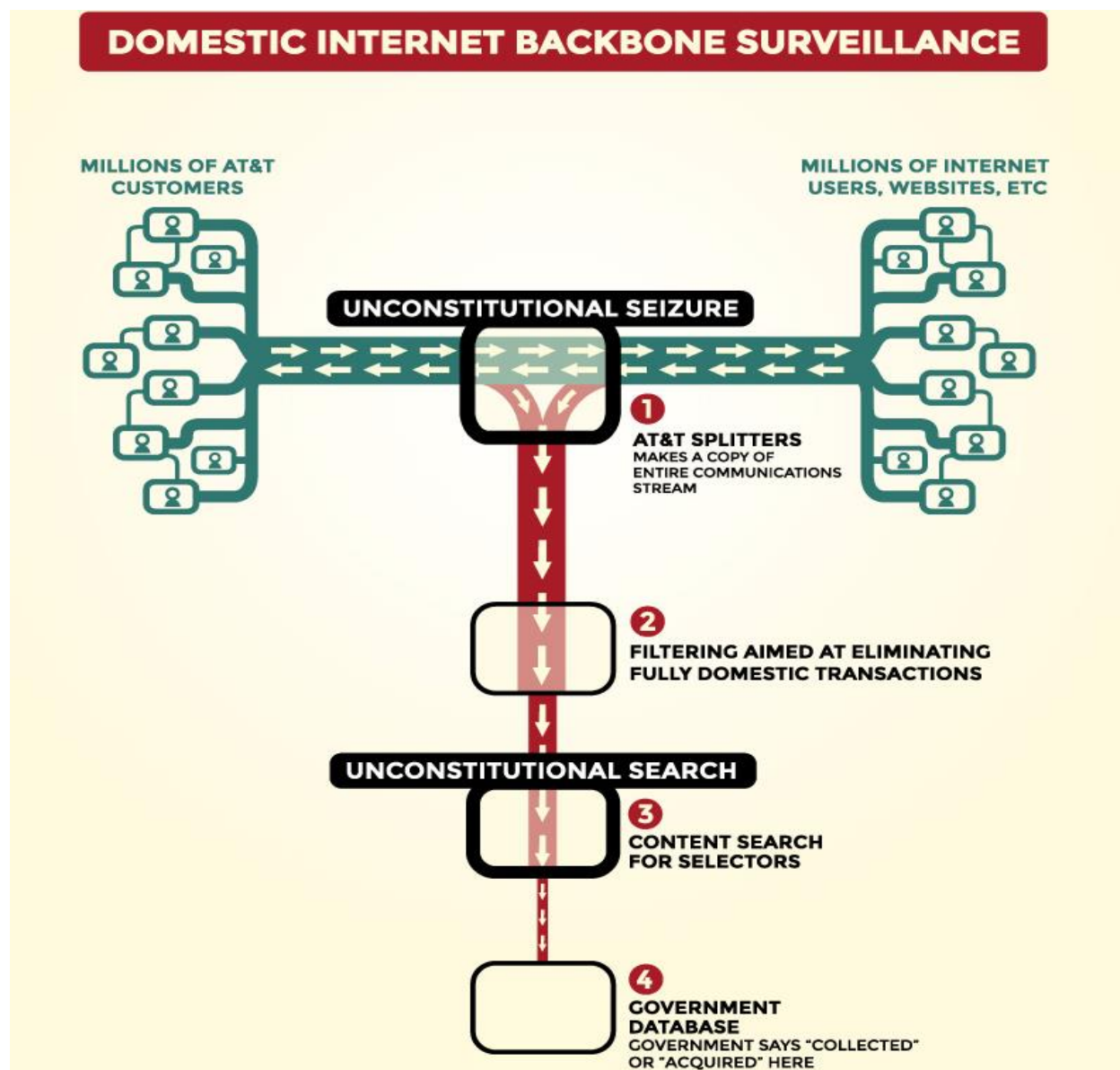
### **III.6 Reactions to Obama's reforms.**

Benjamin Franklin once stated: *"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."* This quotation is often used in relation to new technologies and worries about government spying. Franklin was indeed an innovator, but it's safe to assume he didn't foresee a future with smartphones and all the privacy concerns they entail. However, his arguments are often used to address these problems (All Things Considered, 2015).

The US Constitution and democratic system require the government to be transparent and accountable to its citizens. Previous experience has shown that hidden surveillance techniques are almost always used for political purposes (ACLU, n.d.). In this direction, several human rights groups, on the one hand, are suing the NSA and Obama over metadata gathering, asserting civil rights abuses, and, on the other hand, are requesting a pardon for the guy who exposed Obama's lack of openness (Waddell, 2016; McCarthy, 2016). The ACLU, Amnesty International, the EFF, and Human Rights Watch want President Obama to forgive the former NSA contractor (Waddell, 2016). Namely, the ACLU has filed a few cases to defend the fundamental freedoms of association, free expression, and privacy. Such cases were: (a) *Amnesty v. Clapper* (against the FAA); (b) *Wikimedia Foundation v. NSA* (against the "Upstream" program); (c) the Freedom of Information Act lawsuit (with the Media Freedom Information Access Clinic at Yale Law School—against E.O. 12333); (d) three motions in the Foreign Intelligence Surveillance Court (FISC) (requesting the release of confidential documents allowing the monitoring of Americans); (e) a submission of a brief in the FISC in defense of the First Amendment rights of FISC order recipients, such as internet and phone firms, to reveal information regarding NSA and FBI national security requests

(ACLU, n.d.) (ACLU, 2021). Besides this, the EFF had also led efforts to halt illegal surveillance and put government monitoring programs back inside the law and Constitution. Such cases were: (a) Jewel v. NSA (lawsuit against the NSA's dragnet surveillance), (b) Shubert v. Obama (same claims), (c) First Unitarian v. NSA (lawsuit opposing NSA phone metadata collection), (d) Hepting v. AT&T, (lawsuit against involvement of the AT&T - a collaborating telecommunications company - in unlawful NSA surveillance), Smith v. Obama (EFF and the ACLU have appealed a nurse's lawsuit against the NSA's collection of phone records (EFF, n.d.).

Figure 14 – Domestic Internet Backbone Surveillance.



(Source: <https://www.eff.org/nsa-spying>)

Likewise, civil-rights organizations' pardon proposals coincide with Oliver Stone's Snowden biopic. Full-page advertisements ran in "The Washington Post" and "Politico." Big-name supporters in computing (Wikipedia's Jimmy Wales and Apple's Steve Wozniak), Hollywood (Danny Glover, Susan Sarandon), human rights promotion (George Soros), and academics have signed a letter requesting a pardon for Snowden. Contrary to White House press office declarations, many believed that the Obama administration had frequently been unfriendly to journalists and whistleblowers, undermining his promise of unprecedented openness. Earlier, Snowden and his allies believed the president would have made a peace offering before leaving office. On the contrary, he removed any possibility for a pardon (Waddell, 2016).

## **Chapter IV: Edward Snowden Disclosures: Discussion and Reflections.**

“Though the outcome of my efforts has been demonstrably positive, my government continues to treat dissent as defection, and seeks to criminalize political speech with felony charges that provide no defense. However, speaking the truth is not a crime. I am confident that with the support of the international community, the government of the United States will abandon this harmful behavior.”

— Edward Snowden to Chancellor Angela Merkel,  
European Parliament president Norbert Lamment, and  
German attorney general Harald Range, October 31, 2013

“The prime reason for secrecy is that you don’t want the targets to know what you are doing. But often in democracies, another reason is that you don’t want your citizens to know what their government is doing on their behalf to keep them secure, as long as it’s within their country’s law.”

—Walter Pincus, in the Washington Post, December 25, 2013

“I would say the best part of the Obama administration would be his continuance of the protections of the homeland using the big metadata programs, the NSA being enhanced.”

—Jeb Bush, April 21, 2015

“We have it back. The statue is free.”

—Snowden bust activists, May 7, 201

### ***IV.1 Snowden's motives: A Whistleblower or a Traitor?***

In 2013, the term "Edward Snowden" became linked with words like "hero," "traitor," "whistleblower," and "spy." These classifications are probably justified because he obtained about 1.7 million documents from the NSA, many of which, according to the Pentagon, fall under the category of highly sensitive material. Is Snowden a hero for sparking a discussion about intelligence activities or a traitor for obtaining sensitive information? To just consider Snowden a hero or a traitor is a mindless approach to categorizing him, because both of those words have a lot of possible meanings. In contrast, the media's depiction of Snowden is a "false dichotomy." A "false dichotomy" is essentially when two choices are presented to a public, in this case to Americans, and are thought to be mutually exclusive in order to preserve simplicity, such as "you are wrong or right" (Puntambekar, n.d.).

His revelations about government monitoring activities horrified many Americans. With such programs now under threat, the argument over whether Snowden's activities were justified is heating up (Smith, 2014). The "world's most wanted man" is among the most controversial characters in contemporary history. This is especially noticeable in the United States, since opinions over his disclosure of sensitive material could not be more polarized. According to many law experts and the U.S. government, his acts broke the Espionage Act of 1917, which says that leaking government secrets is a treasonous act. Despite breaking the law, Snowden said he had a moral responsibility to act (Alati, 2015; Ethics Unwrapped, n.d.). *"To inform the public as to that which is done in their name and that which is done against them"* was his argument for "whistleblowing." Snowden believed that the government's violations of privacy should be exposed regardless of legality. Also, Snowden has supporters. Jesselyn Radack of the Government Accountability Project justified his actions as moral, saying he acted for the public's benefit. *"Snowden may have violated a secrecy agreement, which is not a loyalty oath but a contract, and a less important one than the social contract a democracy has with its citizenry,"* Radack added. Others contended that the legislation was wrong and unconstitutional, thus he was not morally accountable. In contrast, Eric Holder, the US Attorney General, rejected Snowden's reasoning. Holder said, "He broke the law. He caused harm to our national security, and I think that he has to be held accountable for his actions" (Ethics Unwrapped, n.d.).

Generally, in a democracy, whistleblowing is a procedure that works in a strange way, just like all of democracy's concepts. On the one hand, whistleblowers may hurt society by raising

violence or helping foes. On the other hand, depending on the demands of the population, the limits of acceptable whistleblowing procedures shift; consequently, it is disrespectful to democratic ideals for government officials to impose a specific whistleblower policy. In practice, whistleblowing is a way to stop a government agency from becoming too authoritarian when the gap between them and the people they serve has grown too wide (Guitar, 2018). Following this narrative, E. Snowden, in his own words, justified his actions and the motives behind them in the video interview with the Guardian. To illustrate, when Glenn Greenwald asked him the following question, *"One of the things people are going to be most interested in, in trying to understand what—who you are and what you're thinking, is whether there came some point in time when you crossed this line of thinking about being a whistleblower to making the choice to actually become a whistleblower. Walk people through that decision-making process."*, he immediately responded *"When you're in positions of privileged access, like a systems administrator for these sort of the intelligence community agencies, you're exposed to a lot more information on a broader scale than the average employee, and because of that, you see things that may be disturbing. But over the course of a normal person's career, you'd only see one or two of these instances. When you see everything, you see them on a more frequent basis, and you recognize that some of these things are actually abuses. And when you talk to people about them in a place like this, where this is the normal state of business, people tend not to take them very seriously and, you know, move on from them. But over time, that awareness of wrongdoing sort of builds up, and you feel compelled to talk about it. And the more you talk about it, the more you're ignored, the more you're told it's not a problem, until eventually you realize that these things need to be determined by the public, not by somebody who was simply hired by the government."* Furthermore, and as detailed below in the interview, Greenwald fundamentally asked Snowden, *"If your motive had been to harm the United States and help its enemies, or if your motive had been personal material gain, were there things that you could have done with these documents to advance those goals that you didn't end up doing?"* and the latter answered *"Absolutely. I mean, anybody in the positions of access with the technical capabilities that I had could, you know, suck out secrets, pass them on the open market to Russia. You know, they always have an open door, as we do. I had access to, you know, the full rosters of everyone working at the NSA, the entire intelligence community, and undercover assets all around the world, the locations of every station we have, what their missions are, and so forth. If I had just wanted to harm the U.S., you know, that—you could shut down the surveillance system*

*in an afternoon. But that's not my intention. And I think, for anyone making that argument, they need to think, if they were in my position, and, you know, you live a privileged life—you're living in Hawaii, in paradise, and making a ton of money—what would it take to make you leave everything behind?"* (Russel, 2013).

Obviously, Snowden's defenders consider him a "whistleblower." A government employee who exposes government misbehavior. Whistleblowers holding secret information are protected by law. However, these laws initially compel whistleblowers to submit their suspicions to the intelligence agencies' inspector general or the intelligence committees of Congress. Snowden didn't do this. Snowden claimed he was not protected as a whistleblower since he was a private contractor and not a state employee. He believed that if he had followed the protocol, his constitutional protection would have been unclear. Thus, Snowden triggered a tremendous discussion about mass surveillance. Was the NSA violating privacy or protecting Americans? Yes, to both questions, according to the Freedom Act. However, what should be done about Snowden, who began the scandal? Should he have been concerned about being a villain or a hero? (Constitutional Rights Foundation, 2016)

Standing alongside Journalist Jay Epstein's book, "How America Lost Its Secrets: Edward Snowden, The Man, and The Theft," it accurately portrays Snowden's two points of view. The first portrays him as a whistleblower who risked everything to expose unethical American government spying techniques. The second implies that Snowden was a spy who conducted espionage for other countries in order to benefit personally, and that he was probably too smart by half (Johnson, et al., 2014). In that case, what was Edward Snowden's true motivation for obtaining a large number of secret National Security Agency archives? Edward Jay Epstein claims he has uncovered a remarkable answer: that even though he initially intended to expose official illegalities occurring by the US government, by the time he landed in Moscow he had become an active "espionage source" for the Russian spy agencies, under an agreement directly authorized by Vladimir Putin. Moreover, he is more persuasive in questioning Mr. Snowden's image as a selfless whistleblower. At a minimum, Mr. Epstein demonstrates that much of Mr. Snowden's plot does not work perfectly and that his tactics were morally questionable, even if one recognizes the benefit he achieved by drawing attention to the NSA's domestic data-collection practices (Budiansky, 2017). This can be explained and at the same time makes us suspicious about Snowden's top four "questionable" and "weird" selections: First, to quit Dell for a lower-paying position at Booz Allen with NSA access.

Second, to select Hong Kong as his primary destination. Third, to publicly acknowledge his role in the "leak." The fourth and last choice was to depart Hong Kong—where China's spy agencies may have spoken with him—for Moscow (Moon, 2017).

Additionally, analyzing Snowden's tactics and supporting Epstein's approach, we conclude that (a) Snowden is a reclusive individual with delusions about his self-significance. (b) There are strong indicators that he got assistance from NSA collaborators who might still be in crucial NSA positions. (c) He worked as a contractor for Booz Allen in order to attend an NSA site in Hawaii. (d) He promised to deliver secret material to Guardian reporter Laura Portia in 6 to 8 weeks before starting work at the NSA site where he stole it. (e) He had 5 weeks to get 16 passwords, get into accounts, and transfer data. (f) He made these commitments and actions as a new worker with no prior NSA contacts or relationships, then (g) Snowden escaped to Hong Kong, and all was set until Vladimir Putin directly authorized his trip to Moscow (Moon, 2017).

Consequently, it is crucial to point out that the debriefing with Snowden will be a huge job for Russian intelligence and that they will try to hide any details they find useful. Snowden has deeply hurt intelligence agencies, those of close allies, and perhaps the US's capability to combat the War on Terror by revealing the NSA's infrastructure and its powers. Taking into consideration this crisis, what can be taught? Intelligence, counterintelligence, and spy specialists have remained mostly undercover. Congress and politicians must be educated on the fact that we cannot always choose the cheapest approach. Technology brings benefits, but it also comes with risks. People allowed into secure locations might need to be tested and checked more meticulously. Snowden's stealing and lying are going to cost Americans a lot more than what it would cost to screen Snowden, Manning, and others more extensively. Undoubtedly, after 9/11, several things we took for granted changed completely in almost every social or political sector. In order to continue as a society, we must find a method to reconcile our fundamental beliefs of individual privacy and freedom with the necessity to function at a security level that protects people and the nation. This may take more work to stop people from using data gathering or other intelligence information to shut down opposing opinions while still letting professionals safeguard the nation and its people (Moon, 2017).



## ***IV.2 The consequences of the Snowden revelations.***

Since June 2013, Edward Snowden's disclosure of thousands of secret papers exposing extremely sensitive U.S. monitoring operations has dramatically escalated issues about privacy, trust, liberty, and national security in connection to the usage of global technology and communication systems (Rubinstein & Hoboken, 2014). In that case, "the world's most wanted man" is one of history's most controversial individuals. His releases of sensitive information have split the US, notably. Many Americans, including top officials, have openly called Snowden a cowardly traitor and urged him to come back to face a plethora of criminal offenses, including those arising from the 1917 Espionage Act. Yet many people have gone to huge efforts and taken significant risks to defend and aid him in exposing the most serious surveillance crimes ever revealed (Alati, 2015).

The Snowden leaks were the worst intelligence disaster in US history. Snowden's motives and whether he operated alone or with a foreign intelligence agency remained unclear, with Russia and China being the main suspects. The idea that he might have had external aid came from the fact that lots of the data he stole didn't get out to the public because it was about how the NSA broke into foreign computer systems, like those of China and Russia. Obviously, Snowden's impact was hard to measure, and the media that published the revelations said they did not impair US national security. But it was clear that the US had lost a strategic advantage in cyber power. That advantage would have deteriorated over years, but the effects of such a quick, massive loss were likely serious and moved beyond the cybersphere, perhaps causing a broader decline in Washington's worldwide core capabilities. Also, terrorist organizations like al-Qaeda have started to change their encryption techniques and minimize their use of information and communications technology (ICT) (Anon., 2014).

As a result, we may detect two sorts of effects from Snowden's case: the negative ones and the positive ones (Konstantopoulos, 2017). Analyzing the negative effects, the primary impact of Snowden's disclosures is more closely related to the deterioration of US foreign relations, security, and secrecy than it is to the erosion of privacy. Firstly, the UK and US administrations are alarmed about the sizable, illegal leaks of confidential material by disgruntled personnel, known as "whistle-blowers." The US spends US\$11 billion on classification annually. Nonetheless, little is known about elite views regarding secrecy and its enemies. At an era when lawmakers are actively assessing these science-security problems, we must recognize this remarkable gap. Secondly,

Snowden's huge releases of classified NSA data caused national security concerns (Johnson, et al., 2014). Former NSA and CIA director Michael Hayden feared that the Snowden revelations would reveal U.S. intelligence "tactics, techniques, and procedures" to terrorists. Thirdly, the revelations also exposed U.S. allies' espionage tactics. Theresa May, Britain's Home Secretary, stated that they damaged global intelligence. She highlighted that the Islamic State has created a clip containing Snowden leak-inspired non-detecting instructions (Constitutional Rights Foundation, 2016). Fourthly, in the areas of politics and diplomacy, relations between the U.S. and its allies were hurt or even destroyed (von Solms & van Heerden, 2015). In particular, (1) Brazil: The president of Brazil postponed an official visit to Washington because she was upset that the NSA had spied on her and other Brazilian politicians. The Brazilian president's office cited a "*lack of... explanations and commitment to cease interceptive activities*" for the cancellation. Additionally, the spying scandal diminished U.S. prospects of selling fighter jets (36 F-18 fighter jets) to Brazil (Hennessey & Bevins, 2013; Boadle & Soto, 2013; Groll, 2013). (2) Germany: The German government reacted strongly to Chancellor Angela Merkel's phone tapping. Attempts to stop reciprocal intelligence activities have also increased. Germany wanted an intergovernmental agreement and a security services agreement with the US to replace the current legislation. Later, German society had two reactions to the spying allegations. On the one hand, there was a significant decrease in US trust. On the other hand, most Germans didn't feel endangered by the NSA. In short, that trust crisis was the most crucial since Germany opposed the US invasion of Iraq in 2003 in the UN Security Council (Zawilska-Florczuk & Frymark, 2014). (3) Russia: Relations between the United States and Russia reached an all-time low when Moscow rejected U.S. demands and granted temporary asylum to Snowden. Many in Congress were arguing that the Snowden case was the Kremlin's latest snub to the White House. Furthermore, the Russian President attempted to diminish the role of US intelligence in the eyes of the West when he was questioned about Russia's stance on mass surveillance on a TV show by Snowden. He responded, "*Our agents are controlled by law. You have to get court permission to put an individual under surveillance. We don't have mass permission, and our law makes it impossible for that kind of mass permission to exist,*" highlighting the fact that Russia does not conduct widespread surveillance as Snowden revealed in the US (Kelemen, 2013; Gentleman & Hopkins, 2014). (4) Cloud computing: Snowden's NSA disclosures changed cloud computing, offering advantages and challenges alike. After the facts were revealed, privacy arguments exploded. The discoveries caused foreign distrust in American

cloud computing, which led to enormous withdrawals and an economic struggle for American computer businesses and the American economy. Governments' worries about US-based cloud computing are hurting American cloud services. For example, IBM is spending more than \$1 billion to build data centers outside of the US, Microsoft has lost a lot of business, especially in Brazil, and non-US tech companies are picking up the business that American companies lost because they were afraid of NSA spying. The policies and suggestions of countries will have a big effect on how businesses work and what they do (Soviak, 2015; Cain Miller, 2014). (5) Privacy Concerns: People's privacy concerns have been heightened as a result of the Snowden revelations. Individual privacy may be returning as a cultural norm after the Snowden disclosures. In a November 2013 Harris Poll, 80% of people amended their social media privacy parameters, most within six months. Consequently, people's interest in privacy measures such as anonymizers and encryption has skyrocketed (Harvard University, n.d.; Eset, 2014; von Solms & van Heerden, 2015).

That being said, there are also a few benefits: (1) Right after the disclosures, Obama proposed increased oversight of the intelligence community's monitoring activities in order to balance Americans' safety and privacy (Madhani & Jackson, n.d.). On January 17, 2014, he announced an NSA reform proposal that would cease the storage of phone call data. He suggested a number of changes to how the NSA should perform surveillance and intelligence collection (Savage, 2014; von Solms & van Heerden, 2015). In particular, he ordered the Section 215 program's initial change. The N.S.A. would stop tracking Americans' calls, and phone companies would keep bulk records but not for longer than usual. Also, the N.S.A. would need a fresh court order to access certain documents. The government may access the program's phone metadata only when a court permits particular numbers for national security searches (The White House, 2014) (Savage, 2014; von Solms & van Heerden, 2015). Additionally, the results of any query are restricted to metadata stemmed from a two-hop rather than a three-hop procedure (The White House, 2014; von Solms & van Heerden, 2015). (2) Much more is known about the actions of governments. For example, the NSA secretly demanded users' data from Facebook, Google, and Microsoft, and it captured, saved, and analyzed "metadata" from every call and text in Mexico, Kenya, and the Philippines. (3) Mass surveillance has provoked strong popular resistance. In a 13-country Amnesty International survey, 71% of voters disapproved of their governments' spying on internet and phone use. (4) Judges found several of these programs unlawful. The UK's secret

service legal authority ruled that parts of the US-UK intercepted communication exchange were illegal before December 2014. In May 2015, a US appeals court declared bulk phone data gathering unlawful. (5) Tech companies and software developers were incorporating privacy features into their products. (6) Global experts criticized the current status quo, and they argued that excessive spying threatens human rights. (7) Companies were defying governments. Apple, Facebook, Google, Microsoft, Twitter, and Yahoo have started a campaign to stop the mass collection of personal information. (8) The laws that supported bulk surveillance were under further review. A UK government committee has recommended reforming intelligence agency legislation to increase transparency and The USA Freedom Act prohibited the government from mass gathering phone data in the United States (Amnesty International, 2015).

To sum up, Mr. Snowden revealed thousands of confidential papers detailing US and other global surveillance operations. His actions greatly impacted the US government and intelligence sector. These disclosures damaged counterterrorism operations and confused interactions with internet firms, putting national security at stake while also hurting US-allied ties and leading to a worldwide rejection of wide surveillance. The Snowden leaks were the most catastrophic violation of US secrets in history (Lands, 2017).

### ***IV.3 The institutions as counterweights and overseers of the security state: Changes after the Snowden revelations and proposals for the protection of classified information.***

Three crucial institutions that act as counterweights and oversight to the security state have been substantially changed as a result of the discussion that Snowden helped to initiate (Wizner, 2017).

First of all, "the Courts." In March 2013, barely three months before the initial Snowden leaks, a constitutional challenge to an NSA monitoring program was rejected by the U.S. Supreme Court. To illustrate, the case was no other than the "Clapper v. Amnesty International USA" case (Wizner, 2017). The U.S. Supreme Court declined to grant standing to citizens of the United States who worried that their communications with citizens of other nations might be intercepted by the American government. The Court determined that the plaintiffs could not demonstrate that their interception was sufficiently likely to occur since they could not be the genuine targets of surveillance permitted by the disputed legislation, 50 U.S.C. Section 1881a. By denying standing, the Court significantly constrained U.S. citizens' ability to oppose the federal government's expanding monitoring practices (Rinehart, 2014). Following this, in June 2013, "The Guardian" revealed that the National Security Agency was collecting the telephone information of millions of Verizon customers, one of America's major telecommunications providers, under a top-secret court ruling. The ACLU was a client, too, and sued the National Security Agency for collecting vast amounts of phone records (ACLU, 2015; Wizner, 2017). Thus, in the wake of Snowden's effects, the U.S. Court of Appeals for the Second Circuit ruled in *ACLU v. Clapper* that the NSA's telephone records program exceeded Congress' 2001 authorization (Section 215 of the Patriot Act). The court unanimously rejected the government's hidden interpretations of Section 215. The court ruled that Section 215 did not permit the mass gathering of telephone records. Also, it objected to the secret and one-sided Foreign Intelligence Surveillance Court's approval of this restrictive interpretation of the law (FISA Court) (Greene, 2015). The decision was a big win for advocates across the political scene, within and outside the government, who have argued that some of the agency's surveillance operations are overbroad and unconstitutional and that Congress' 1978 oversight mechanism isn't performing well. Also, it paved the way for other organizations to challenge the government's controversial intelligence policies and actions (Jaffer, 2015).

In addition, "Congress." On March 12, 2013, Clapper testified before the U.S. Select Committee on Intelligence as national intelligence director, a role established in 2004 to oversee foreign, military, and domestic intelligence for national security. The committee oversees executive branch intelligence activities and has access to confidential briefings, sources, and funding. During the public hearing, Oregon Democrat Sen. Ron Wyden questioned Mr. Clapper whether the NSA gathers *"any type of data at all on millions or hundreds of millions of Americans."* *"No, sir," Mr. Clapper said. "Not wittingly"* (Contorno, 2014; Andrew Blake The Washington Times, 2019). The response was shown to be false when the Guardian released a top-secret court order obtained by Snowden, which revealed the NSA was collecting the phone data of millions of US residents (Ackerman, 2014). Thus, after Snowden's leaks, everyone was talking about Clapper's false claim. The intelligence head subsequently admitted he fought to keep sensitive programs secret at the hearing. Clapper said he answered in the *"least untruthful manner"*. He apologized to Wyden. Furthermore, a discussion over privacy and national security "has been welcomed" by the Obama administration (Ackerman, 2014; Fahrenthold, 2013; Contorno, 2014). Wyden and other members of Congress already knew the answer to the aforementioned question. Clapper already knew the answer. Yes, was the answer. But none of them managed to alter the public record. This debate demonstrates how the security state often resists legislative oversight. Even Senator Wyden, who opposed the intelligence community's policies and disinformation, felt it was worthless to inform the public. *"When the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry,"* Wyden said on the Senate floor in May 2011. That was correct, but in that case, unfortunately, it was Edward Snowden, not Congress, who gave Americans a voice in the discussion (Wizner, 2017). After a discussion pitting Americans' skepticism of intrusive government against worries of terrorist threats, the Senate decided to move reform measures to replace the bulk phone data program exposed by Snowden. Most Democrats, including Obama, approved the Freedom Act. Also, the House approved it by 338 to 88 on May 13 (Zengerle & Strobel, 2015). After a heated discussion, the intelligence agency and its supporters used their whole arsenal of tactics to imply that lawmakers who let the Patriot Act's full powers expire would be responsible for future terrorist attacks. This line of thinking had essentially assured congressional approval in earlier decades, but in the aftermath of the Snowden disclosures, a bipartisan alliance of politicians questioned the intelligence community's policies. However, the USA Freedom Act did not fix mass surveillance

problems, but it revived congressional oversight, which was unthinkable before Snowden (Wizner, 2017).

Moreover, "the Media." In 2004, two New York Times investigative writers found that President George W. Bush had allowed the NSA to perform massive domestic eavesdropping in violation of the Foreign Intelligence Surveillance Act. However, they did not disclose their results until December 2005, after President Bush was reelected. After national security officials—including the president—warned The Times that the publication would jeopardize a crucial program and endanger American lives, the newspaper suppressed the story for almost a year. Only when its own reporter, James Risen, was going to write a book about the story did the Times change its mind. No one has ever seriously suggested that NSA program disclosure harms national security. Consequently, Snowden was convinced by this incident that he shouldn't provide the papers to just one media source. Because of this decision, other news and media organizations like The Washington Post and The Guardian had to think twice not only about the government's usual cautions but also about competitors getting the story first. As a result of the involvement of more news organizations, the field of national security reporting has been drastically altered (Wizner, 2017).

Consequently, following the Snowden discussion, the three aforementioned vital intelligence oversight mechanisms have been improved. It may seem paradoxical that such a serious violation of the law had the effect of reviving effective democratic oversight, but it is almost true if we take into consideration that reforming congressional oversight of intelligence is incredibly challenging (Wizner, 2017). However, safeguarding classified sensitive national security data and other controlled information is the first step and the foundation for achieving essential oversight reform. This is crucial not only to the executive branch, which decides, for the most part, what information needs to be kept safe, but also to Congress, which utilizes these data to fulfill its constitutional duties. It has created methods to protect controlled information in its possession, although these procedures have changed over the years between the two chambers and panels within each chamber. For instance, both chambers have formed offices of security to consolidate related duties, although these were created twenty years apart. Also, other committee distinctions arise. Some of the proposed changes are contentious, as they frequently seek to establish unifying standards for congressional offices and personnel, as well as to improve access appropriateness criteria (Kaiser, 2010). Namely, some of these proposals may include: 1) Congress

must have security clearances to access classified information. This requirement would prevent leaks and accidental disclosures by restricting access to "trustworthy" members. 2) Require senators or Senate personnel to sign a secrecy oath to gain access, similar to the House requirements. This demand would have banned intelligence institutions from sharing classified material with Members of Congress and their personnel, as well as officials and staff of the executive branch, unless the receivers had approved a nondisclosure agreement committing that they would not intentionally in any way reveal any secret information to any unauthorized person. 3) Instruct all cleared staff—or just the highest levels—to submit detailed financial statements every year. This option may help identify and investigate financial wrongdoing. (4) Strengthening encryption. Improved encryption technologies can help protect classified information and improve privacy while enhancing national security (Weinstein, 2023).

In conclusion, the Constitution gives Congress the responsibility of overseeing the executive branch's operations in order to ensure democratic accountability and to raise the standard of decision-making. The work of the U.S. intelligence services is very important to national security, so it must be done in secret. These features make professional external oversight essential for preventing abuses and corruption and enhancing the quality and reliability of intelligence efforts, but they also make that oversight very complex. Intelligence and oversight crises haunt US history. Learning from these experiences and mistakes, Congress has developed a credible framework and mechanism for oversight. However, congressional overseers face obstacles and difficulties that undermine intelligence oversight and Congress's attempts to hold US intelligence agencies accountable (DeRosa, 2022).



#### ***IV.4 Intelligence vs Democracy: How to achieve harmony between security and privacy and shape the pathway to reform?***

The right to privacy in the era of surveillance is a divisive topic with a long history. This debate was at its most heated in 2001, after the 9/11 terrorist attacks, and again in 2013, when Edward Snowden revealed that a lot of people were being watched. In both instances, the debate that followed emphasized whether monitoring and intelligence were fundamental for security or whether they violated the right to privacy (Roy, 2018). In democracies, the function of intelligence remains contentious and challenging at times. Democracies rely on transparency. Yet they face threats from both abroad and at home that need to be defended by all parts of national power, including intelligence. Like the military, intelligence needs careful oversight and compliance with the US Constitution and national legislation. However, in protecting national security, sometimes intelligence threatens democratic values. Today's intelligence operation is more complicated than ever before, and the oversight system that balances security and liberty has been sharply challenged (Roger, 2020).

In a democracy, the most important thing intelligence agencies do is tell the government about risks from both inside and outside the country. Therefore, defining intelligence is crucial at this time. Due to intelligence's range and variety, its necessity is disputed. According to Mark Lowenthal, intelligence has at least three purposes. It is the process through which governments request, gather, analyze, and disseminate necessary data, and plan and carry out covert activities. Intelligence includes the results of intelligence collection, analysis, and covert activities. Intelligence also refers to the organization's agencies. Process—gathering and utilizing information for a purpose—is the most important of the three characteristics for this topic. Since methods, information sources, and future purposes vary, much about them must remain unclear. Those who familiarize themselves with intelligence processes and their limits are more likely to recognize that not everything is knowable (Bruneau & Dombroski, n.d.) .

Also, New York University law and philosophy professor Jeremy Waldron has looked at how war and crises change people's ideas about freedom and safety in the post-9/11 world (Waldron, 2003). Time and group differences affect liberty in societies periodically. Time may influence people's views on how much liberty they need and are willing to sacrifice for security. However, liberty may vary across people and groups, as demonstrated in the post-9/11 period with

Muslim and ethnic groups that behaved or looked like media-portrayed terrorists. This might suggest that people with foreign names and connections with other nations, particularly Middle Eastern countries, may be subject to greater spying and metadata gathering than those with American or western-sounding names, regardless of nationality. When discussing liberty (privacy) and security and how people's perceptions of them change over time, it's important to keep in mind that time impacts can be seen in both short-and long-term terms (Olesen, n.d.). On June 7, 2013, President Obama defended the monitoring programs and said that it is unrealistic for the nation to have 100% security and 100% privacy, and that society must make compromises in terms of privacy to achieve security (Spetalnick & Holland, 2013; Olesen, n.d.). This phrase contrasts with Benjamin Franklin's 1775 remarks (Olesen, n.d.): "*They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety*" (Franklin, 2021). After 250 years, the globe has altered dramatically (Olesen, n.d.). Today's world is a challenging arena to manage. Since life is so fast-paced and globalized, there are a lot of new and rising threats, and there are few opportunities for thoughtful thinking. In addition, the number of laws and regulations that everyone must follow is expanding (Jensen, III, et al., 2018; Obama, 2013). Since 1775, the US has become a worldwide powerhouse, fought multiple wars, had internal disputes, and attracted many enemies. In 1775, no one could have predicted globalization and the rise of weaponry that could kill thousands in minutes—weapons that the US's adversaries have, too. Thus, terrorism and hostile threats have significantly expanded, making security a more vital virtue (Olesen, n.d.). Certainly, the US faces a variety of threats. Most of them are complicated. The US is deeply engaged globally. So, since it operates in a risky environment, it must accept the risks as well. Since the end of the Cold War, the IC has endeavored to define its position in American governance. As things now stand, it must be ready to handle anything from natural catastrophes to WMDs. Many of these hazards are known, while others are not. National leaders must monitor these rising threats and prepare the country and its resources to react (Jensen, III, et al., 2018; Obama, 2013).

Some people say that democracy and intelligence don't go together very well and that intelligence should be illegal. Like pacifism, this ideology obviously requires peaceful, non-threatening state interactions (Roger, 2020). But, in reality, to preserve constitutional democracy, intelligence and security agencies must ensure public safety. They have to deal with an underestimation of real threats and overreactions to fears of insecurity at the same time. They're

divided between the desire to "do something," even if it is illegal, and the necessity to follow the law. More than ever before, they must decide what is and isn't their job, such as information-gathering. They must consider legal, constitutional, and ethical issues. They must be mindful of political and administrative bodies' duties in a democratic nation regulated by the rule of law. They must realize that politicians and officials today understand institutional principles less well and sometimes know nothing about limits. They'll have to remind political leaders of their duties. In a nation based on the rule of law, intelligence agencies and courts cannot carry out political duties. Therefore, aren't the security services supposed to protect democracy and the law? This should encourage policymakers, particularly elected representatives, to scrutinize new measures and fight security policy's internal momentum. Above all, actions that limit civil liberties and basic rights should be rigorously assessed, using empirical data, for their effectiveness, need, legality, appropriateness, and discriminatory effects on vulnerable minorities. The intelligence agencies and their oversight organizations must be included in this evaluation. Their duty is to safeguard the constitutional legal system of their nation. They may evaluate the effectiveness, synergy, and social impact of previous initiatives. Finally, it's crucial to educate the public about genuine hazards stemming from terrorism and how they might be mitigated. Thus, people and civil society groups may help preserve the democratic legal system (Willink, 2007). As Bruce Schneier - Lecturer in Public Policy at the Harvard Kennedy School - stated "*Prevention is impossible. Mitigation is important. Intelligence and counterattack are critical, but neither is as effective as addressing the root causes of terrorism*" (Schneier, 2003). The democratic state's rule of law, basic rights, diversity, and compassion are not terrorism's roots. However, democracy and the rule of law are the primary tools for combating this. To prevent terrorism, democracy and the rule of law should not be limited. They should be used to combat terrorists globally (Willink, 2007).

Consequently, for real intelligence reform, role advancement and best practices are required, and the IC must constantly face pressure from inside and outside to change its culture, tactics, and techniques, as well as have strong opinions about itself and its place in a complicated world. As ideas for how to do intelligence work in a free democracy with a big threat at home are looked into, the DNI needs to be able to act quickly on good ideas and get them written into new laws and rules. Success depends on effective policies. The intelligence reform is based on the Intelligence Reform and Terrorism Prevention Act and EO 12333. The review of EO 12333 enhanced the DNI's capacity to establish stable rules, but it did not eliminate all of the IRTPA's

vagueness. It is unclear that legislation will provide DNI with clear power in the foreseeable future. Intelligence is now a vital part of the majority of national-security agencies. Experts within and outside the IC should reopen the discussion about intelligence centralization. Regardless of the result of the discussion, IC must handle the challenges that sometimes lead to disputes, especially in the homeland defense sector. It is needed to find cheaper, faster, and more relevant methods to gather, analyze, and use data. Moreover, the DNI's "decision advantage" idea must be applicable not just to policymakers but also, for example, to soldiers in Baghdad or Kabul, who demand the appropriate intelligence to respond faster than the foe. It is needed to share more and keep less information, particularly with the internal state, regional, and local governments, and foreign allies (Clapper, Jr., 2010). To illustrate, as Jennifer Sims, Director of Intelligence Studies at Georgetown University, stated, *"...the key to intelligence-driven victories may not be the collection of objective 'truth' so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision-maker's quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence"* (McConell, 2015).

Aside from that, given that the government can collect, store, and search massive amounts of metadata through Section 215, this could violate the 4th Amendment in many cases (Atkins, 2014). Clearly stated in the 4th Amendment: *"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 warrant 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"* (Legal Information Institute, n.d.). The government has suggested amendments to reform Section 215, but it has not changed the NSA's metadata search standard yet. Thus, another essential reform is to place a right to privacy in metadata due to the vast volumes of information that can be extracted from it, exposing the private details of an individual's life. The Fourth Amendment should protect metadata. This would enable the NSA to get a warrant from FISC indicating probable cause that the subject is a terrorist. Therefore, a stronger standard (instead of reasonable and articulable suspicion) for the government to examine metadata offsets the need for privacy in this vast quantity of sensitive material against the need to safeguard Americans from possible terrorist threats (Atkins, 2014; Webster, 2021).

Looking forward, the demand for intelligence looks to be rising. On the one hand, when it comes to foreign policy, intelligence depends on the extent of international participation (e.g.,

power deployed) and the kind of foreign policy conducted. On the other hand, when it comes to domestic policy, the volume of domestic intelligence required varies based on the amount and type of deployed power. Governmental organizations can manage social policy successfully in many cases without the aid of intelligence. However, when hazards grow, or are seen to grow, preserving security may need the utilization of more and more intelligence in order to protect against such threats. In many of those cases, intelligence powers created for one reason may be utilized for others. For example, the government will undoubtedly use counterterrorism surveillance for law enforcement. Last but not least, technological advances might boost external and internal surveillance but also power holders' capacity to secure the nation. Therefore, these will undoubtedly increase the necessity and demand for enhanced domestic intelligence capabilities in the foreseeable future (Marrin, 2014).

New threats and new technology make it hard to figure out how the intelligence services can protect American security while staying true to American values. Finding the right balance has always been challenging. There was a Red Scare a century ago. Truman was worried about establishing an American Gestapo in the 1940s. The 1970s were marked by unlawful internal surveillance and covert assassination attempts against foreign leaders. Also, recent issues have arisen about the NSA's warrantless surveillance program. Notwithstanding all the worries about intelligence services being too powerful, Pearl Harbor, 9/11, and the Iraq WMD tragedy serve as a reminder that the opposite is also true: when intelligence organizations become too weak, horrible things may also occur (Zegart, 2022).

## Chapter V: Conclusions

“Our mission every day is to seek the truth, speak the truth.”

- Daniel Coats, director of National Intelligence, 2017–2019 (Thoennes, 2019)

People have talked about how the Snowden leaks show that some types of surveillance are information-heavy and often involve the Internet, while other types are more about "national security." In this context, the notion of "security" also needs to be reviewed, which is another challenge for research. Security is hard to explain, just like surveillance or privacy. This is especially true now, when national security has become a top priority for many countries. It's a controversial idea that's frequently mistakenly thought to clash with privacy and civil liberties. If the concept of security is to remain connected to the needs, goals, and welfare of people, far more multidimensional interpretations of it are necessary. These must be addressed in conjunction with the other issues raised by the "Snowden disclosures," namely privacy and surveillance (Lyon, 2015).

Obviously, Snowden believed that the publication of classified NSA documents was crucial, and he didn't want the story to end as Macbeth fears, as *"a tale told by an idiot, full of sound and fury, Signifying nothing."* That story hasn't been finished, and it's unclear whether the disclosures will impact US surveillance in the future. However, one instrumentally positive outcome stemming from Snowden's shocking criminal behavior was that the US can finally have the conversation about surveillance it should have had when these laws were created. Britain may do so too (Landau, 2013). Furthermore, it is unclear if the IC can win back American trust. Despite the fact that there aren't many public opinion surveys on intelligence, the ones that do exist indicate that the public is skeptical of intelligence while recognizing the importance of its goals (Roger Z., 2020). Thus, following Snowden, a 2019 Pew Research study found that most Americans think companies and the government monitor their online and offline activities. In particular, six-in-ten U.S. adults believe it is impossible to live without companies or the government collecting data on them (Auxier, et al., 2019).

In the long run, one thing that has happened over and over again in the history of American intelligence is the constant, intense conflict between secrecy and democracy. This is because the government needs to be strong enough to keep people safe while also being disciplined enough to protect people's rights. Concerns about NSA spying, data privacy, and counterterrorism have a long history. In that case, when President Truman did sign the National Security Act in 1947, he feared establishing an American Gestapo and demanded the new intelligence organization have no domestic intelligence-gathering or law enforcement powers (Zegart, 2022).

Over 150 years before, the Framers sought to balance democracy and security (Zegart., 2022). James Madison, the principal architect of the Constitution, was profoundly concerned about how to achieve harmony, going *"back and forth over the course of his long career... about how security should inflect the powers we invest in government,"* as Ritika Singh stated. *"In Madison's vacillations . . . we see fascinating prototypes of our own"* (Singh, 2013; Zegart., 2022). Finding a good balance between security risks and limits on individual freedom will always mean making hard choices and having difficult conversations. In dictatorships, intelligence agencies have full control over the power of the state. In democracies, intelligence services use the state's power according to the willingness of the people (Zegart, 2022). In summary, history has been creating a long shadow. The organizational abilities, difficulties, and controversies of today's intelligence agencies are based on the United States' founding debates, the nation's increasing position on the globe, and age-old coordination issues (Zegart., 2022).

## **Bibliography:**

113th Congress, 2013-2014. *CONGRESS.GOV*. [Online]

Available at: <https://www.congress.gov/bill/113th-congress/house-bill/3361>

[Accessed 19 1 2023].

Abdo, A., 2014. *American Civil Liberties Union*. [Online]

Available at: <https://www.aclu.org/news/national-security/new-documents-shed-light-one-nsas-most-powerful-tools>

[Accessed 16 11 2022].

Ackerman, S. & Ball, J., 2014. *The Guardian*. [Online]

Available at: <https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo>

[Accessed 4 1 2023].

Ackerman, S., 2014. *The Guardian*. [Online]

Available at: <https://www.theguardian.com/world/2014/jan/31/obama-admits-intelligence-chief-fault-senate-testimony>

[Accessed 30 1 2023].

ACLU, 2013. *ACLU*. [Online]

Available at:

[https://www.aclu.org/sites/default/files/field\\_document/usa\\_freedom\\_act\\_talking\\_points.pdf](https://www.aclu.org/sites/default/files/field_document/usa_freedom_act_talking_points.pdf)

[Accessed 19 1 2023].

ACLU, 2015. *American Civil Liberties Union*. [Online]

Available at: <https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program>

[Accessed 28 1 2023].

ACLU, 2021. *American Civil Liberties Union*. [Online]

Available at: <https://www.aclu.org/cases/aclu-v-united-states?redirect=cases/aclu-v-fbi-fisa-court-motions-requesting-public-access-rulings-nsa-bulk-surveillance>

[Accessed 19 1 2023].

ACLU, 2022. *American Civil Liberties Union*. [Online]

Available at: <https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance?redirect=time-rein-surveillance-state-0>

[Accessed 16 11 2022].

ACLU, n.d. *American Civil Liberties Union*. [Online]

Available at: <https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance?redirect=time-rein-surveillance-state-0>

[Accessed 19 1 2023].



Addicott, J. F., Hossain Bhuiyan, M. J. & Chowdhury, T. M., 2012. *Globalization, International Law, and Human Rights*. New Delhi: Oxford University Press.

Alati, D., 2015. Cowardly Traitor Or Heroic Whistleblower?: The Impact Of Edward Snowden's Disclosures On Canada And The United Kingdom's Security Establishments, Tennessee: Lincoln Memorial University Law Review.

Alati, D., 2015. Cowardly Traitor Or Heroic Whistleblower?: The Impact Of Edward Snowden's Disclosures On Canada And The United Kingdom's Security Establishments, Tennessee, USA: s.n.

Alhinnawi, B. et al., 2015. The Snowden Revelations And Their Effects On European It-Related Decisions And Decisionmaking, Tilburg, The Netherlands: Tilburg University.

All Things Considered, 2015. *NPR*. [Online]  
Available at: <https://www.npr.org/2015/03/02/390245038/ben-franklins-famous-liberty-safety-quote-lost-its-context-in-21st-century>  
[Accessed 19 1 2023].

American Civil Liberties Union, n.d. *ACLU*. [Online]  
Available at: <https://www.aclu.org/other/foreign-intelligence-surveillance-act-news-and-resources>  
[Accessed 3 11 2022].

American Civil Liberties Union, n.d. *ACLU*. [Online]  
Available at: <https://www.aclu.org/why-fisa-amendments-act-unconstitutional>  
[Accessed 3 11 2022].

American Civil Liberties Union, n.d. *ACLU*. [Online]  
Available at: <https://www.aclu.org/about/aclu-history>  
[Accessed 3 11 2022].

American Library Association, 2014. *American Library Association*. [Online]  
Available at: <https://www.ala.org/awardsgrants/president-barack-obama%E2%80%99s-review-group-intelligence-and-communications-technologies>  
[Accessed 19 1 2023].

Amnesty International UK, 2020. *Amnesty International UK*. [Online]  
Available at: <https://www.amnesty.org.uk/edward-snowden-nsa-whistleblower-pardon>  
[Accessed 3 1 2023].

Amnesty International, 2015. *Amnesty International*. [Online]  
Available at: <https://www.amnesty.org/en/latest/campaigns/2015/06/7-ways-the-world-has-changed-thanks-to-edward-snowden/>  
[Accessed 22 1 2023].

Andrew Blake The Washington Times, 2019. *AP NEWS*. [Online]  
Available at: <https://apnews.com/article/business-33a88feb083ea35515de3c73e3d854ad>  
[Accessed 28 1 2023].

Andrew, C., Aldrich, R. J. & Wark, W. K. eds., 2020. *Secret Intelligence: A Reader*. 2nd ed. Oxon UK, NY USA: Routledge.

Andrews, S., Burrough, B. & Ellison, S., 2014. *Vanity Fair*. [Online]  
Available at: <https://archive.vanityfair.com/article/2014/5/the-snowden-saga>  
[Accessed 8 12 2022].

Anon., 2014. Strategic Policy Issues. *Strategic Survey*, 17 9, Volume 114, pp. 32-33.

Anon., 2016. *American Academy of Arts and Sciences*. [Online]  
Available at: <https://www.amacad.org/daedalus/internet>  
[Accessed 21 11 2022].

Ariel, E.-L. & Freeman, S., 2013. *Huffpost*. [Online]  
Available at: [https://www.huffpost.com/entry/edward-snowden-poll\\_n\\_4175089](https://www.huffpost.com/entry/edward-snowden-poll_n_4175089)  
[Accessed 18 1 2023].

Associated Press, 2013. *POLITICO*. [Online]  
Available at: <https://www.politico.com/story/2013/08/edward-snowden-timeline-of-events-095057>  
[Accessed 16 12 2022].

Atkins, E., 2014. Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?. *Washington Journal of Law, Technology & Arts*, 7 1, pp. 77-78.

Atkins, E., 2014. Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?. *Washington Journal of Law, Technology & Arts*, 1 7, pp. 62, 82.

Atkins, E., 2014. Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?. *Washington Journal of Law, Technology & Arts*, 1 7, Volume 10, pp. 87-88.

Atkins, E., 2014. Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?. *Washington Journal of Law, Technology & Arts*, 1 7, Volume 10, pp. 71-88.

Auxier, B. et al., 2019. *Pew Research Center*. [Online]  
Available at: <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>  
[Accessed 8 2 2023].

- Ball, J., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>  
[Accessed 4 1 2023].
- Ball, J. & Ackerman, S., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/2013/aug/09/nsa-loop-hole-warrantless-searches-email-calls>  
[Accessed 4 1 2023].
- Ball, J., Borger, J. & Greenwald, G., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>  
[Accessed 4 1 2023].
- Bamford, J., 2014. *Wired*. [Online]  
Available at: <https://www.wired.com/2014/08/edward-snowden/>  
[Accessed 8 12 2022].
- Barak, G., ed., 1991. 'Old wine, new bottles and fancy labels'. In: *Crimes by the Capitalist State: An Introduction to State Criminality*. New Brunswick USA: Rutgers University Press, p. 185–217.
- Barnes, J. E., 2022. *What Is the Espionage Act and How Has It Been Used?*. [Online]  
Available at: <https://www.nytimes.com/2022/08/15/us/politics/espionage-act-explainer-trump.html>  
[Accessed 3 11 2022].
- Bauman, Z. et al., 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, pp. 120-144, 121.
- BBC News, 2013. *BBC News*. [Online]  
Available at: <https://www.bbc.com/news/world-us-canada-23768248>  
[Accessed 16 12 2022].
- Beeman, R., 2010. *The Penguin guide to the United States Constitution : a fully annotated Declaration of Independence, U.S. Constitution and amendments, and selections from the Federalist Papers*. New York: Penguin Books.
- Begley, J. & Scahill, J., 2015. *The Intercept*. [Online]  
Available at: <https://theintercept.com/2015/02/19/great-sim-heist/>  
[Accessed 18 1 2023].
- Bellaby, R., 2012. What's the Harm? The Ethics of Intelligence Collection. *Intelligence and National Security*, 24 2, Volume 27, p. 103.

- Bellaby, R., 2012. What's the Harm? The Ethics of Intelligence Collection. *Intelligence and National Security*, 24 2, Volume 27, pp. 96, 109-117.
- Bellaby, R., 2017. The Ethics of Intelligence. Στο: R. Dover, H. Dylan & M. S. Goodman, επιμ. *The Palgrave Handbook of Security Risk and Intelligence*. London, UK: Springer Nature, p. 395.
- Bellaby, R. W., 2018. Too many secrets? When should the intelligence community be allowed to keep secrets?. *University of Chicago Press Journal*, p. 14.
- Biermann, K., 2015. *ZEIT ONLINE*. [Online]  
Available at: <https://www.zeit.de/digital/datenschutz/2015-02/bnd-nsa-mass-surveillance>  
[Accessed 4 1 2023].
- Bill of Rights Institute, 2022. *Bill of Rights Institute*. [Online]  
Available at: [https://billofrights.org/resources/principles-and-virtues?gclid=EAIaIQobChMI3KePpZTx7QIVA5SGCh0MNQ3REAAYASAAEglwQfD\\_BwE](https://billofrights.org/resources/principles-and-virtues?gclid=EAIaIQobChMI3KePpZTx7QIVA5SGCh0MNQ3REAAYASAAEglwQfD_BwE)  
[Accessed 21 10 2022].
- Boadle, A. & Soto, A., 2013. *Reuters*. [Online]  
Available at: <https://www.reuters.com/article/uk-usa-brazil-jets-idUKBRE97BORD20130812>  
[Accessed 22 1 2023].
- Bomboy, S., 2022. *The Espionage Act's constitutional legacy*. [Online]  
Available at: <https://constitutioncenter.org/blog/the-espionage-acts-constitutional-legacy>  
[Accessed 3 11 2022].
- Boraz, S. C., 2007. Executive Privilege: Intelligence Oversight in the United States. In: T. C. Bruneau & S. C. Boraz, eds. *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*. Texas USA: University of Texas Press, pp. 29-37.
- Born, H. & Caparini, M. eds., 2007. *Democratic Control of Intelligence Services Containing Rogue Elephants*. 1 ed. Hampshire UK, Burlington USA: Ashgate Publishing Limited, Ashgate Publishing Company.
- Born, H. & Jensen, F., 2007. Intelligence Services: Strengthening Democratic Accountability. In: H. BORN & M. CAPARINI, eds. *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Burlington, USA: Ashgate Publishing Company, pp. 257-270.
- BORN, H., JOHNSON, L. K. & LEIGH, I. eds., 2005. *Who's Watching the Spies : Establishing Intelligence Service Accountability*. 1 ed. Washington, D.C.: Potomac Books, Inc..
- Brandom, R., 2014. *The Verge*. [Online]  
Available at: <https://www.theverge.com/2014/1/27/5350714/new-nsa-documents-reveal-massive-data-collection-from-mobile-apps>  
[Accessed 4 1 2023].

- Breslow, J. M., 2014. *PBS*. [Online]  
Available at: <https://www.pbs.org/wgbh/frontline/article/obama-on-mass-government-surveillance-then-and-now/>  
[Accessed 19 1 2023].
- Bruneau, T. C. & Dombroski, K. R., n.d. *Reforming Intelligence: The Challenge Of Control In New Democracies*, s.l.: s.n.
- bruneau, t. c. & florina matei, c. (., 2010. Intelligence In The Developing Democracies: The Quest For Transparency And Effectiveness. In: L. K. Johnson, ed. *The Oxford Handbook of National Security Intelligence*. 1 ed. New York USA: Oxford University Press.
- Budiansky, S., 2017. *The Wall Streer Journal*. [Online]  
Available at: <https://www.wsj.com/articles/edward-snowdens-real-motive-1484611115>  
[Accessed 21 1 2023].
- Bump, P., 2022. *The Washington Post*. [Online]  
Available at: <https://archive.ph/tjAAF>  
[Accessed 3 11 2022].
- Cain Miller, C., 2014. *The New York Times*. [Online]  
Available at: [https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?\\_r=0](https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0).  
[Accessed 25 2 2023].
- Caparini, M., 2007. Controlling and Overseeing Intelligence. In: H. BORN & M. CAPARINI, eds. *DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES: Containing Rogue Elephants*. Burlington, USA: Ashgate Publishing Company, pp. 3-24.
- Caparini, M., 2007. Controlling and Overseeing Intelligence Services in Democratic States. In: H. BORN & M. CAPARINI, eds. *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Burlington, USA: Ashgate Publishing Company, p. 3.
- Casto, W. R., n.d. IF MEN WERE ANGELS. *Harvard Journal of Law & Public Policy*, Volume 35, p. 663.
- Chan, J., 2013. *World Socialist Web Site*. [Online]  
Available at: <https://www.wsws.org/en/articles/2013/06/14/hong-i14.html>  
[Accessed 4 1 2023].
- Childress, S., 2015. *PBS*. [Online]  
Available at: <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/>  
[Accessed 19 1 2023].

- Čirjak, A., 2020. *WorldAtlas*. [Online]  
Available at: <https://www.worldatlas.com/articles/5-important-elements-of-the-us-political-system.html>  
[Accessed 21 10 2022].
- Clapper, Jr., J. R., 2010. The Role Of Defense In Shaping U.S. Intelligence Reform. In: L. K. Johnson, ed. *The Oxford handbook of national security intelligence*. Oxford, UK: Oxford University Press, Inc., p. 637.
- Clarke, R. A. et al., 2014. *The NSA Report - Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*. New Jersey, USA: Princeton University Press.
- Coats, D. R., 2019. *Office of the Director of National Intelligence*. [Online]  
Available at: <https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy>  
[Accessed 3 11 2022].
- Cohen, J., 2012. Democracy and Liberty. In: J. Elster, ed. *Deliberative Democracy*. Cambridge UK: Cambridge University Press, pp. 185 - 231.
- Collins, n.d. *Collins English Dictionary*. [Online]  
Available at: <https://www.collinsdictionary.com/dictionary/english/ethics>  
[Accessed 6 2 2023].
- Condon, S., 2014. *CBS News*. [Online]  
Available at: <https://www.cbsnews.com/news/obamas-nsa-changes-raise-more-questions-than-answers/>  
[Accessed 19 1 2023].
- Congress.gov, 2020. *Constitution Annotated: Analysis and Interpretation*. [Online]  
Available at: <https://constitution.congress.gov/constitution/amendment-4/>  
[Accessed 22 10 2022].
- Congressional Research Service, 2021. *Congressional Research Service*. [Online]  
Available at: <https://crsreports.congress.gov/product/pdf/R/R40138>  
[Accessed 3 11 2022].
- Constitutional Rights Foundation, 2016. *Constitutional Rights Foundation*. [Online]  
Available at: [https://www.crf-usa.org/images/pdf/gates/snowden\\_nsa.pdf](https://www.crf-usa.org/images/pdf/gates/snowden_nsa.pdf)  
[Accessed 22 1 2023].
- Contorno, S., 2014. *Politifact*. [Online]  
Available at: <https://www.politifact.com/article/2014/mar/11/james-clappers-testimony-one-year-later/>  
[Accessed 28 1 2023].

- Davies, D., 2019. *NPR*. [Online]  
Available at: <https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia>  
[Accessed 16 12 2022].
- DeRosa, M. B., 2022. Congressional oversight of US intelligence activities. In: S. Miller, M. Regan & P. F. Walsh, eds. *National Security Intelligence and Ethics*. New York: Routledge, p. 216.
- DeRosa, M. B., 2022. Congressional oversight of US intelligence activities. In: S. Miller, M. Regan & P. F. Walsh, eds. *National Security Intelligence and Ethics*. NY USA: Routledge, p. 219.
- Dover, R., Dylan, H. & Goodman, M. S., 2017. *The Palgrave Handbook of Security Risk and Intelligence*. 1 ed. London, UK: Macmillan Publishers Ltd..
- EFF, n.d. *Electronic Frontier Foundation*. [Online]  
Available at: <https://www.eff.org/nsa-spying>  
[Accessed 19 1 2023].
- Eset, 2014. *Welivesecurity by ESET*. [Online]  
Available at: <https://www.welivesecurity.com/2014/11/17/privacy-security-post-snowden-pew-research-confirms-eset-findings/>  
[Accessed 13 4 2023].
- Ethics Unwrapped, n.d. *Ethics Unwrapped*. [Online]  
Available at: <https://ethicsunwrapped.utexas.edu/case-study/edward-snowden-traitor-hero>  
[Accessed 19 1 2023].
- Etzioni, A., 2014. NSA: National Security vs. Individual Rights. *Intelligence and National Security*, 24 1, Volume 30, pp. 100-101.
- Etzioni, A., 2014. NSA: National Security vs. Individual Rights. *Intelligence and National Security*, 24 1, p. 119.
- Etzioni, A., 2014. NSA: National Security vs. Individual Rights. *Intelligence and National Security*, 24 1, p. 111.
- Etzioni, A., 2014. NSA: National Security vs. Individual Rights. *Intelligence and National Security*, 30(1), p. 100.
- Fahrenheit, D. A., 2013. *The Washington Post*. [Online]  
Available at: [https://www.washingtonpost.com/politics/after-years-of-obscure-warnings-wyden-gets-sought-after-privacy-debate-in-wake-of-nsa-revelations/2013/07/28/267efd1a-f573-11e2-861b-70461cc1cd24\\_story.html](https://www.washingtonpost.com/politics/after-years-of-obscure-warnings-wyden-gets-sought-after-privacy-debate-in-wake-of-nsa-revelations/2013/07/28/267efd1a-f573-11e2-861b-70461cc1cd24_story.html)  
[Accessed 30 1 2023].

Franklin, B., 2021. *ycombinator*. [Online]

Available at: <https://news.ycombinator.com/item?id=27875223>

[Accessed 30 1 2022].

Freeman, M., 2011. *Human Rights: An Interdisciplinary Approach*. 2nd ed. UK: Polity Press.

FT.COM, 2014. *Financial Times*. [Online]

Available at: <https://www.ft.com/content/9f45bcb2-a616-11e3-8a2a-00144feab7de>

[Accessed 5 1 2023].

Gallagher, R., 2014. *How Secret Partners Expand Nsa's Surveillance Dragnet*. [Online]

Available at: <https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>

[Accessed 24 11 2022].

Gallagher, R., 2014. *The Intercept*. [Online]

Available at: <https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/>

[Accessed 5 1 2023].

Gallagher, R., 2014. *The Intercept*. [Online]

Available at: <https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>

[Accessed 5 1 2023].

Gallagher, R. & Greenwald, G., 2015. *The Intercept*. [Online]

Available at: <https://theintercept.com/2015/01/28/canada-cse-levitation-mass-surveillance/>

[Accessed 4 1 2023].

Gardner, L. C., 2016. *The War on Leakers: National Security and American Democracy from Eugene V. Debs to Edward Snowden*. 1 ed. NY, USA: The New Press.

Gass, N., 2016. *POLITICO*. [Online]

Available at: <https://www.politico.com/story/2016/05/white-house-obama-edward-snowden-223742>

[Accessed 18 1 2023].

Gellman, B. & Soltani, A., 2013. *The Washington Post*. [Online]

Available at: [https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html)

[Accessed 5 1 2023].

Gellman, B. & Poitras, L., 2013. *The Washington Post*. [Online]

Available at: <https://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

[Accessed 4 1 2023].

Gellman, B. & Soltani, A., 2013. *The Washington Post*. [Online]

Available at: [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](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)

[Accessed 5 1 2023].

Gellman, B. & Soltani, A., 2014. *The Washington Post*. [Online]

Available at: [https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html)

[Accessed 5 1 2023].

Gentleman, A. & Hopkins, N., 2014. *The Guardian*. [Online]

Available at: <https://www.theguardian.com/world/2014/apr/17/putin-edward-snowden-russia-mass-surveillance>

[Accessed 22 1 2023].

George, R. Z., 2020. *Intelligence in the National Security Enterprise : An Introduction*.

Georgetown, USA: Georgetown University Press.

Gidda, M., 2013. *The Guardian*. [Online]

Available at: <https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>

[Accessed 16 12 2022].

Gill, P., 2009. Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'?

*Intelligence and National Security*, 1 2, Volume 24, p. 78.

Gill, P., 2012. Intelligence, Threat, Risk and the Challenge of Oversight. *Intelligence and National Security*, 27 4, pp. 206-222.

Gill, P. & Phythian, M., 2018. *Intelligence in an Insecure World*. 3rd Edition ed. Medford, MA

02155, USA: Polity Press.

Government Accountability Project, 2013. *Government Accountability Project*. [Online]

Available at: <https://whistleblower.org/snowden-timeline/>

[Accessed 3 1 2023].

Greene, D., 2015. *Electronic Frontier Foundation*. [Online]

Available at: <https://www.eff.org/el/deeplinks/2015/05/aclu-v-clapper-and-congress-how-second-circuits-decision-affects-legislative>

[Accessed 28 1 2023].

Greenslade, R., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/2013/aug/19/edward-snowden-nsa-secrets-glenn-greenwald-laura-poitras>  
[Accessed 8 12 2022].

Greenwald, G., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>  
[Accessed 3 1 2023].

Greenwald, G. & MacAskill, E., 2013. *The Guardian*. [Online]  
Available at: [2023](#)  
[Accessed 4 1 2023].

Greenwald, G. & MacAskill, E., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>  
[Accessed 4 1 2023].

Grill, P. & Phythian, M., 2018. *Intelligence in an Insecure World*. 3rd ed. Cambridge UK, Medford USA: Polity Press.

Groll, E., 2013. *Foreign Policy*. [Online]  
Available at: <https://foreignpolicy.com/2013/12/19/boeing-just-lost-a-huge-defense-contract-thanks-to-ed-snowden/>  
[Accessed 23 1 2023].

Guitar, J. L., 2018. *Snowden Is (Not) A Whistleblower: An Analysis Of Ideographs And Anti-Democratic Rhetorical Strategies Within The U.S. Government's Response To Edward Snowden*, Detroit, Michigan, Usa: Joshua L. Guitar.

Haggerty, K. D. & Samatas, M., 2010. Surveillance and Democracy: An Unsettled Relationship. In: *Surveillance and Democracy*. New York, USA: Routledge-Cavendish, p. 272.

Harding, L., 2014. *The Snowden Files: The Inside Story of the World's most Wanted Man*. 1 ed. Great Britain: Guardian Books, London, and Faber and Faber Ltd., London.

Harvard University, n.d. *Harvard.edu*. [Online]  
Available at: [https://scholar.harvard.edu/files/marciasoviak/files/law\\_ppr\\_cloud\\_computing\\_chicago\\_style\\_1.docx](https://scholar.harvard.edu/files/marciasoviak/files/law_ppr_cloud_computing_chicago_style_1.docx)  
[Accessed 13 4 2023].

Hastedt, G. P., 1991. *Controlling Intelligence*. 1 ed. Great Britain, New York USA: Frank Cass & Co. Ltd..

Hennessey, K. & Bevins, V., 2013. *Los Angeles Times*. [Online]  
Available at: <https://www.latimes.com/world/la-xpm-2013-sep-17-la-fg-snowden-fallout->

[20130918-story.html](#)

[Accessed 23 1 2023].

Herb, J. & Sink, J., 2013. *THE HILL*. [Online]

Available at: <https://thehill.com/policy/defense/152964-sen-feinstein-calls-snowdens-nsa-leaks-an-act-of-treason/>

[Accessed 4 1 2023].

Hopkins, N., 2013. *The Guardian*. [Online]

Available at: <https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>

[Accessed 4 1 2023].

Inkster, N., 2014. The Snowden Revelations: Myths and Misapprehensions. *Survival: Global Politics and Strategy*, 12 2, p. 52.

Inkster, N., 2014. The Snowden Revelations: Myths and Misapprehensions. *Survival: Global Politics and Strategy*, 15 3, pp. 51-60.

Jaffer, J., 2015. *American Civil Liberties Union*. [Online]

Available at: <https://www.aclu.org/news/national-security/what-aclu-v-clapper-means>

[Accessed 28 1 2023].

Jaycox, M., 2014. *EFF*. [Online]

Available at: <https://www.eff.org/el/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet>

[Accessed 16 11 2022].

Jensen III, C. J., McElreath, D. H. & Graves, M., 2018. *Introduction to Intelligence Studies*. 2nd ed. New York, USA: Routledge, p. 264, 266.

Jensen III, C. J., McElreath, D. H. & Graves, M., 2013. *Introduction to Intelligence Studies*. 2nd ed. New York, USA: Routledge, p. 84

[Accessed 28 07 2023].

Johnson, L. K., 1989. *America's Secret Power The CIA in a Democratic Society*. 1st εκμ. Oxford USA: Oxford University Press, Inc.

Johnson, L. K., 2002. *Bombs, bugs, drugs, and thugs : intelligence and America's quest for security*. 1 ed. New York, USA: New York University Press.

Johnson, L. K., 2008. Establishment of modern intelligence accountability. In: R. A. Miller, ed. *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror*. New York, USA: Routledge, p. 45.

Johnson, L. K., 2015. *issforum*. [Online]

Available at: <https://issforum.org/forums/ins-snowden>

[Accessed 12 2023].

Johnson, L. K. et al., 2014. An INS Special Forum: Implications of the Snowden Leaks. In: *Intelligence and National Security*. s.l.:s.n., pp. 793-810.

Johnson, L. K. et al., 2014. An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security*, 8 8, Volume 29, pp. 794-795.

Johnson, L. K. et al., 2014. INS Special Forum: Implications of the Snowden Leaks. *National Security Intelligence and National Security*, 8 8, pp. 802-803.

Kaiser, F. M., 2010. Congressional Oversight of Intelligence: Current Structure and Alternatives. In: P. R. Haas, ed. *Intelligence Oversight And Disclosure Issues*. NY USA: Nova Science Publishers, Inc., p. 1.

Kaiser, F. M., 2010. Protection Of Classified Information By Congress: Practices And Proposals. In: P. R. Haas, ed. *Intelligence Oversight And Disclosure Issues*. New York, USA: Nova Science Publishers, Inc., p. 111.

Keefe, E. O., 2013. *The Washington Post*. [Online]

Available at: <https://www.washingtonpost.com/news/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/>

[Accessed 17 11 2022].

Kelemen, M., 2013. *npr*. [Online]

Available at: <https://www.npr.org/2013/08/04/208796058/snowden-case-illustrates-decline-in-u-s-russia-relations>

[Accessed 22 1 2023].

Kelion, L., 2013. *BBC*. [Online]

Available at: <https://www.bbc.com/news/technology-23051248>

[Accessed 5 1 2023].

Kibbe, J., 2010. Congressional Oversight of Intelligence: Is the Solution Part of the Problem?. *Intelligence and National Security*, 10 3, Volume 1, pp. 24-49, 27.

Konstantopoulos, I. L., 2017. Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden. In: G. C. Bitros & N. C. Kyriazis, eds. *Democracy and an Open-Economy World Order*. Athens, Greece: Springer International Publishing, p. 15.

Konstantopoulos, I. L., 2017. Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden. Στο: G. C. Bitros & N. C. Kyriazis, eds. *Democracy and an Open-Economy World Order*. Athens, Greece: Springer International Publishing, pp. 16, 17.

Konstantopoulos, I. L., 2017. Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden. In: G. C. Bitros & N. C. Kyriazis, eds. *Democracy and an Open-Economy World Order*. Athens, Greece: Springer International Publishing, p. 16.

Konstantopoulos, I. L., 2017. Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden. In: G. C. Bitros & N. C. Kyriazis, eds. *Democracy and Ethics vs. Intelligence*. Athens, Greece: Springer International Publishing, p. 4.

Kratz, J., 2017. *National Archives: Pieces of History*. [Online]  
Available at: <https://prologue.blogs.archives.gov/2017/06/15/defining-a-spy-the-espionage-act/>  
[Accessed 3 11 2022].

Landau, S., 2013. *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, s.l.: IEEE Computer and Reliability Societies.

Lands, C., 2017. *Academia.edu*. [Online]  
Available at:  
[https://www.academia.edu/39876754/How the Revelations of Edward Snowden Impacted the US Government and the Intelligence Community](https://www.academia.edu/39876754/How_the_Revelations_of_Edward_Snowden_Impacted_the_US_Government_and_the_Intelligence_Community)  
[Accessed 1 2 2023].

Laperrugue, J., 2019. *POGO*. [Online]  
Available at: <https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance>  
[Accessed 4 1 2023].

Lashmar, P., 2018. From Silence to Primary Definer: The Emergence of an Intelligence Lobby in the Public Sphere.. *SAGE Journals*, 48(3), pp. 411 - 430.

Lawne, R., n.d. *Fieldfisher*. [Online]  
Available at: <https://www.fieldfisher.com/en/insights/us-surveillance-s702-fisa-eo-12333-prism-and-ups>  
[Accessed 18 11 2022].

Leary , A., 2014. *Tampa Bay Times*. [Online]  
Available at: <https://www.tampabay.com/rubio-says-hes-concerned-about-obamas-nsa-reforms/2161569/>  
[Accessed 19 1 2023].

Lee, T. B., 2013. *The Washington Post*. [Online]  
Available at: <https://www.washingtonpost.com/news/the-switch/wp/2013/08/02/sen-obama-warned-about-patriot-act-abuses-president-obama-proved-him-right/>  
[Accessed 18 1 2023].

Legal Information Institute, n.d. *Cornell Law School*. [Online]  
Available at: [https://www.law.cornell.edu/wex/search\\_warrant](https://www.law.cornell.edu/wex/search_warrant)  
[Accessed 30 1 2023].

Lowenthal, M. M., 2020. *Intelligence From Secrets to Policy*. 8th ed. California USA, London UK: CQ Press, an Imprint of SAGE Publications,.

Lyon, D., 2015. *Academia.edu*. [Online]  
Available at:  
[https://www.academia.edu/51762302/The\\_Snowden\\_Stakes\\_Challenges\\_for\\_Understanding\\_Surveillance\\_Today](https://www.academia.edu/51762302/The_Snowden_Stakes_Challenges_for_Understanding_Surveillance_Today)  
[Accessed 2023 2 28].

MacAskill, E. et al., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>  
[Accessed 4 1 2023].

MacAskill, E. & Dance, G., 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>  
[Accessed 8 12 2022].

Madhani, A. & Jackson, D., n.d. *USA TODAY*. [Online]  
Available at: <https://eu.usatoday.com/story/news/politics/2013/08/09/obama-news-conference/2636191/>  
[Accessed 22 1 2023].

Madison, J., 1788. *Federalist No. 51*, New York, USA: J. & A. McLean.

Marcon, A. R., 2015. *The Discursive Enactment of Edward Snowden*, Ottawa, Canada: Alessandro R. Marcon, Carleton University.

Marks, J., 2021. *American Bar Association*. [Online]  
Available at: <https://www.americanbar.org/groups/crsj/publications/crsj-featured-articles/espionage-act-reform-bill/>  
[Accessed 3 11 2022].

Marrin, 2017. *How the Revelations of Edward Snowden Impacted the US Government and the Intelligence Community*, TX, USA: s.n.

Marrin, S., 2014. Systems of intelligence: The United States. In: R. Dover, M. S. Goodman & C. Hillebrand, eds. *Routledge Companion to Intelligence Studies*. New York, USA: Routledge, p. 153.

- McCarthy, J., 2016. *Global Citizen*. [Online]  
Available at: <https://www.globalcitizen.org/en/content/human-rights-groups-want-edward-snowden-pardoned/>  
[Accessed 19 1 2023].
- McConell, J. M., 2015. *VISION 2015: A Globally Networked and Integrated Intelligence Enterprise*, Washington, DC: Director Of National Intelligence.
- McCubbins, M. D. & Schwartz, T., 1984. Congressional Oversight Overlooked: Police Patrols versus Fire Alarms. *American Journal of Political Science*, 2, Volume 28, pp. 165-179.
- McDermott, P., 2018. Secrets and Lies — Exposed and Combatted: Warrantless Surveillance Under and Around the Law 2001-2017. *Secrecy and Society*, 2, Volume 2, p. 23.
- McDermott, P., 2018. Secrets and Lies — Exposed and Combatted: Warrantless Surveillance Under and Around the Law 2001-2017. *Secrecy and Society*, 9, Volume 2, p. 53.
- McParland, K., 2013. *National Post*. [Online]  
Available at: <https://nationalpost.com/opinion/kelly-mcparland-edward-snowden-stands-by-his-right-to-betray-without-being-pursued>  
[Accessed 3 1 2023].
- microfocus, n.d. *microfocus*. [Online]  
Available at: <https://www.microfocus.com/en-us/what-is/open-source-intelligence-osint>  
[Accessed 16 2 2023].
- Mill, S. J., 1861. In: *Considerations on Representative Government*. London, UK: Cambridge University Press, p. 84.
- Miller, R. A. ed., 2008. *US National Security, Intelligence and Democracy From the Church Committee to the*. 1 ed. New York USA: Routledge.
- Miller, S., 2017. The Ethics of Whistleblowing, Leaking and Disclosure. In: R. Dover, H. Dylan & M. S. Goodman, eds. *The Palgrave Handbook of Security Risk and Intelligence*. London, UK: Springer Nature, p. 479.
- Mirfattahi, M., 2019. *Once Silence is Broken: The Transparency Discourse of the NSA and CIA*, Leiden, The Netherlands: Leiden University.
- Monteiro, R. L., 2014. *the balance between freedom and security in the age of surveillance. a brief analysis of the recent intelligent electronic surveillance scandals.*, Singapore, New York: National University of Singapore Law School.
- Moon, M. E., 2017. *How America Lost its Secrets: Edward Snowden, The Man and The Theft. By E The Theft. By Edward Jay Epstein. New Y y Epstein. New York, N.York, N.Y.; Alfr .; Alfred A. K ed A. Knopf, 2017.*, South Florida, USA: Journal of Strategic Security.

Moon, M. E., 2017. *How America Lost its Secrets: Edward Snowden, The Man and The Theft*. By Edward Jay Epstein. New York, N.Y.; Alfred A. Knopf, 2017., South Florida, USA: Journal of Strategic Security.

Mullin, J., 2013. *arsTECHNICA*. [Online]

Available at: <https://arstechnica.com/tech-policy/2013/06/nsa-leaker-ed-snowdens-life-on-ars-technica/>

[Accessed 8 12 2022].

N.S.A., 2013. *Wikimedia Commons*. [Online]

Available at: [https://commons.wikimedia.org/wiki/File:PRISM\\_Collection\\_Details.jpg](https://commons.wikimedia.org/wiki/File:PRISM_Collection_Details.jpg)

[Accessed 4 1 2023].

NBC News, 2014. *NBC News*. [Online]

Available at: <https://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871>

[Accessed 16 12 2022].

Nicoll, A. & Delaney, J. eds., 2014. Obama's limited response on NSA surveillance. *Strategic Comments*, 1, 19(10), p. 2.

Nicoll, A. & Delaney, J. eds., 2014. Obama's limited response on NSA surveillance. *Strategic Comments*, 1, 19(10), p. 3.

Obama, B., 2005. *Obama Speeches*. [Online]

Available at: <http://obamaspeeches.com/041-The-PATRIOT-Act-Obama-Speech.htm>

[Accessed 19 1 2023].

Obama, B., 2013. *The Bill of Rights Institute*. [Online]

Available at: <https://billofrightsinstitute.org/activities/handout-d-president-barack-obama-press-conference-august-9-2013>

[Accessed 30 1 2023].

Obama, B., 2014. *President Obama's Full NSA Speech* [Interview] 2014.

Office of the Press Secretary, 2008. *The White House*. [Online]

Available at: <https://georgewbush-whitehouse.archives.gov/news/releases/2008/07/20080731-2.html>

[Accessed 16 11 2022].

Olesen, M., n.d. *The Snowden Disclosures: Balancing Security and Privacy in a Panoptic Society*, Aalborg, Denmark: Aalborg University.

Omand, D. & Phythian, M., 2018. *Principled Spying - The Ethics Of Secret Intelligence*. 1 ed. Oxford UK: Oxford University Press.



Omand, S. D. & Phythian, M., 2012. Ethics and Intelligence: A Debate. *International Journal of Intelligence and CounterIntelligence*, 30 11, pp. 38-63, 55.

Ott, M. C., 2003. Partisanship and the Decline of Intelligence Oversight. *International Journal of Intelligence and CounterIntelligence*, 1 3, pp. 69-94.

OTT, M. C., 2003. Partisanship and the Decline of Intelligence Oversight. *International Journal of Intelligence and CounterIntelligence*, pp. 73-76.

Perloth, N., Larson, J. & Shane, S., 2013. *The New York Times*. [Online]  
Available at: [http://home.etf.rs/~proka/CRYPTO/NSA\\_NY\\_Times.pdf](http://home.etf.rs/~proka/CRYPTO/NSA_NY_Times.pdf)  
[Accessed 4 1 2023].

Poitras, L., Rosenbach, M. & Stark, H., 2013. *SPIEGEL International*. [Online]  
Available at: <https://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html>  
[Accessed 4 1 2023].

Poitras, L., Rosenbach, M. & Stark, H., 2013. *SPIEGEL International*. [Online]  
Available at: <https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html>  
[Accessed 4 1 2023].

Price, J., n.d. *Academia*. [Online]  
Available at:  
[https://www.academia.edu/29871255/Recasting\\_a\\_Hero\\_The\\_Obama\\_Administration\\_s\\_Rhetorical\\_de\\_construction\\_of\\_Edward\\_Snowden](https://www.academia.edu/29871255/Recasting_a_Hero_The_Obama_Administration_s_Rhetorical_de_construction_of_Edward_Snowden)  
[Accessed 18 1 2023].

Price, J., n.d. *Academia*. [Online]  
Available at:  
[https://www.academia.edu/29871255/Recasting\\_a\\_Hero\\_The\\_Obama\\_Administration\\_s\\_Rhetorical\\_de\\_construction\\_of\\_Edward\\_Snowden](https://www.academia.edu/29871255/Recasting_a_Hero_The_Obama_Administration_s_Rhetorical_de_construction_of_Edward_Snowden)  
[Accessed 12 4 2023].

Puntambekar, A., n.d. *Academia*. [Online]  
Available at: [https://www.academia.edu/32709839/Edward\\_Snowden\\_Hero\\_or\\_Traitor\\_pdf](https://www.academia.edu/32709839/Edward_Snowden_Hero_or_Traitor_pdf)  
[Accessed 19 1 2023].

Ray, M., 2022. *Britannica*. [Online]  
Available at: <https://www.britannica.com/biography/Denzel-Washington>  
[Accessed 3 1 2023].

Reilly, M., 2013. *Huffpost*. [Online]  
Available at: [https://www.huffpost.com/entry/obama-nsa-surveillance\\_n\\_3455771](https://www.huffpost.com/entry/obama-nsa-surveillance_n_3455771)  
[Accessed 18 1 2023].

Reuters Staff, 2013. *Reuters*. [Online]

Available at: <https://www.reuters.com/article/us-russia-snowden-timeline-idUSBRE9700TT20130801>

[Accessed 3 1 2023].

Richardson, M., 2016. Surveillance Publics After Edward Snowden. In: *Contemporary Publics*. UK: s.n., pp. 164-165.

Rinehart, L. C., 2014. Clapper v. Amnesty International USA: Allowing the FISA Amendments Act of 2008 to Turn "Incidentally" into "Certainly". *Maryland Law Review*, Volume 73, pp. 1047-1048.

Roger Z., G., 2020. *Intelligence in the National Security Enterprise : An Introduction*. Washington, DC, USA: Georgetown University Press.

Roger, G., 2020. Intelligence and American Democracy. In: *Intelligence in the National Security Enterprise : An Introduction*. Georgetown: Georgetown University Press, pp. 265-266.

Roger, G. Z., 2020. *Intelligence in the National Security Enterprise : An Introduction*. Washington, DC: Georgetown University Press.

Rosenbach, E. & Peritz, A. J., 2009. *Confrontation or Collaboration? Congress and the Intelligence Community*, Cambridge USA: Harvard University.

Roy, K., 2018. *Media Discourse of the Right to Privacy under Surveillance: An analysis of the media coverage from post-9/11 to post-Snowden US*, s.l.: Kuntal Roy.

Roy, K., 2018. *Media Discourse of the Right to Privacy under Surveillance: An analysis of the media coverage from post-9/11 to post-Snowden US*, London, Bilbao, Gothenburg: University of Deusto, University of Gothenburg, University of Roehampton.

Rubinstein, I. & Hoboken, J. V., 2014. *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, New York: New York University School Of Law.

Russel, M., 2013. *Marotta On Money*. [Online]

Available at: <https://www.marottaonmoney.com/edward-snowdens-motivations-in-his-own-words/>

[Accessed 19 1 2023].

Savage, C., 2014. *The New York Times*. [Online]

Available at: <https://www.cnbc.com/2014/03/25/obama-to-call-for-end-to-nsa-bulk-data-collection.html>

[Accessed 22 1 2023].

- Scahill, J. & Begley, J., 2015. *The Intercept*. [Online]  
Available at: <https://theintercept.com/2015/03/10/ispy-cia-campaign-steal-apples-secrets/>  
[Accessed 4 1 2023].
- Schneier, B., 2003. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York, USA: Copernicus Books.
- Schwartz, M. & Preston, J., 2013. *The New York Times*. [Online]  
Available at: <https://archive.nytimes.com/thelede.blogs.nytimes.com/2013/06/23/tracking-snowden/>  
[Accessed 4 1 2023].
- Seamon, R. H., 2008. NSA domestic surveillance: presidential power and the Fourth Amendment. In: R. A. Miller, ed. *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror*. 1 ed. New York, USA: Routledge, pp. 128-131.
- Seglins, D., 2015. *CBC*. [Online]  
Available at: <https://www.cbc.ca/news/canada/cse-monitors-millions-of-canadian-emails-to-government-1.2969687>  
[Accessed 4 1 2023].
- Seglins, D., 2015. *CBC*. [Online]  
Available at: <https://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978>  
[Accessed 4 1 2023].
- Shane, S. & Somaiya, R., 2013. *The New York Times*. [Online]  
Available at: <https://www.nytimes.com/2013/06/17/world/europe/new-leak-indicates-us-and-britain-eavesdropped-at-09-world-conferences.html>  
[Accessed 4 1 2023].
- Sharma, A., Breeden II, J. & Fruhlinger, J., 2021. *csoonline*. [Online]  
Available at: <https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html>  
[Accessed 16 2 2023].
- Shirbon, E., 2013. *Reuters*. [Online]  
Available at: <https://www.reuters.com/article/uk-europe-surveillance-idUKBRE9A103H20131102>  
[Accessed 4 1 2023].
- Singh, R., 2013. *Lawfare*. [Online]  
Available at: <https://www.lawfareblog.com/madisons-vacillations-and-ours>  
[Accessed 8 2 2023].

SMITH, P., 2014. *The New York Times*. [Online]  
Available at: <https://www.scholastic.com/content/dam/teachers/migrated-assets-not-associated-with-content/migrated-pdfs-and-other-files/upfront022414edwardsnowden.pdf>  
[Accessed 20 1 2023].

Snowden, E., 2016. *Edward Snowden Interview on Apple vs. FBI, Privacy, the NSA, and More* [Interview] (25 2 2016).

Soviak, M., 2015. A Transformative Era in Cloud Computing: Questions, Developments, and Affirmations in Light of Snowden's NSA Revelations. Στο: G. Kim, και συν. επιμ. *Harvard Undergraduate Law Review*. Cambridge, USA: The Harvard Law Review, pp. 59, 60, 63.

Spetalnick, M. & Holland, S., 2013. *Reuters*. [Online]  
Available at: <https://www.reuters.com/article/usa-security-records-obama-idINDEE9560BL20130608>  
[Accessed 30 1 2022].

Strohm, C. & Wilber, D. Q., 2014. *Bloomberg*. [Online]  
Available at: <https://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says?leadSource=uverify%20wall>  
[Accessed 8 12 2022].

Sundby, S. E., 1988. A Return to Fourth Amendment Basics: Undoing the Mischief of *Camara* and *Terry*. *Minnesota Law Review*, 2, Volume 72, pp. 383, 383-84.

Szoldra, P. & Kelley, M. B., 2013. *INSIDER*. [Online]  
Available at: <https://www.businessinsider.com/leaked-nsa-slide-of-google-cloud-2013-10>  
[Accessed 21 11 2022].

The Editorial Board, 2014. *The New York Times*. [Online]  
Available at: [https://www.nytimes.com/2014/01/18/opinion/the-president-on-mass-surveillance.html?\\_r=1](https://www.nytimes.com/2014/01/18/opinion/the-president-on-mass-surveillance.html?_r=1)  
[Accessed 19 1 2023].

The Guardian, 2013. *The Guardian*. [Online]  
Available at: <https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>  
[Accessed 3 1 2023].

The Guardian, 2013. *theguardian.com*. [Online]  
Available at: <https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>  
[Accessed 5 1 2023].

The New York Times, 2013. *Communications of the ACM*. [Online]  
Available at: <https://cacm.acm.org/news/167514-nsa-able-to-foil-basic-safeguards-of-privacy->

on-web/fulltext

[Accessed 5 1 2023].

The Washington Post, 2013. *NSA Secrets Government Spying in the Internet Age*. 1 ed. New York USA: Diversion Books.

The White House - Office of the Press Secretary, 2013. *The White House*. [Online]

Available at: <https://obamawhitehouse.archives.gov/the-press-office/2013/08/09/background-president-s-statement-reforms-nsa-programs>

[Accessed 18 1 2023].

The White House, 2014. *The White House*. [Online]

Available at: <https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m>

[Accessed 19 1 2023].

Thoennes, C., 2019. *Defense Intelligence Agency*. [Online]

Available at: <https://www.dia.mil/News-Features/Articles/Article-View/Article/1744523/dia-director-delivers-worldwide-threat-assessment/>

[Accessed 8 2 2023].

Thompson II, R. M., 2014. *The Fourth Amendment Third-Party Doctrine*, Washington, D.C., USA: Congressional Research Service.

Timberg, C., 2013. *The Washington Post*. [Online]

Available at: [https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342\\_story.html](https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html)

[Accessed 4 1 2023].

Toor, A., 2016. *The Verge*. [Online]

Available at: <https://www.theverge.com/2016/11/21/13697072/obama-snowden-pardon-nsa-trump-pompeo>

[Accessed 18 1 2023].

Trifunov, D., 2013. *The World*. [Online]

Available at: <https://theworld.org/stories/2013-06-21/edward-snowden-says-british-spy-agency-gchq-worse-nsa>

[Accessed 4 1 2023].

U.S. DoJ, 2014. *The White House: President Barack Obama*. [Online]

Available at: <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>

[Accessed 17 11 2022].

U.S. Supreme Court, 1979. *Find Law*. [Online]

Available at: <https://caselaw.findlaw.com/us-supreme-court/442/735.html>

[Accessed 4 1 2023].

U.S.C., n.d. *Office of the Law Revision Counsel of the United States Code*. [Online]

Available at:

[https://uscode.house.gov/view.xhtml?req=\(title:50%20section:1861%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:50%20section:1861%20edition:prelim))

[Accessed 3 1 2023].

von Solms, S. & van Heerden, R., 2015. *Research Gate*. [Online]

Available at:

[https://www.researchgate.net/publication/275019554\\_The\\_Consequences\\_of\\_Edward\\_Snowden\\_NSA\\_Related\\_Information\\_Disclosures](https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures)

[Accessed 22 1 2023].

Von Spiegel Staff, 2013. *SPIEGEL International*. [Online]

Available at: <https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>

[Accessed 18 1 2023].

Waddell, K., 2016. *The Atlantic*. [Online]

Available at: <https://www.theatlantic.com/technology/archive/2016/09/would-obama-pardon-edward-snowden/500105/>

[Accessed 19 1 2023].

Waldron, J., 2003. Security and Liberty: The Image of Balance. *The Journal of Political Philosophy*, Volume 11, pp. 191-210.

Webster, D. A., 2021. *The Law Office of David A. Webster*. [Online]

Available at: <https://thewebsterlawoffice.com/2021/06/probable-cause-vs-reasonable-suspicion/>

[Accessed 30 1 2023].

Weinstein, G., 2023. *Forbes*. Encryption: The Necessary Tool For U.S. National Security And The Intelligence Community [Online]

Available at: <https://www.forbes.com/sites/digital-assets/2023/05/07/encryption-the-necessary-tool-for-us-national-security-and-the-intelligence-community/>

[Accessed 14 7 2023].

Wikipedia, 2022. *Wikipedia, the free encyclopedia*. [Online]

Available at: [https://en.wikipedia.org/wiki/Executive\\_Order\\_12333](https://en.wikipedia.org/wiki/Executive_Order_12333)

[Accessed 16 11 2022].

Wikipedia, 2023. *Wikipedia*. [Online]  
Available at: [https://en.wikipedia.org/wiki/Tailored\\_Access\\_Operations](https://en.wikipedia.org/wiki/Tailored_Access_Operations)  
[Accessed 18 1 2023].

Wikipedia, n.d. *Wikipedia*. [Online]  
Available at: [https://en.wikipedia.org/wiki/Barack\\_Obama\\_on\\_mass\\_surveillance#cite\\_note-Obama\\_Speeches-1](https://en.wikipedia.org/wiki/Barack_Obama_on_mass_surveillance#cite_note-Obama_Speeches-1)  
[Accessed 19 1 2023].

Wikipedia, n.d. *Wikipedia*. [Online]  
[Accessed 2023].

Willink, H. T., 2007. To what extent may in a constitutional democracy the rule of law be limited in order to protect it against terrorism? *Accountability Of Intelligence And Security Agencies And Human Rights*. The Hague, The Netherlands: Review Committee On The Intelligence And Security Services (Ctivd) Faculty Of Law Radboud University, Nijmegen, pp. 26-27.

Wizner, B., 2017. What Changed After Snowden? A U.S. Perspective. *International Journal of Communication*, p. 897.

Wizner, B., 2017. What Changed After Snowden? A U.S. Perspective. *International Journal of Communication*, p. 898.

Wizner, B., 2017. What Changed After Snowden? A U.S. Perspective. *International Journal of Communication*, pp. 899-900.

Wizner, B., 2017. What Changed After Snowden? A U.S. Perspective. *International Journal of Communication*, p. 900.

Wolf, Z. B., 2013. *CNN Politics*. [Online]  
Available at: <https://edition.cnn.com/2013/08/12/politics/obama-snowden-whistleblower/index.html>  
[Accessed 18 1 2023].

Wood, D. M., 2009. The 'Surveillance Society': Questions of History, Place and Culture. *European Journal of Criminology*, pp. 179, 179-194.

Ybo, B., 2007. *Accountability Of Intelligence And Security Agencies And Human Rights*. The Hague, Review Committee On The Intelligence And Security Services (Ctivd) Faculty Of Law Radboud University, Nijmegen, pp. 157-158.

Yugas, A., 2022. *The New York Times*. [Online]  
Available at: <https://www.nytimes.com/2022/09/26/world/europe/edward-snowden-russia-citizenship.html>  
[Accessed 3 1 2023].

Zawilska-Florczuk, M. & Frymark, K., 2014. *Centre for Eastern Studies*. [Online]  
Available at: [https://www.files.ethz.ch/isn/176400/commentary\\_124\\_0.pdf](https://www.files.ethz.ch/isn/176400/commentary_124_0.pdf)  
[Accessed 22 1 2023].

Zegart., A. B., 2022. *Spies, lies, and algorithms : the history and future of American intelligence*.  
New Jersey, USA: Princeton University Press.

Zengerle, P. & Strobel, W., 2015. *The Reuters*. [Online]  
Available at: <https://www.reuters.com/article/us-usa-security-surveillance-idUKKBN0OGORF20150601>  
[Accessed 30 1 2023].

Zetter, K., 2015. *Wired*. [Online]  
Available at: <https://www.wired.com/2015/02/snowden-spy-agencies-screwed-us-hacking-crypto-keys/>  
[Accessed 18 1 2023].

Ζαφειρόπουλος, Κ., 2015. *Πως Γίνεται Μια Επιστημονική Εργασία; Επιστημονική Έρευνα Και Συγγραφή Εργασιών*. 2 επιμ. σ.λ.:Εκδόσεις Κριτική ΑΕ.

Κυριαζή, Ν., 1998. *Η Κοινωνιολογική Έρευνα - Κριτική Επισκόπηση Μεθόδων & Τεχνικών*. 1 επιμ. Αθήνα: Ελληνικές Επιστημονικές Εκδόσεις.

Λιαργκόβας, Γ. Π., Ζαχαρίας, Δ. & Δημήτριος, Κ., 2018. *Μεθοδολογία Της Έρευνας Και Συγγραφή Επιστημονικών Εργασιών*. 1 επιμ. σ.λ.:Τζιόλας.