NATIONAL GRADUATE SCHOOL OF POLITICAL SCIENCES
Department of Military and Strategic Studies

U.S. Intelligence and Mass Surveillance After 9/11 Events

A dissertation submitted in partial satisfaction of the requirements for the master degree of strategic and international studies

Realised by:
Drioueche Asma Sarra Youssra

Supervised by:
Dechemi Tewfik

Jury

Pr. Ben AbdeLaaziz Mustapha……..……..President
Mr. Dechemi Tewfik…..…….Advisor
Mr. Boukachabia……...……...Member

Universitary year: 2015-2016

« *I think it's important to understand that you can't have one hundred percent security and then have one hundred percent privacy and zero inconvenience, we're going to have to make some choices as a society* »

President Barack Obama in his statement on June 07, 2013, in California

To the one I owe my passion for English, to my role model, my inspiration in life, My Father

To my guardian and my guide, My Mother

To the source of my never-ending laughter, My Brother

Acknowledgment

I would like to express my very deep gratitude to my supervisor Mr. Dechemi for accepting to supervise me and for assisting me to accomplish this humble work.

I wish to acknowledge with much appreciation Mr. Saibi for helping me with my research.

I would also like to acknowledge the help provided by my teacher Mr. Khouas.

Acronyms

ACLU: American Civil Liberties Union

ADPR: Associate Director for Privacy and Records

AFSA: Armed Forces Security Agency

AIG: Authorities Integration Group

ANT: Advanced Network Technology

AOL: America Online

ARDA: Advanced Research and Development Activity

AT&T: American Telephone and Telegraph

BNDD: Bureau of Narcotics and Dangerous Drugs

CCTV: Closed Circuit Television

CGI: Coast Guard Intelligence

CIA: Central Intelligence Agency

CLPO: Civil Liberties and Privacy Office

COMINT: Communications Intelligence

CSS: Central Security Service

CYBINT: Cyber Intelligence

DARPA: Department of Advanced Research Projects Agency

DEA: Drug Enforcement Administration

DIA: Defense Intelligence Agency

DIOCC: Defense Intelligence Operations Coordination Center

DNI: Director of National Intelligence:

DNINT: Digital Network Intelligence

DOD: Department of Defense

ELINT: Electronic Intelligence

EU: European Union

FBI: Federal Bureau of Investigation

FIPPs: Fair Information Practice Principles

FISA: Foreign Intelligence Surveillance Act

GCHQ: Government Communications Headquarters

GOINT: Geo-spatial Intelligence

GPS: Global Positioning System

HUMINT: HUMan INTelligence

I&A: Office of Intelligence and Analysis

IAO: Information Awareness Office

IC: Intelligence Community

ICO: Information Commissioner Office

IMINT: IMAgery INTelligence

INR: Bureau of Intelligence Research

IRS: Internet Revenue Service

ITT: International Telephone and Telegraph

MASINT: MEAsurement And SIGnature Intelligence

MCIA: Marine Corps Intelligence Agency

MI: Military Intelligence

MIP: Military Intelligence Program

NGA: National Geo-Intelligence Agency

NIMA: National Imagery and Mapping Agency

NIP: National Intelligence Program

NRO: National Reconnaissance Office

NSA: National Security Agency

NSC: National Security Council

ODOC: Office of the Director of Compliance

OGC: Office of the General Counsel

OICI: Office of Intelligence and Counterintelligence

OIG: Office of the Inspector General

ONI: Office of Naval Intelligence

OSINT: Open-Source Intelligence

PATRIOT ACT: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

SIGINT: SIGnal INTelligence

TECHINT: TECHnical INTelligence

TFI: Office of Terrorism and Financial Intelligence

TIA: Terrorist Information Awareness

UK: United Kingdom

UKUSA: United Kingdom-United States of America

U.S.A: United States of America

USA FREEDOM ACT: Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, dragnet-collection and Online Monitoring Act

USSR: Union of Soviet Socialist Republics

WMDs: Weapons of Mass Destruction

Abstract

Despite the vast research about the 9/11 events and its effects, little is known about the ambiguous mass surveillance programs conducted by the U.S Intelligence Agencies during this period and how they spied not only on their citizens, but also on populations from all around the world.

That is why this study aims at identifying the impact of the 9/11 attacks on the conduct of the U.S Intelligence Community. The purpose of this research also involves examining the relationship between both of National Security and Individual Liberties post the 9/11 period.

The preliminary results of this research shows that after the 9/11 events, the amount of mass surveillance programs established by the U.S Government incredibly increased, as well as the legislation set to authorize these blurred activities.

The conclusions drawn from this study portray mass surveillance after the 9/11 events as more aggressive than in the past and thirstier for gathering all kind of data, be it unnecessary one about all the individuals even the innocent ones. This led to a sparking controversy between the advocates of mass surveillance in the name of securing the country, and those protesting against these surveillance activities in the name of defending the individuals' freedoms.

Key words: U.S Intelligence Agencies; the 9/11 events; Mass surveillance; National Security; Individual Liberties.

RÉSUMÉ

Malgré les nombreuses études consacrées aux événements du 11 septembre 2001, les informations concernant les programmes secrets suivis par les services de renseignements américains restent insuffisantes.

Cette recherche a pour objectif d'étudier l'impact des événements du 11 septembre sur le comportement des services de renseignement américains vis-à-vis de la surveillance de masse. Cette étude vise aussi à examiner la relation entre les libertés individuelles et la sécurité nationale.

Les résultats préliminaires de cette recherche montrent que l'éventail des programmes suivis par les services de renseignement américains après les événements du 11 septembre a incroyablement évolué, de même que l'arcenal juridique mis en place pour justifier les activités de surveillance de masse.

Les résultats auxquels nous sommes parvenus prouvent, à travers l'agressivité des programmes adoptés par les services de renseignements américains, que le comportement de ces derniers a effectivement changé après les attaques du 11 septembre, ce qui a ravivé le débat entre les partisans des activités de surveillance de masse qui penchent vers la promotion de la securité nationale, et les opposants à ces activités qui sont en faveur des libertés individuelles.

Les mots clés : les services de renseignements américains- les événements du 11 septembre 2001- la surveillance de masse- la securité nationale- les libertés individuelles.

ملخص

بالرغم من كثافة الأبحاث المكرسة لدراسة أحداث 11 أيلول 2001 وتأثيراتها المختلفة، إلا أن المعلومات التي تتعلق بالبرامج السرية التي اتبعتها أجهزة المخابرات الأمريكية بعد هذه الأبحاث، و كيف تمكنت هذه الأجهزة في هذه الفترة من التجسس ليس فقط على مواطنيها، بل على الأفراد في شتى بقاع العالم، لم يتم التطرق إليها بشكل كبير.

في هذا الإطار، جاءت هذه الدراسة من أجل معالجة تأثير أحداث الحادي عشر من سبتمبر على السلوك المنتهج من قبل المخابرات الأمريكية، كما يهدف هذا البحث إلى دراسة العلاقة بين الأمن القومي و الحريات الفردية بعد هذه الفترة.

الاستنتاجات الأولية لهذه الدراسة تبين أن حجم البرامج المتبعة من قبل المخابرات الأمريكية بعد أحداث 11 سبتمبر تزايد بشكل غير معقول، كما أن القوانين التي كرست في هذه الفترة بغية إضفاء الشرعية على تلك النشاطات المشبوهة لا تعد و لا تحصى.

النتائج المتوصل إليها من خلال هذه الدراسة تثبت أن سلوك المخابرات الأمريكية تأثر بشكل كبير بأحداث الحادي عشر من أيلول، يظهر ذلك من خلال عدائية البرامج و النشاطات المتعلقة بمراقبة الجماهير بعد هذه الفترة وتعطشها لجمع كل المعلومات، حتى غير الضرورية منها وحول كل الأفراد حتى الأبرياء منهم، هذا ما أدى إلى إشعال الجدل بين أولئك الذين لا يمانعون أن تتم مراقبتهم شرط تحقيق الأمن القومي و حمايته من كل التهديدات وأولئك الذين يعارضون هذه النشاطات باعتبارها تقيد الحقوق و الحريات الفردية.

الكلمات المفتاحية: أجهزة المخابرات الأمريكية- أحداث 11 سبتمبر 2001- مراقبة الجماهير- الأمن القومي- الحريات الفردية

TABLE OF CONTENTS

List of Figures

INTRODUCTION

Lately, the focus of the media and the non-governmental organizations increased towards issues linked to mass surveillance and its impact on individual liberties, especially after the revelations made by both WIKILEAKS and several whistle-blowers such as Edward Snowden, a former NSA employee who has sought to shed light on the Government's secret monitoring by providing concrete proof of global communications surveillance programs.

In spite of the sudden appearance of this matter in the media and political sphere, mass surveillance is considered as an activity that has been conducted by states for ages, if not for the changing and ever enhanced techniques used in the surveillance activities, due to the progress in the realm of information and communications technologies.

These technologies have developed tremendously during the cold war because of the lack of security. The United States along with its allies have long invested in these technologies aiming at improving their surveillance programs in order to shield their national security and increase their power.

The 9/11 events were another shifting point in the history of mass surveillance. During this period of time, the U.S.A has seized the opportunity to adopt a more ubiquitous view towards security matters, boosting its mass surveillance mechanisms more than ever and keeping these programs hidden.

The U.S Intelligence Agencies became like a vacuum machine: the more individuals produced data about themselves through their electronic devices and systems, the more these agencies exploited them on the grounds that the threat of terrorism could be anywhere and could hit again at any given moment.

This incredibly huge progress witnessed in the tracking and surveillance technologies created a post privacy world and challenged the prospects for the survival of human freedom and dignity which are only possible if a zone of offline privacy is respected, or else the most personal decisions will fall prey to the manipulation of the corporations, of the media and the government.

This never-ending bargain between security and liberty sparked once again as a consequence to the 9/11 events leading to an endless struggle between the defenders of mass surveillance for the sake of safeguarding their nation and those objecting to these operations to protect their freedoms.

That is why a study in this matter was crucially needed to verify the arguments of both parties and to examine whether or not mass surveillance was necessary to preserve the American national security even if that means crushing the most fundamental human rights. For this end, the research will be conducted to examine the following question:

How did the U.S intelligence agencies change their conduct towards mass surveillance after 9/11 events?

In order to clarify the research question, some subsidiary questions had to be asked:

- Why do the U.S intelligence agencies conduct mass surveillance activities, and in what proportions?
- What are the techniques used by the U.S intelligence agencies to pursue mass surveillance?
- How deep is mass surveillance rooted in the national security, and to what extent is it considered as a violation to individual liberties?

Hypothesis

In pursuance of verifying the research question, as well as the subsidiary questions, we chose the following hypothesis:

The 9/11 attacks accelerated mass surveillance by investing in programs and legislating laws, leaving a broader margin of freedom of maneuver to the U.S intelligence agencies.

As for the subsidiary hypotheses, we chose the following ones:

- Mass surveillance aims at gathering data all around the world in order to safeguard national security.
- Mass surveillance is conducted by using techniques that collect data on the net, phone calls, cameras…
- Mass surveillance is an important tool used by intelligence agencies to preserve the national security.
- Individual liberties are targeted by mass surveillance programs created by the U.S intelligence agencies.

Research space

- **Time:** from the 9/11 events until the year 0f 2016.
- **Place:** United States of America specifically and all around the world in general.

Importance of the research

Speaking from a timely aspect, the importance of this subject shows the fact that after 9/11 events, mass surveillance became more aggressive and blurred. Space-wise, this research is important since the U.S has the largest intelligence community, and therefore conducts the widest number of mass surveillance activities. As for the subject itself, its importance lies in the fact that it is a controversial subject which generated a lot of law reforms, and questioned the authority of the highest members of the U.S government. This subject is also of a great importance, since it focuses on crucial issues regarding individual liberties and especially the right to a private life.

Goals

Among the objectives of this humble research is to get a clearer and more profound perspective on this controversial subject. In addition to that, the purpose of this subject is to raise awareness and to push people to know more about their rights and liberties and to participate in the government's decisions. Furthermore, this study aims at knowing about the extent of National Security and also the limits of Individual liberties.

Research method

In pursuance of surrounding all the aspects about this subject, it was necessary to use some methods.

The first one is "Case Study" which is essential, for we can't handle all the cases, and since the U.S has the most enormous intelligence agencies and pursue the largest amount of surveillance activities, the study would be more applicable to this country.

The second one is "Context Analysis" which is vital in the process of analyzing all the laws and acts and discourses in the U.S in terms of national security and individual liberties, and comparing them to the reality.

Used approaches

For the sake of accomplishing a methodological work; using some theories relevant to our study was crucial.

In the process of displaying the origins as well as the evolution of both mass surveillance and the U.S Intelligence Community, the historical approach imposed itself.

As for creating a dialectics between both National Security and Individual Liberties and determining the relationship between the two of them, "Realist", "legal" and 'moral' approaches had to be used.

Previous studies

In order to get a better view on this subject, a profound look at the precedent literatures had to be taken. Among these studies, the most beneficial one was 'Data and Goliath: The hidden battles to Collect your Data and Control your World' written by Bruce Schneier who spoke about how and why the U.S government is conducting mass surveillance activities.

In addition to 'Intelligence and National Security' by Clark Ransom who talked about the existing relationship between both intelligence and national security in the United States of America.

PART ONE: INTELLIGENCE AGENCIES AND MASS SURVEILLANCE IN THE U.S: A CONCEPTUAL FRAMEWORK AND HISTORICAL BACKGROUND

INTRODUCTION

Intelligence is and has always been a critical and decisive component on which every state depends to safeguard its national security, preserve its borders, and protect its citizens.

After being limited once to the military domain, intelligence today broke into several areas, from economy to society to culture, nothing seems impossible to achieve through this activity.

In pursuance of achieving as perfect of a product as possible, intelligence must be guided by certain principles, it must also follow some phases required to convert information to intelligence. This complex activity is conducted by services or agencies which must be specialized in the field, and which primary mission is to collect and analyze data about foreign entities.

Mass surveillance, one of the activities carried out by intelligence agencies has broken the rule which implies that intelligence is restricted to spying on foreign countries, nowadays intelligence is also concerned with monitoring individuals in order to prevent criminal activities.

Owing its power to a certain extent to intelligence and mass surveillance, the United States of America has invested long and hard in creating the most robust spy network in the world so that its national security is protected and its hegemony is preserved.

The so-called the 'U.S Intelligence Community' conducted mass surveillance activities through a number of programs aiming at targeting individuals inside and outside the country using all kinds of techniques.

CHAPTER ONE: INTELLIGENCE AGENCIES AND MASS SURVEILLANCE: A CONCEPTUAL FRAMEWORK

Intelligence has always been considered as a vital component in any state's power. Its importance could be reflected not only by the constant need of the country for this crucial activity, but by the increase of this need as new events emerge.

That is why, intelligence is a difficult activity that must be conducted by specific agencies which follow a certain set of principles, and it also requires a delicate process in order to achieve the desirable outcome.

Intelligence tuned out to be so significant that it kept evolving as new events emerged. After being limited to spying on foreign countries, intelligence became also involved in monitoring citizens to prevent criminal activities.

Section I. Intelligence Agencies and the Concept of Intelligence

Intelligence is an essential activity that goes through a set of steps leading to as perfect of a product as possible.

Giving the importance of this activity, intelligence could only be conducted by specialized agencies whose primary task is to preserve the national security.

I. Introduction To Intelligence

A. Definition

Formulating a brief definition of so broad a term as intelligence is like making a microscopic portrait of a continent and the product of this effort is likely to have less value than the process of arriving at it.

Misunderstandings within the intelligence community often result from incompatible understandings of the meaning of the word intelligence. Moreover, the assignment and coordination of functions, responsibilities and relationships among the members of the community must rest upon an agreed interpretation of this word in the laws and directives which govern our work.

Before trying to give a precise meaning of intelligence, below are few displayed definitions:

"Know the enemy, know yourself, victory will never be endangered. Know the ground, know the weather, your victory will then be total."[1]

"By intelligence, we mean every sort of information about the enemy and his country, in short, of our own plans and operations".[2]

"The collection of information of military or political value. It may include information gathering, surveillance, observation, reconnaissance, spying, espionage, undercover work, infiltration, Elint, cyber espionage, Humint".[3]

"It is information concerning a foreign entity, usually (although not always) an adversary, as well as agencies concerned with collection of such information. It is intimately tied with the intelligence cycle, a process whereby raw information is acquired, converted into intelligence and disseminated to the appropriate consumers".[4]

"The obtaining or dispensing of information, particularly secret information, also, the persons engaged in obtaining information; secret service"[5]

"Intelligence – the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to planning".[6]

---

1 Sun Tzu, *the art of war*. translated by Griffith Samuel (New-York: Oxford University Press, 1963), p. 129.

2 "Joint intelligence", *joint publication 2-0 (*U.S military, 2013), p. I-1, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

3 Oxford Dictionnaries, sv. "intelligence", http://www.oxforddictionaries.com/definition/english/intelligence.

4 Encyclopedia of espionage, intelligence and security, Volume 2, ed. Lee Lerner and Brenda Wimoth, sv. "intelligence".

5 Webster's Unabridged, cited in : Martin T. Bimfort, a definition of intelligence, *Cental Intelligence Agency*, 18 september 1995, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm.

6 Dictionary of United States Military Terms for Joint Usage. Cited in : Martin T. Bimfort, ibid.

In addition to the previous definitions, in this one the author adds that the analysis resulting from the process of intelligence comes from "all available information concerning the intentions, capabilities and objectives of other countries which are significant to a government's development and execution of plans, policies, decisions and courses of action"[1]

According to the above definitions, intelligence may be looked at as a process including series of interactive steps, formally referred to as an "intelligence cycle", or as the finished product resulting from that process, or a number of organizations that appear as a set of state actors located at different levels of the government structure, known collectively as the intelligence community which deliver multiple services to governments, or series of missions carried out by those institutions in order to satisfy the needs of policymakers; such as counterintelligence.

Intelligence may be defined as the collecting and processing of that information about foreign countries and their agents which is needed by a government for its foreign policy and for national security. The conduct of activities abroad to facilitate the implementation of foreign policy, and the protection of process and product, as well as persons and organizations concerned with these, against unauthorized disclosure.

At a broader level, a standard definition of strategic intelligence is the knowledge and foreknowledge of the world around us; the prelude to presidential decision and action, a tangible product collected and analyzed (assessed or interpreted) in hopes of achieving a deeper understanding of subversive activities, or political, economic, social and military situations around the world.

At a narrower level or tactical level, intelligence refers to events and conditions on specific battlefields or threats of war, what military commanders refer to as "situational awareness". It could concern threats inside the country by local radicals or the infiltration of hostile intelligence agents or terrorists inside the state, or it could concentrate on threats and opportunities overseas.[2]

1 Ibid.

2 Loch K.Johnson, *handbook of intelligence studies* (London : Routledge,2007), p.1.

Intelligence as an information is different from the everyday kind of information, because intelligence usually has a secret component, intelligence analysts blend the open source with information that other nations try to keep hidden.[1]Furthermore, intelligence allows anticipation or prediction of future situation.[2]

Intelligence can be thought of as a jigsaw puzzle. The picture one seeks is full information about subversive activities inside the country, or the capabilities and the intentions of existing and potential adversaries on the world stage. Some intelligence pieces of the puzzle could be found in publicly available documents, others will be derived from spying, whether human agents or machines.

As a result of the above definitions, intelligence aims at providing information and assessments to facilitate accomplishments of the mission; this purpose is supported by more-specific purposes:

-Inform the commander: by helping him in planning, directing, operating, and conducting their assessment through the analysis of the adversary and the operational environment to allow the commander to exploit opportunities in order to maintain the initiative;

- Identify, define and nominate objectives: military planning counts on the determination of clearly defined, achievable, and measurable objectives, by taking in consideration the command's responsibilities, the mission, the intent, and also the adversary (weather, operational area, intentions, objectives, strengths, weaknesses, human factors, ect);

- Support the planning and execution of operations; commanders and staffs at all levels of command demand intelligence for planning, directing, conducting and assessing operations, then help with the execution of the plan with the strategic, operational and tactical intelligence needed to achieve the objectives;

- Counter adversary deception and surprise: intelligence analysts must be aware of the probability that they are being deceived and ought to consider all possible adversary intentions, by using multiple collection sources;

- Support friendly deception effort: misguide the adversary to attain surprise;

1 Ibid., p. 2.

2 "joint intelligence", Op. Cit., p. ix.

- Assess the effects of operations: intelligence contributes in the evaluation of military operations by assessing their influence on all aspects of the operational environment.[1]

To conclude with, intelligence is highly needed for it provides reasoned insight into future conditions, and since knowledge is power, then intelligence is a part of this power, because of its support to the exercise of other parts of power.

B. Principles

Intelligence is guided by a set of principles which help in achieving the desirable outcome. These principles are cited below.

Perspective: intelligence analysts have to get into the adversary's head by following the perspective of "how will the enemy probably perceive this action, and what are his possible responses".

Synchronization: it must be synchronized with operations and plan to provide awareness to intelligence requirements in time to affect the decision intended to be supported. Operation plan and operation order, are the driving force that dictate the sequencing of intelligence operations.[2]

The attacks against the USA at Pearl Harbor in 1941 and more recently against the twin towers and the pentagon in 2001 reflect the importance of accurate intelligence.

Integrity: it is the hall mark of the intelligence profession; it demands credibility and truthfulness, despite of all kinds of pressure (the false estimation of USA/British intelligence agencies about the existence of WMDs in Iraq).[3]

It is noted on the wall of the CIA headquarters building is the inscription "Ye shall know the truth, and the truth shall make you free". Sadly, no one has yet developed the formula by which intelligence agency can know the truth, the whole truth, and nothing but the truth..[4]

---

1 Ibid., p. I-3

2 Ibid., p. X.

3 ibid., p. XI.

4 Fabius Maximus, "How useful are our intelligence agencies? To what degree are they blinded by prejudice and institutional needs?", *Fabius Maximus Website*, https://fabiusmaximus.com/2010/04/13/intel-2/

Unity of efforts: coordination through cooperation and common interests to achieve a desired end state is important to perceive intelligence operations. The unity is facilitated by centralized planning and direction.

Prioritization: it helps in addressing requirements and effectively managing risk by identifying the most important tasks.

Excellence: producers of intelligence ought to achieve the highest possible quality outcome by making intelligence anticipatory, timely, accurate, usable, complete, relevant, objective and available.

Prediction: intelligence is most useful when it focuses on the future and the adversary intentions.[1] However, the events of the past decades like the 9/11, Iraq 2003, 7/7 bombing in London, Paris and Brussels show that intelligence is still not error free.[2]

Agility: intelligence has to be agile and flexible to meet changing operational situations, needs, priorities and opportunities.

Collaboration: in order to reach the highest level of fidelity, there must be a consultation with analysts and experts.

Fusion: it is the process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of the detected activity.[3]

Secrecy: it is important as a barrier to surveillance since without secrets, it is not intelligence. However, it can sometimes raise the question about legality, morality, and accountability.[4]

C. Process

The relating of one set of information to another, or the comparing of information against a database of knowledge already held, and the drawing of conclusions by an intelligence analyst, is the foundation of the process by which intelligence is produced.[5]

1 "joint intelligence", Op. Cit., p. XI.

2 Karolis kupcikas, "the importance of intelligence to international security", *E-Internatoinal Relations Student*, november 8, 2013, http://www.e-ir.info/2013/11/08/importance-of-intelligence-to-international-security/

3 "joint intelligence", ibid.

4 Karolis kupcikas, ibid.

5 "joint intelligence", ibid.

Intelligence operations are wide ranging activities conducted by intelligence staffs, aiming to provide commanders with relevant, accurate and timely intelligence. While the decision makers express the need for intelligence data, intelligence managers convert it into collection plans. The raw information will be gathered by different intelligence techniques and given to analysts for integration, evaluation, and finally finished intelligence product that will be disseminated to the decision maker who will provide feedback to intelligence managers for further additions.[1]

Planning and direction: policymakers establish demands for the intelligence community on several subjects and provide them with guidelines to determine their collection strategies, personnel, equipment and intelligence architecture necessary for supporting force deployments. This step provides quick response to probable crises.

Collection: it concerns the acquisition of raw information necessary to satisfy the demands in the collection plan. It includes direction, scheduling, control of specific collection platforms, human intelligence services and alignment processing, exploitation, and reporting resources with planned collection.[2] Gathering information can be based on two methods, by reviewing published documents (news papers, radio, periodicals, intelligence sources…) which is known as overt technique or through covert technique by penetrating the privacy of others.[3]

Processing and exploitation: by converting raw information into forms which can be understood and readily used by commanders and decision makers at all levels.

Analysis and production: during this operation, intelligence is produced by the collection capabilities assigned to the joint force. All processed information is integrated, evaluated, analyzed and interpreted to create products which will satisfy the commander's priority intelligence demands,[4] which makes analysis the main challenge for intelligence, since it deals with examining numerous kinds of information and drawing conclusions from that analysis.[5]

---

1 "special report, who's watching the watchers? : a comparative study of intelligence organisations oversight mechanisms in Latin America", *Privacy International,* p. 4, https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf.

2 "joint intelligence", Op. Cit, p. XII.

3 Karolis kupcikas, ibid.

4 "joint intelligence", ibid.

5 "who's watching the watchers? *Op. Cit*., p. 3.

Dissemination and integration: here, intelligence is delivered to consumer.

Evaluation and feed back: the evaluation of the performance of intelligence operations by intelligence personnel at all levels.[1]

This diagram here below shows the steps through which intelligence goes through to achieve the desirable outcome.

Figure 1: representing the process of intelligence[2]

D. Methods

In their search for as perfect information about threats and opportunities as they can find, countries turn to a large array of spying techniques, which are considered as well-defined areas of intelligence planning, collection, processing, exploitation, analysis and production and dissemination using a specific category of technical or human resources.

1 "joint intelligence", *Op. Cit.*, p. XIII.

2 Ibid., p. I-7.

Intelligence sources are the means that help with the observation and recording of the information relating to a targeted location organization or individual. These sources include people, documents, equipment, and technical sensors. These disciplines are often classified into more specific subcategories.

- GEOINT: geo-spatial intelligence[1] is a visual representation of activities on earth gathered from satellite, aerial photography, mapping data.[2]
- HUMINT: human intelligence, collected from direct sources -legal and clandestine means,[3] by persons on the ground either friendly accredited diplomats or military attachés, non-governmental organizations, patrolling, prisoners of war, refugees, Special Forces or traveler debriefing. It is the oldest discipline which uses spies, in order to gain advantage over opponents by accessing their secrets, usually through stealthy observation or by intercepting written messages.[4]
- SIGINT: signal intelligence through the interception of communication known as COMINT[5] (which is only acceptable with a court order), in telephone conversations or e-mail transmissions, or by handling written communications like letters or electromagnetic emanations known as ELINT.[6]
- MASINT: measurement and signature intelligence is a highly technical intelligence obtained by identifying and analyzing environmental byproducts of developments of interests including: (geophysical, nuclear, electro-optical, radar…). It involves technical intelligence data or other imagery and signal intelligence to describe distinctive characteristics of targets.[7]

1 Eric Rosenbach and Aki J. Peritz, *Confrontation or collaboration, congress and the intelligence community* (USA: Harvard Kennedy School, 2009), p. 12.

2 "joint intelligence", Op. Cit., p. B-1

3 Lee Lerner and Brenda Wimoth, op. Cit., p. 89.

4 "joint intelligence", Op. Cit., p. I-5

5 Eric Rosenbach and Aki J. Peritz, *Loc. Cit.*

6 Ransom J. Clark, *intelligence and national security : a reference handbook* (London: Praeger security international, 2007), p. 26.

7 Ibid.

- OSINT: open-source intelligence[1] which is based on information in the public sector either domestically or abroad (news, seminars, conferences, radio, TV broadcasts, graphics, commercial databases …).[2]
- TECHINT: until the Second World War, technical intelligence referred to intelligence regarding an enemy's weapons systems. Nowadays, it describes literally all intelligence gathered by the use of technical methods, which evolved as a result to the electronic communications advances.[3]
- CYBINT/DNINT: is the intelligence from intercepted digital data communications transmitted between or resident on networked computers.[4]
- IMINT: imagery intelligence uses photography made either from overhead (balloons, airplanes, satellites) or on the ground.[5]

Signals intelligence and human intelligence are of widespread and general applicability. They can produce intelligence on any topic(for example, the intentions, plans, negotiations, activities and achievements of people involved in the development, acquisition, deployment and use of unconventional weapons), since ultimately the data they acquire stem from the human beings involved.

Imagery is more confined to the study of objects (buildings, aircraft, roads, topography). However, modern techniques have extended its abilities (for instance, infra-red photography can in some circumstances show where an object was, even though it may have gone by the time the photograph is taken.[6]

1 Eric Rosenbach and Aki J. Peritz, ibid.

2 Ibid.

3 encyclopedia of espionage, intelligence and security, ibid..

4 "report to director (Lt Gen Jim Clapper)", NSA scientific advisory, p. 20. avalable in *NSA archives*, http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa22.pdf

5 Ransom J. Clark, Loc. Cit..

6 Joint Services Command and Staff College, advanced command and staff course, *strategic intelligence study period,* sep 04 – Jul 05 (N. 8), p. 2B-2.

II. Intelligence Agencies

A. Definition

The term "intelligence agency" historically referred to a state organization that deals with gathering and interpreting information about an enemy.[1]However, nowadays intelligence agencies encompass any government and other public agencies, as well as private agencies, which are responsible for the collection, analysis and exploitation of valuable information in support of law enforcement, national security and foreign policy objectives. [2]

This makes these agencies an effective instrument of a national power, since they are responsible for conducting espionage on other governments or for preventing other governments' espionage attempts (counterintelligence).[3]

Personnel of any intelligence agency is called agent, spy or undercover officer, who vowed to devote their life to work as a secret agent for the state, there by imposing the need for these agents to stay unrecognized.[4]

Means of information gathering are both overt and covert and may include espionage (communication interception, cryptanalysis, cooperation with other institutions, and evaluation of public source). The assembly and propagation of this information is known as intelligence analysis.

B. Functions

The role of intelligence has undergone fundamental shifts since the end of the cold war. Intelligence is no longer the purview of a few high level decision makers, it is now everybody's business. Within conflict zones intelligence is collected, analyzed and used at lower and lower levels of command, and even within tranquility of domestic life, local law enforcement and even ordinary citizens have become producers and consumers of intelligence.

---

1 The Free Dictionnary, sv. "intelligence", http://www.thefreedictionary.com/intelligence.

2 Margaret Rouse, "intelligence community", *tech target*, http://searchsecurity.techtarget.com/definition/intelligence-community.

3 "intelligence agencies", *Wikia: the home of fandom*, http://memory-alpha.wikia.com/wiki/Intelligence_agency.

4 encyclopedia of espionage, intelligence and security, *Loc. Cit*.

Intelligence agencies can provide the following services for their national governments:

1. Provision of collection and analysis of data in areas relevant to national security;
2. Give early warning of impending crises;
3. Serve national and international crisis management by helping to discern the intentions of current or potential opponents;
4. Inform national defense planning and military operations;
5. Protect sensitive information secrets, both of their own sources and activities and those of other state agencies;
6. May act covertly to influence the outcome of events in favor of national interests or influence international security;
7. Act as a defense against the efforts of other national intelligence agencies (counter intelligence).[1]

To sum up, Intelligence as an extremely difficult activity conducted by intelligence agencies has evolved tremendously. This drastic transformation may be seen in its functions which changed from gathering information about the enemy and its intentions, to collecting, analyzing and assessing data about foreign countries and also citizens. This transformation is also reflected by the intelligence's interference in other domains besides the military one.

This change also affected the way intelligence agencies work due to the evolution of technology. After performing as collection and analysis units, they became fully-pledged covert armies by operating in shadows, called upon to take action when no one else can. This makes them the most sensitive protective security shield for a country.

1 "the role of intelligence", *federation of american scientists*, february 23, 1996.

Section II. Mass Surveillance

Intelligence has always been involved with spying on foreign entities; however after a while it became also interested in monitoring ordinary citizens which is known as 'mass surveillance', and just like intelligence, mass surveillance experienced many transformations throughout history, leading to a progress in the techniques used in conducting it.

I. Definition

The word "surveillance" is derived from the french word "surveiller", which means watching over. It refers to the act of monitoring and processing the behavior and activities of people by paying distributive, close and sustained attention to them, for the purpose of influencing, managing, directing or protecting them, which makes it an ambiguous practice that either generates a positive or a negative effect.[1]

To be more specific, "mass surveillance" is the subjection of an entire population or a significant element of it in order to collect data about them, by accessing to an unlimited number of users' private communications, e-mails content or other personal information of a wide set of people, so that they are well defined, without any suspicion related to a particular individual or group.[2]

In 2006, the surveillance studies network produced a report for the Information Commissioner Office (ICO), in which the term mass surveillance was defined as: "where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance".[3]

The Electronic Frontier Foundation also defined this concept saying that it is "the pervasive surveillance of an entire or a substantial fraction of a population". This in today's globalized and very connected world means that mass surveillance is affecting each of us.[4]

---

1 Kiril Mitov, "influence of mass surveillance on business and society", *robopartans group, https://robopartans.com/wp-content/uploads/2014/03/MassSurveillance.pdf.*

2 "Mass Surveillance", *privacy international*, https://www.privacyinternational.org/node/52.

3 United Kingdom, House of Lords, constitution committee, "surveillance: citizens and the state" (London, January 21, 2009).

4 Kiril Mtrov, ibid.

The surveillance is usually carried out by governments or governmental organizations; however it could also be carried out by private companies, either on behalf of governments or at their own initiative.[5]

There are two kinds of mass surveillance, untargeted one that collects data about every single person for possible future use, and a targeted one which is directed at specific individuals such as suspected terrorists and criminals. So clearly the type of untargeted mass surveillance is illegal because t affects innocent people.

The legality and the permission necessary to engage in mass surveillance is different from one country to another, but in most cases a court order is required since mass surveillance involves a systematic interference with people's right to privacy. However, governments always argue that in order to protect their citizens from all kind of threats, especially terrorism, there is no escaping from mass surveillance.

II. Historical Background

The mass surveillance culture is not completely modern; it's been used for ages, because knowing what everyone was doing was considered in all the civilizations paramount to the security of the state. Nevertheless, the advances in technology enhanced the capacities of governments to collect greater amounts of data much more efficiently.

Going back in history, we find that mass surveillance has always been an issue. In the late 1215, in Rome, the Pope Innocent the third presided over a great council of the church known as "the Fourth Lateran Council". This latter investigated even in what it called "crimes of thought" by trying to find out the content of the populations' minds, through bishops representatives who will inquire at least once a year to discover if anyone holds secret conventicles or who differ in their life and habits from the normal way of living of the faithful. Those who had been convicted of heresy would be subject to lifelong scrutiny of their thoughts by ecclesiastical authorities to ensure they did not return to their "old errors". This was threatening to the freedom of individuals.

5 "Bernie Sanders on Privacy and digital rights", *feelthebern.org*, http://feelthebern.org/bernie-sanders-on-privacy-and-digital-rights/.

Other forms of mass surveillance could be found in the roman constitutions. While the twenty first one mandated that all citizens confess all their sins to a priest at least once a year or else they would be excluded. The thirty eighth one required to keep records of each trial, whereas the sixty eighth one stated that Jews and Muslims have to wear distinguishing clothes to be recognizable for the authorities.

The majority of the population accepted the simplest statements of belief they were required to make. They lived within a system of full surveillance that was deeply feared, and even the most powerful opponents of the political activities of the papal curia did not dare attack the church.

What these stories made clear, is that everything was known and that justice was only possible through a system of total surveillance, which was easily practiced with the idea of "if you are innocent, you have nothing to fear" and that mass surveillance was necessary to keep the population safe from enemies.[1]

By the eighteenth century, centralized administrations were created, which made it easier for the governments to gather and keep written records of data about the population. Later on, under the influence of Alphonse Bertillon, a new system was established to identify and monitor people through files that included photographs and series of anthropometric measurements (height, eye color…) and dactyloscopic data (fingerprints).[2]

In the late 1800, Jeremy Bentham came up with the concept of "Panopticon", which was a design that led according to Michel Foucault to the foundation of modern surveillance. This principle of construction was applicable to any kind of institution in which people are kept under inspection (prisons, work-houses, hospitals, manufactures, schools…).The circular structure required all the prisoners' cells to have a window allowing in sunlight so that the inmates lived in a constant fear of being watched that guaranteed a surveillance of great efficiency even if nobody was in the guard tower.[3].

1 Amanda Power, "under watchful eyes: the medieval origins of mass surveillance", *Lapham's Quarterly,* (2012), http://www.laphamsquarterly.org/spies/under-watchful-eyes.

2 Sophie Coeuré, "the origins of mass surveillance", interviewed by Ivan Jablonka, translated by Arianne Dorval, *books and ideas*, http://www.booksandideas.net/The-Origins-of-Mass-Surveillance.html

3 Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W.W. Norton & Company, 2015), p. 28.

Michel Foucault wrote about this idea "hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power".[1]

A lot of prisons since the nineteenth century were constructed with the Panopticon's circular theme, but due to the limited observation provided by the center tower's view, this concept failed to create a complete surveillance reality that became later on not limited just to prisons but to all the society.

In his book "1984" George Orwell extended the concept of the Panopticon so that it covered the entire society. Thanks' to the invention of telescreen, the state could have a total visual and auditory access into homes, streets, workplaces, to remind the population that they are constantly being watched.[2] The closed circuit television (CCTV) was according to George Orwell a key technology in mass observation since it could be placed everywhere, creating a state of control, a reminder to stay in line which Bentham hoped to reach, and there was of course no way of knowing whether you were being watched at any given moment, how often or on what system the thought of observing everybody all the time was permanently conceivable.

Nowadays, we talk about a digital mass surveillance through the loss of control over the terms of the infrastructure where personal data are stored and circulated by users of digital services, mobile applications and online platforms.[3]

In conclusion, mass surveillance experienced a huge change over the years, as new technologies emerged, such as new image analysis algorithms in CCTV, the inclusion of new sensor systems that go beyond visual surveillance and new data integration capabilities that put together traditional surveillance along with advanced profiling and data mining techniques, which provided states with greater and virtually instantaneous powers and paved the way for a change of scale in the gathering, processing and storage of data.

1 Kevin Manish, "surveillance ethics", in *internet encyclopedia of philosophy*, http://www.iep.utm.edu/surv-eth/.

2 Chris Thompson, "the history of mass surveillance", *truthout*, june 21, 2013, http://www.truth-out.org/speakout/item/17139-the-history-of-mass-surveillance.

3 David Wright et al. "sorting out smart surveillance", *computer law & security review*, (2010), p. 344.

III. Techniques Of Mass Surveillance

For years, it's been confirmed over and over again that governments around the world are relying on different tools to spy on their citizens. They can listen in on cell phone calls, use voice recognition, scan mobile networks, read e-mails and text messages, censor web pages, track people through GPS and even change the content of e-mails while en route to a recipient, or secretly turn on webcams in personal laptops, leading to a surveillance on a massive scale.

The methods of mass surveillance allow governments to capture virtually all aspects of our lives. The gathered data is processed by different information techniques and statistical methods and the resulting information is presented with the help of data visualization programs to obtain rapid insight and to make further actions possible.

The most known tools used by state departments to practice mass surveillance are the following:

- Postal surveillance: by photographing all the mail sent and recording the license plates and facial features of customers.
- Cameras: video cameras contribute in observing an area, they are often connected to a recording device or IP network and watched by a security guard or law enforcement officer.

In the U.S.A, the Department of The Homeland Security awards billions of dollars per year for local, state and federal agencies to install modern video surveillance equipment.

- Cell phone tracking: by tapping into the cables that connect the cell networks globally and cooperating with communications companies to install intercept equipment. This technique is widespread officially and unofficially. In some countries, the intelligence agencies have the capacity to activate microphones in cell phones remotely by accessing their diagnostic or maintenance features to listen to conversations that take place near the person holding the phone, even if it is off, it can be easily detected using the multilateration technique to calculate the differences in time for a signal travel from the cell phone to each of several cell towers near the owner of the phone.

For instance, in the U.S.A, telephone calls are constantly recorded using a top secret order from foreign intelligence surveillance court to find out what communications you made and received, who you talked to, where you were when you talked to them, the lengths of your conversation and what sort of device you were using, which is known as "Bulk Collection".

To protect the customer's privacy, Apple's iphone6 has been designed to encrypt e-mails, contacts, photos with a code generated by a complex mathematical algorithm that is unique to an individual's phone. This initiative was not welcome by intelligence agencies.

- Watch lists: governments declare that they are backup law enforcement in prevention of terrorism, but in reality they are considered to be one of the methods of mass surveillance, since everyone has to give their details to prove that they don't figure in the watch list. For instance, in order to travel by plane in the U.S.A, one has to be accepted by checking against "A NO FLY LIST" to fight terrorism and catch terrorist or suspected ones, Nevertheless, these lists turned out to be ineffective because of the false flag terror.
- Internet surveillance: Although the internet was not supposed to be subject to centralization, it has become the most important tool for monitoring the data and the traffic, using automated internet surveillance computers that identify trigger words, certain visited websites, communicating or chatting with suspicious individuals.
- Social network analysis: such as Facebook, MySpace, Twitter, from which data like personal interests, beliefs, thoughts and activities are extracted. Intelligence agencies in the U.S.A invest heavily in research involving the social network, considering the amount of terrorist cells spread on the internet. Some consider the social networking to be a "participatory surveillance", since users are putting personal data themselves.
- Biometric: which analyzes physical or/and behavioral characteristics for authentication, identification or screening purposes, including fingerprints, DNA, facial patterns, manner of walking, voice, human identification at a

distance. The F.B.I is spending one billion dollars to build a new biometric database that will store DNA, facial recognition data, fingerprints, palm prints and other biometric data of people living in the U.S.A.

- Aerial: by collecting data from an aerial vehicle like a plane or a helicopter, for the purposes of critical infrastructure protection, border patrol, transit monitoring and general surveillance. Over the years, developed systems consisting of large teams of self directed drone planes have been designed in order to monitor the mass.
- Data mining and profiling: the application of statistical techniques and programmatic algorithms to discover thanks to an electronic trail, previously unnoticed relationships within the data of a person that perhaps is not consciously aware of themselves, like a call from home, phone card, rented video. when many such transactions are collected, they can be used to assemble a detailed profile revealing the actions, habits, beliefs… of the individual, which is then used by programs like ADVISE or TALON to determine whether the person is a military, criminal or political threat.
- Satellite Imagery: This contributes in detecting chemical traces or for identifying objects in buildings, underground…
- Radio Frequency Identification Tagging: this technique is incorporated into a product, an animal or a person to track those using radio waves.[1]
- The ANT catalog[Advanced Network Technology]: if the data wanted by intelligence services resides in inaccessible places, they use their specialized materials from the ANT catalog (cell phone networks, keyboards, monitors, routers, services, wireless lan, room surveillance, USB, firewalls).

To conclude, the variety of mass surveillance techniques used by governments has evolved to capture all the aspects of their citizens' life, and expose all of their habits and relationships to constant monitoring enhanced by modern technologies. And Even if needed to catch criminals, mass surveillance is still considered as a highly offensive procedure taken against individuals' rights to a private a life.[2]

1 "Surveillance. Types of Surveillance :Cameras, Telephone ECT", *Word Systems inc.*

2 Jacob Appelbaum, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox", *spiegel online,* december 29, 2013.

Defining the word mass surveillance as watching over, reflects a certain idea about governments, how is it that the government has the ability of watching over?, what distinguishes them from ordinary citizens so that they have the privilege of watching without being watched; without submitting to the slightest amount of oversight.

If anything could be concluded from this chapter is that modern technologies have contributed greatly in developing means of intelligence, helping this latter to explore other fields than the military one. Mass surveillance has also benefited from modern technologies which gave bigger powers to the government to conduct such activities allowing them to collect the data available about their citizens, and because of this technological progress, the tools used by intelligence agencies to conduct mass surveillance have seemed to be more ambiguous and less transparent than ever, leading to a total secrecy surrounding these activities.

Mass surveillance could be justified if it is targeted towards monitoring suspected groups or individuals. However, untargeted mass surveillance is not legitimate since it harms innocent people and generates a feeling of obedience and fear that reminds the populations to stay in line at all times, preventing any opposition from arising.

CHAPTER TWO: U.S. INTELLIGENCE AGENCIES AND MASS SURVEILLANCE BEFORE 9/11 EVENTS

Giving the importance of intelligence in empowering countries, the United States of America has always relied on this crucial component to safeguard its national security and to preserve its hegemony. that is why, time after time the U.S.A kept on building the most robust empire of intelligence agencies that has ever existed in the world.

Among the missions carried out by this so-called 'Intelligence Community', is conducting mass surveillance activities by establishing a number of programs aiming at collecting information whether inside or outside the country.

SECTION I. THE U.S. INTELLIGENCE COMMUNITY

The United States has constantly given a tremendous amount of significance to intelligence and more specifically to mass surveillance, therefore it has invested greatly in founding and enhancing its intelligence agencies.

I. Overview

The United States Intelligence Community is a federation of seventeen separate government agencies[1] that work both separately and together in order to pursue intelligence activities considered necessary for the conduct of foreign relations and national security of the United States.

This wide, complexly structured Intelligence Community was established on the basis of the National Security Act of 1947[2] and the executive order 12333, signed on December 4, 1981 by the U.S.A President Ronald Reagan. However its structure was revised in the Intelligence Reform and Terrorism Prevention Act of 2004,[3] in which the

1 Michael German, "The U.S Intelligence Community Is Bigger Than Ever,But Is It Worth the Cost?", *Defense One*, february 6, 2015, http://www.defenseone.com/ideas/2015/02/us-intelligence-community-bigger-ever-it-worth-it/104799/.

2 encyclopedia of espionage, intelligence and security, ibid., sv. "intelligence and law enforcement agencies"

3 David R. Shedd, What guides the U.S Intelligence Community, the daily signal, march 28, 2016, http://dailysignal.com/2016/03/28/what-guides-the-us-intelligence-community/

head of the Intelligence Community became the Director of National Intelligence who is in charge of controlling the National Intelligence Program budget, establishing goals and priorities for the I.C and directing the process of national intelligence by the members of the I.C.

Members of the Intelligence Community include intelligence agencies, military agencies and civilian intelligence and analysis offices within federal executive departments. These agencies are linked through an array of data sharing platforms and portals, including the National Counter-terrorism Assessment Team, 71 FBI Joint Terrorism Task Forces, 56 Field Intelligence Groups and 78 state and local Intelligence Fusion Centers, which can put together military and private sector participants.[1]

The annual intelligence budget exceeds 70 billion dollars; However that number represents just a small portion of what the U.S spends on national security.

II. The Intelligence Community Tasks

The intelligence community precedes its tasks under two separate programs:

1. The National Intelligence Program (NIP); previously known as National Foreign Intelligence Program, as defined by the national security act of 1947 "refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of National Intelligence and the head of a United States Department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed forces".

2. The Military Intelligence Program(MIP): includes the programs, project or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operation by the United States Armed Forces; it is directed by the Under Secretary of Defense for Intelligence.

Among their several activities, the members of the intelligence community gather and produce foreign and domestic intelligence, contribute to military planning and perform espionage.

1 Michael German, ibid.

Executive order 12333 made the intelligence community in the U.S.A responsible for the following tasks:

- Gathering of information required by the president, the National Security Council, the Secretary of State, the Secretary of Defense and other executive branch officials, using all available legal means under the U.S Constitution and in accordance with the president's national security priorities.
- Collecting information to protect against international terrorism, proliferation of weapons of mass destruction, drug crimes and other hostile activities.
- Protecting the security of information, installations, property and employees
- Production and dissemination of intelligence.
- Support of diplomatic and administrative activities in the USA.[1]

Overall, the U.S intelligence community strives to provide valuable insight on essential issues by collecting raw intelligence, analyzing it and producing timely and relevant products[2] that support the whole of U.S government efforts to preserve the homeland and avoid strategic surprises by anticipating emerging events, providing counterintelligence and defeating terrorists and preventing them from accessing to weapons of mass destruction, which makes the US Intelligence Community the most powerful spy network in the world.[3]

III. Members Of Intelligence Community

There are sixteen members of the U.S intelligence community (seventeen if we count the Office of the Director of National Intelligence). This intelligence community is headed by the President and the National Security Council (NSC) which relies on the Director of National Intelligence to manage the sixteen agencies.

The Intelligence Community employs over 150,000 people and has a budget of about 44 billion dollars a year, making it the largest and most expensive of intelligence agencies ever assembled by any country in history.[4]

1 Bruce Schneier, op.cit., p. 50.

2 Ransom J. Clark, Op. Cit., p. 24.

3 Direction of National Intelligence, *Op. Cit.*, p. 6.

4 Loch K. Johnson, *Op. Cit.,* p4.

The U.S intelligence community is made up of bureaucracies that operate in secrecy to help prevent leaks of classified information and penetration by foreign intelligence services. Every single member of the intelligence community is in charge of certain duties and tasks.

A. The Central Intelligence Agency(CIA)

It is a civilian foreign intelligence service of the U.S government and an independent executive branch agency founded in 1947. This agency is responsible for the collection, analysis, production and dissemination of all-source data[1] but mainly with the use of (Humint)[2] for the conduct of foreign intelligence[3] and counterintelligence without performing any internal security missions within the United States; it is charged of the establishment of intelligence in accordance with other elements of the intelligence community, in addition to supporting administrative and technical activities in and outside the country, it also conducts covert action activities agreed by the President, furthermore, the C.I.A conducts foreign relationships with intelligence services of other states.[4]

The C.I.A falls into four elements: 'the National Clandestine Service' which gathers foreign intelligence that is not obtainable through other means, 'the Directorate of Intelligence' which analyzes and produces reports, briefings and papers on key foreign intelligence issues, 'the Directorate of Science and technology' which accesses, gathers and exploits data to facilitate the execution of the C.I.A's missions, and 'the Directorate of Support'[5] which delivers a full range of support including acquisitions, communications, facilities services, financial management, information technology, medical services, logistics and the security of agency personnel.

1 The United States of America, National Commission on Terrorist Attacks, "9/11 Commission Report", p. 86.

2 Eric Rosenbach and Aki J. Peritz, *confrontation or collaboration? : congress and the intelligence community* (USA: Belfer Center for Science and International Affairs, 2009), p. 15.

3 "Top 10 Best intelligence agencie in the world", *ABC news Point*, December 15, 2014, http://www.abcnewspoint.com/top-10-best-intelligence-agencies-in-the-world-2015/

4 Encyclopedia of espionage, intelligence and security, sv. "intelligence and espionage carreers".

5 "Members of the IC", *Office of the Director of National Intelligence web site*, https://www.dni.gov/index.php/intelligence-community/members-of-the-ic.

B. Director of National Intelligence (DNI)

As the Cabinet of the Intelligence Community and a part of the Office of the Director of National Intelligence (ODNI), the DNI directs and oversees all national intelligence programs and serves as principal advisor to the President, the National Security Council (NSC), and the Homeland Security Council on intelligence issues.[1]

C. The Defense Intelligence Agency (DIA)

It is an external intelligence service of the United States, an element of the department of Defense and a branch of the Defense, Department specialized in defense and military intelligence.[2]

Established in October 1, 1961 and designated a combat support agency in 1986, the D.I.A mission is to gather, analyze, produce and assess foreign and counterintelligence, political, economic, industrial, geographic and medical intelligence to support national and departmental tasks.

This agency provides defense intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other defense department and non-defense agencies and informs them about the military intentions and capabilities of foreign governments and non-state actors. This organization also directs all issues concerning the Defense Attaché system. All in all, the DIA produces approximately one-fourth of all intelligence content into the President's Daily Brief.

In December 2007, The D.I.A established the Defense Intelligence Operations Coordination Center (DIOCC) to seamlessly integrate all defense intelligence resources on the transitional threats to U.S national security and to enhance defense intelligence collaboration. This agency also established in August 2008 the Defense Counterintelligence and Humint Center and the Joint Intelligence Task Force for Combating Terrorism.

1 Eric Rosenbach and Aki J. peritz, *op. Cit*., p. 14.

2 Loch K. Johnson, *Loc. Cit.*

D. The National Security Agency (NSA):

Originating as a unit to decipher coded communications in World War I, then known as the Signal Security Agency that intercepted and deciphered the communications[3] of the Axis powers during World War 2; this Defense Department was officially established as the N.S.A in a memorandum of October 24, 1952 by President Truman, but at the time this agency wasn't introduced to the public for secrecy reasons and was referred to as ' no such agency' and since then it has become one of the biggest intelligence agencies in term of employees and budget.

The N.S.A is divided into The Signals Intelligence Directorate, The Information Assurance Directorate, The Central Security Service, the N.S.A/CSS Threat Operations Center, The National Security Operations Center and The Research Directorate.

The N.S.A is responsible for global monitoring, gathering and processing of data for foreign and counterintelligence purposes. In addition to handling the transmission and the distribution of signals intelligence and communications security material; the N.S.A conducts foreign cryptologic liaison relationships, it also protects the U.S government communications and information systems[2] against penetration and network warfare, which makes this agency the forefront of communications and information technology.

E. The National Reconnaissance Office (NRO)

Established in September 1961, the NRO is a part of the Defense Department and considered to be one of the 'big five' U.S intelligence agencies responsible for research and development, acquisition, launch, deployment, operation of overhead systems[3] and related data processing facilities to gather information.[4] Along with conducting foreign liaisons relating to the formerly mentioned tasks; it also provides satellite intelligence to several government organizations, such as (SIGINT) to the N.S.A and can even warn about potential trouble spots around the world and help plan military operations[5], which makes it a foundation for global situational awareness.

---

3 "9/11 Commission Report", Op. Cit. p. 87.

2 "Members of the IC", ibid.

3 Eric Rosenbach and Aki J. peritz, O*p. Cit*., p.p. 15-16.

4 "9/11 Commission Report", Loc. Cit.

5 "Members of the IC", ibid.

The Director of the N.R.O is selected by the Secretary of Defense with the concurrence of the D.N.I and also serves as the Assistant to the Secretary of the Air Force.

F. The National Geospatial-Intelligence Agency (NGA)

It was known as the National Imagery and Mapping Agency (NIMA) until 2003.It is a combat support agency under the United States Department of Defense and an intelligence agency of the United States Intelligence Community, at the same time it provides timely and accurate geospatial intelligence in support of national security objectives.[1]

Additionally to gathering, analyzing geospatial data (Geoint), describing, assessing and visually depicting physical features and geographically referenced activities on earth[2], this member of the organization of the intelligence community provides assistance during natural and man-made disasters and security planning for major events.[3]

G. Twenty-fifth Air Force (25AF)

Working under the Department of Defense, this agency was originated as The United States Air Force Security Service and finally established on 29 September 2014 as the (25AF). Its main mission is to provide intelligence, surveillance and reconnaissance products, applications, capabilities and ressources, it is also charged of cryptologic activities

H. Army Military Intelligence (MI)

It is the intelligence branch of the United States Army; it provides timely, relevant, accurate intelligence and warfare support to tactical, operational and strategic level commanders

1 Ibid.

2 Eric Rosenbach and Aki J. peritz, O*p. Cit*., p. 15.

3 "Members of the IC", ibid.

I. Marine Corps Intelligence Activity (MCIA)

This department of Defense branch was created in 1987, provides tactical and operational intelligence services[1] to the Marine Corps and the U.S intelligence community and supports the development of service doctrine, force structure, training and education and acquisition.

J. Office of Naval Intelligence (ONI)

It was established on March 23, 1882 for a "seek out and report" on the advancements in other's countries' navies, which makes it the oldest member of the American intelligence community operating under the Department of Defense. It is the leading provider of maritime intelligence to the U.S Navy and joint war fighting forces, as well as national decision makers and other consumers in the Intelligence Community[2], by providing superiority for navy commanders and operational forces and achieving a penetrating knowledge of adversaries and a profound understanding of the maritime environment.

K. The Federal Bureau of Investigation (FBI)

The F.B.I was established in 1908, it serves as the investigative arm of the Department of Justice,[3] and as the nation's prime federal law enforcement organization which makes it a vital link between intelligence and law enforcement communities.

The F.B.I is concerned with domestic intelligence by fighting cyber threats and tracking the activities of suspected subversives or terrorists[4] and paying close attention to terrorist efforts to acquire and use weapons of mass destruction through the adaption to trends in terrorist recruitment, financing and training. The F.B.I mission also involves combating foreign intelligence inside (counterintelligence) the U.S.[5]

1 Ibid.

2 Ibid.

3 Eric Rosenbach and Aki J. peritz, O*p. Cit*., p. 16.

4 Loch K. Johnson, p. 4

5 Encyclopedia of espionage, intelligence and security, ibid.

L. The Drug Enforcement Administration (DEA)

It is a federal law enforcement agency[1] established in 1973 that became a member of the intelligence community working under the Department of Justice in 2006. This agency focuses on fighting drug smuggling and trafficking and use within the United States and enforcing the controlled substance laws and regulations of the United States and facilitates full and appropriate intelligence coordination and information sharing with other members of the U.S Intelligence Community[2]

M. The Bureau of Intelligence and Research (INR)

It is an intelligence unit in the Department of the State[3] and the focal point in it, tasked with providing all-source intelligence support to the United States diplomats and analyzing information, to give them "decision advantage" as they seek to protect and advance American interests around the world.

The bureau provides daily briefings, reports and memoranda to the Secretary and other Department principals and members of Congress and their staffs as appropriate. The INR also develops intelligence policy for the Department of State and works to harmonize all agencies' intelligence activities abroad with the United States policy.

In addition to the previous missions, the INR taps into the expertise of academia, think thanks, research council, non-governmental organizations and the private sector to expand the universe of knowledge available to policymakers and the intelligence community.

N. Coast Guard Intelligence (CGI):

It is the military branch of the United States Coast Guard operating under the Department of the Homeland Security, one of the Nation's five armed services and an element of the Central Security Service established in 1915. Its primary mission is to protect the public from the sea (maritime safety), to preserve maritime mobility, to safeguard U.S economic and security interests in any maritime region in which those interests may be at risk, including international waters and the U.S coasts, ports, and inland waterways.[4]

1 Eric Rosenbach and Aki J. peritz, *Loc. Cit.*

2 "Members of the IC", ibid.

3 Loch K. Johnson, *Loc. Cit*.

4 "Members of the IC", ibid.

The Coast Guard's Intelligence and Criminal Investigations Program include its National Intelligence Element, the Criminal Investigations Service, the Counterintelligence Service, the Intelligence Coordination Center and the Cryptologic Service.

O. The office of Intelligence and Analysis (I&A)

This organization in charge of collecting, analyzing and disseminating intelligence throughout the Department of the Homeland Security to the other members of the United States Intelligence Community to provide actionable intelligence in order to support decision making while working closely with state, local, tribal and private sectors partners.

The I&A focuses on threats related to border security; chemical, biological, radiological and nuclear issues, critical infrastructure, domestic extremists and suspicious travelers entering the U.S.[1]

P. the Office of Intelligence and Counterintelligence (OICI)

It was established under the Department of Energy in 1977, it focuses on collecting intelligence for its department and also technical intelligence about foreign countries for the other members of the intelligence community. It is specialized in nuclear weapons, nuclear proliferation, nuclear energy, radioactive waste and energy security.

Q. The Office of Terrorism and Financial Intelligence (TFI)

It was formed in 2004. This Department of Treasury branch is mainly occupied with safeguarding the financial system and combating the international financial networks[2] against illicit use and fighting rogue nations, terrorists' facilitators, weapons of mass destruction proliferators, money launderers, drug kingpins, serial killers and other national security threats.

1 Eric Rosenbach and Aki J. peritz, O*p. Cit*., p. 17.

2 Ibid.

Considering that The United States of America gives a great deal of importance to intelligence, its Intelligence Community has been evolving extensively over the years due to the changing environment, and it is now bigger than ever. This significance given to these agencies is also obvious through their budget which is mind blowing, and that is without a doubt just the tip of the iceberg.

Each member of the U.S Intelligence Community covers a certain domain whether on domestic or foreign levels, but they all depend on each other to conduct their operations through the exchange of information or technical assistance.

Section II. Mass Surveillance Programs Before 9/11 Events

The practice of mass surveillance in the United States goes back to wartime monitoring and censorship of international communications, and after the First World War the surveillance continued through programs and projects which targeted individuals and organizations. That's why; the following section will be divided into programs targeting U.S citizens, others targeting Non U.S citizens, and those targeting both.

I. Programs Targeting U.S Citizens

A. COINTELPRO

COINTELPRO was the FBI's secret program. Operations of this program which includes several covert and sometimes illegal projects were pursued by the U.S FBI in order to monitor, infiltrate, neutralize, discredit and disrupt the Communist Party and also domestic political organizations such as Civil rights movements when traditional methods of repression (harassment, prosecution exposure…) failed to counter the growing insurgency.

This program officially started in August 1956, but was successfully kept secret until 1971, in part because of frustration with Supreme Court rulings restricting the Government's authority to proceed overtly against dissident groups. The director of the

FBI "J. Edgar Hoover" even issued directives ordering FBI agents to expose, misdirect, discredit, neutralize or otherwise eliminate the activities of those movements and especially their leaders.

Methods used in this program involved anonymous calls, infiltration, waged warfare, IRS audits and creation of documents and misguided stories that would divide these organizations internally, in addition to legal harassments and sometimes even illegal force.

Due to accusations against the COINTELPRO program, the FBI was referred to the Church Committee which found that this program violated specific statutory prohibitions and infringed the constitutional rights of American citizens, and therefore COINTELPRO was shut down in April 1971.

B. The Data Intercept Technology Unit

It is an FBI unit established in 1997 charged with intercepting phone calls and e-mail messages of terrorists and foreign intelligence officials inside the U.S, and it is actually this unit that is responsible for collecting the data from several internet companies such as Google and hands them over to the NSA for further analysis.

C. Carnivore

Originated As a project named 'Omnivore', this software program housed in a computer unit was implemented in October 1997 by the FBI in order to monitor, filter, seize and decipher[1] emails and electronic communications using a customizable packet sniffer and a removable disk drive, which targeted at first criminal activities but then tracked all the users' internet traffic.

This internet surveillance system had to be physically installed at an Internet service provider or other location where it can sniff traffic on a Lan segment to search for email messages in transit. The FBI uses this program in collaboration with the internet service providers, who are obliged under a court order to fully cooperate with the law enforcement agencies in accordance with title3 of the Crime Control and Safe Streets Act of 1968.[2]

1 Talitha Nabbali and Mark Perry, "Going for the Throat: Carnivore in an Echelon World - Part I", *computer law & security report*, vol. 20, 2004, p. 456.

2 Ibid., p.459

The Electronic Frontier Foundation reported concerns about the dangers of this police ware, the FBI got back on those allegations saying that this software can be configured to intercept only electronic communications in conformity with court orders. In addition to that, the FBI sometimes derives legitimacy from the Communications Assistance for Law Enforcement Agencies Act of 1994 which demands that the phone companies design their network in way that will support surveillance systems.[1]

Nonetheless, the truth is that Carnivore did not include appropriate safeguards to prevent misuse and therefore violated the Electronic Communications Privacy Act amended to Title3 of the Crime Control and Safe Streets Act, which clearly states that a court order should be given as long as there is a probable cause that will certify the relevance to an occurring crime.[2]

II Programs Targeting Non U.S. Citizens

The Black Chamber

Also known as The Cipher Bureau, the Black Chamber was the United States' first peacetime cryptanalytic organization, and a forerunner of the National Security Agency. It was based on an agreement between the Acting Secretary of State and the Secretary of War, and established in May 1919 and headed by Herbert O. Yardley, who is considered as the ancestor of today's National Security Agency.

This bureau was disguised as a New York City commercial code company, but was in fact a small and highly secret unit breaking the communications, forging wax seals and invisible inks, obtaining, decoding and reading the private messages of nearly 20 foreign governments.[3] It is best known for solving ciphers and cracking Japanese codes before the disarmament Conference in Washington in 1921.[4]

1 Talitha Nabbali and Mark Perry, "Going for the Throat: Carnivore in an Echelon World - Part II", *computer law & security report*, vol. 20, 2004, p. 85

2 Ibid.

3 "The man who made Edward Snowden inevitable", *The Eonomist*, December 19, 2015, http://www.economist.com/news/christmas-specials/21683975-man-who-made-edward-snowden-inevitable-black-chamber

4 Ibid.

Although the black Chamber played a critical role in U.S diplomacy, it was eventually terminated by Henry Stimson due to budget considerations, and when he did so, he spoke the most famous phrase ever spoken about codes and ciphers: "Gentlemen do not read other gentlemen's mail".

III. Programs Targeting Both U.S. And Non U.S. Citizens

A. Project SHAMROCK

Founded in August 1945, this espionage exercise[1] considered to be the sister project for Project MINARET, dealt with the accumulation and analysis of all telegraphic data entering into or exiting from the U.S.

This project spied on both foreign sources and U.S citizens, especially those considered "unreliable", like a civil rights leader, an antiwar protestor, opposition figures, diplomats, businessmen, non governmental organizations and senior officials of the Catholic Church.[2]

The Armed Forces Security Agency (AFSA) and then the NSA were giving full access to daily microfilm copies of the whole incoming, outgoing and transiting telegrams; the NSA did the operational interception during which it printed and analyzed more than 150,000 in only a month[3], and gave the disseminated information to the CIA, the DOD and the FBI. No court authorized the operation and no warrants were ever issued.

This clandestine program did not require any special technology; international telegrams were simply turned over to NSA at the offices of three cable companies "RCA Global, ITT World Communications, and Western Union International". When RCA Global and ITT World Communications changed to magnetic tapes in the 1960's, NSA made copies of these tapes and subjected them to an electronic sorting process, which means that the international telegrams of American citizens on the "watch lists" could be selected out and disseminated.

---

1 Bruce Schneier, "Project Shamrock", *Shneier on Security*, December 29, 2005, https://www.schneier.com/blog/archives/2005/12/project_shamroc.html

2 "Context of '1945-1975: NSA's Operation Shamrock Secretly Monitors US Citizens' Overseas Communications'", *history commons*, http://www.historycommons.org/context.jsp?item=civilliberties_106.

3 Bruce Schneier, ibid.

Operation SHAMROCK only became known to the public in May 1975, as congressional critics started to investigate this program which was terminated by the NSA director "Lew Allen". The Senate Intelligence Committee chairman "Sen. Frank Church", who was himself on the watch list, stated at that time that this project was probably the biggest government interception program affecting Americans ever undertaken.

B. Project MINARET

MINARET which extended over than three years, was a program initially intended for drug traffickers and terrorist suspects. However it was twisted at the request of the White House to become a tool for tracking legitimate political activities of U.S citizens.[1]

This highly illegal surveillance project publicly acknowledged in the 1970's[2]; was pursued by the NSA to intercept electronic communications that included the names of predestinated US citizens, including senators, prominent journalists, civil rights leaders, actors and especially the anti- Vietnam War protestors; these messages would be later disseminated by the FBI, CIA, BNDD and the Department of Defense.

Operating between 1967 and 1973, more than 5,925 foreigners and 1,690 organizations and U.S citizens were on the Project MINARET watch lists. These watch lists had no juridical oversight and required no warrants for interception. This led to numerous investigations which ended with the creation of the Foreign Intelligence Surveillance Act that restricted the authority of the NSA and imposed warrants and juridical oversight.

C. UKUSA Agreement

This agreement stated to take shape in the early 1940's, when the British Government asked for the exchange of secret intelligence information and technical abilities with the United States, known as the BRUSA Agreement which connected the signals intercept networks of the U.K Government Communications Headquarters (GCHQ) and the National Security Agency (NSA), and the agreement was officially

1 "Declassified NSA files show agency spied on Muhammad Ali and MLK", *The Guardian*, september 26, 2013, http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk.

2 Joseph Fitsanakis, "Files reveal names of Americans targeted by NSA during Vietnam War", *Intelnew.org,* september 26, 2013, https://intelnews.org/2013/09/26/01-1348/

signed on 5 March 1946.[1] Then the agreement expanded to include Canada in 1948, Australia and New Zealand in 1956, which formed some kind of an intelligence alliance, although the U.S was reluctant to include Commonwealth countries as equals and on occasions blocked intelligence sharing wit them.[2]

At first UKUSA was limited to COMINT matters and collateral material for technical purposes, but then it evolved to include SIGINT matters. Under this agreement, the signatory countries pledged to exchange the collection and analysis of traffic, acquisition of communications, documents and equipment, cryptanalysis, decryption and translation.[3]

Despite the fact that the UKUSA agreement stated that it was specifically targeting foreign intelligence, which is defined "all communications of the government or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act there for, and shall include communications of foreign country which may contain information of military, political or economic value" , however we know now from documents leaked by the whistleblower 'Edward Snowden' that the NSA has been able to retain tremendous amount of information from the other members of the five eyes, about their citizens without their knowledge.[4]

D. ECHELON

It is a surveillance program which consists on a vast network of electronic spy stations located all around the world[5], it was established in the late 1960's and operated by the five signatory states in the UKUSA Security Agreement (Australia, Canada, New Zealand, The United Kingdom and The United States) also known as the five eyes.[6]

---

1 Bryce Clayton, "The Massive Metadata Machine: Liberty, Power, And Secret Mass Surveillance in the U.S. and Europe", *Journal of Law and Policy for the information Society*, 10:3 (2014).

2 Richard Norton-Taylor, "Not so secret: deal at the heart of UK-US intelligence", *The Guardian*, June 25, 2010, www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released

3 Bryce Clayton, ibid.

4 Paul Farrell, "history of 5-Eyes-explainer", The Guardian, December 2, 2013, http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

5 Patrick S. Poole, "ECHELON: America's Secret Global Surveillance Network", Echelon Research Ressources, 1999/2000, http://www.web.archive.org/web/20070202171651/http://fly.hiwaay.net/~pspoole/echelon.html

6 Sebastien-Yves Laurent, *Atlas du renseignement : Géopolitique du pouvoir* (Paris: les presses de science po, 2014), p. 22.

This program aimed at monitoring the military and diplomatic communications of the Eastern Bloc during the Cold War[1], later on in the wake of the fall of the U.S.S.R the pretext given to the continued multi-billion dollar budget was fighting terrorism.[2] But what really happened is that this program evolved to become a global massive system for the interception of private and commercial communications and fax traffic and became subjected to an automated analysis by operating listening stations throughout the world[3], for the advantage of the participatory state economies.

The Guardian newspaper summarized the capabilities of the ECHELON system as "a global network of electronic spy stations that can eavesdrop on telephones, faxes and computers. It can even track bank accounts. This information is stored in ECHELON computers, which can keep millions of records on individuals".[4]

ECHELON was first talked about by an investigative journalist 'Duncan Campbell' in an article in the New Statesman titled " Somebody's listening", in which he described the signals intelligence collecting activities of a program code-named ECHELON. In 1996, another journalist "Nicky Hager" described this program in details in his book 'Secret Power- New Zealand's Role in the International Spy Network'. In March 1999, for the first time in history, the Australian government admitted that the top secret UKUSA agreement was true, which led to a series of investigations made by the European Parliament during 2000, and in May 2001, as the Committee finalized the report about ECHELON, a delegation travelled to Washington to attend meetings with CIA, NSA and DOD officials who cancelled all the meetings. When the report was released, the European Parliament stated that ECHELON was in fact used for interception of communications and public switched telephone networks, in order to enable the participatory countries to gain important economic information and to guarantee a leading position in the commercial markets[5].

1 Claude Delesse, *echelon et le renseignement electronique americain*, (Rennes : Ed. OUEST-France, 2012), p.6.

2 Eliot D. Cohen, *Technology of oppression: preserving Freedom and Dignity in an Age of Mass, Warantless Surveillance* (USA: Palgrave MacMillan, 2014), p. 11.

3 Ibid.

4 James Perrone, "The Echelon Spy Network", *The Guardian*, May 29, 2001, http://www.theguardian.com/world/2001/may/29/qanda.janeperrone

5 Peggy Becker, European Parliament, "Development of Surveillance Technology and risk of abuse of economic information", Luxembourg, December 1999, p7.

On August 3, 2015, for the first time the website 'The Intercept' confirmed that the NSA was using ECHELON under an umbrella program called 'FROSTING' which included another program named 'TRANSIENT'.

According to the leaked documents of 'Edward Snowden' the ECHELON intercept stations used by the United States are located in Brazil, Germany, India, Japan, Thailand, United Kingdom, and United States.

E. Thin Thread

It was a program conducted by the United States National Security Agency during the 1990's using wiretapping and sophisticated analysis of the resulting data. This operational system used a method of encrypting sensitive information to concord with privacy laws by identifying automatically probable threats in suspected phone calls with the employment of an automated auditing system to supervise the process by which the analysts dealt with the data for the sake of preventing misuses.

Initially, this program was developed to scan cell phones, searching for signs of terrorist activity, but then this program aimed at extracting large amounts of personal data about citizens.[1]

Thin Thread had an engine for the analysis of data collected and was able to create a detailed profile of targets drawing an entire overview of their contacts and their habits.[2]

This is why, this program was considered a success, for it combined between the ability of sorting out massive amounts of data and preventing at the same time the penetration into the citizens' private life.

This program was later shut down because of what the director of NSA General "Michael V Hayden" called 'the change in priority' that imposed to go with another program "Trailblazer" which, unlike "Thin thread" didn't respect the privacy of U.S citizens.

---

1 Jay Johnson, "ThinThread allows U.S Government to extract vast amounts of personal data". *the voice of Russia*. January 24, 2013, http://sputniknews.com/voiceofrussia/2014_01_24/ThinThread-program-allows-US-Government-to-extract-vast-amounts-of-personal-data-former-NSA-employee-7099/.

2 Pierluigi Paganini, "ThinThread spy system secretly tested on New Zealand population", *Security Affairs*, May 28, 2013, http://securityaffairs.co/wordpress/14749/intelligence/thinthread-us-spy-system-tested-on-nz.html.

All in all, we noticed that after dealing only with breaking codes and forging wax seals; the mass surveillance programs were targeted towards the interception of communications and the deciphering of e-mails.

We also notice that the National Security Agency is involved with every program, and the expanded authority given to this agency has allowed it to perform even illegal operations that affect both U.S and Non U.S citizens.

Another thing could be concluded, is that the mass surveillance programs conducted by the U.S intelligence agencies are only announced after being disclosed, and contrary to what the U.S Government declares regarding these programs saying that they are targeted against suspected terrorists or criminals, it is obvious that these programs consider every individual as suspect

This leads us to think that the U.S Intelligence Community derailed in one point of its main objectives, instead of focusing on protecting the national security, it shifted to monitoring innocent citizens and considering everyone from politicians to civil rights advocates to ordinary citizens as threats, whereas it turns out to be that these individuals have almost never any sort of link to criminal or terrorist groups.

This ridiculously huge number of surveillance programs for which an incredibly insane budget is dedicated, reflects the bloodthirsty need of the U.S intelligence community and more specifically the NSA to collect all the data about the citizens, even unnecessary one.

If the NSA which was involved in an alliance with several other agencies such as GCQK that possesses incredible spying powers, to conduct massive surveillance programs all around the world, and somehow managed to betray that pact and spy even on its allies, what could it possibly do to spy on defenseless citizens.

What could also be noticed is that in spite of ensuring to their clients that their personal data are perfectly protected from any invasion whether by them or by the governments, the telephone and internet companies have over and over compromised their users' privacy either under the pressure of the intelligence agencies or with their own will in exchange for commercial and financial benefits.

Finally, by establishing all these illegal monitoring programs without getting punished for their unlawful actions, these intelligence agencies have proven over and over that they are conducting these activities in light of either a total absence or a fake presence of oversight.

Conclusion of the Part One

In conclusion, intelligence could be seen as a double-edged sword, it may have positive effects that contribute to the protection of the national security and also the safety of the citizens. However it may also have a negative impact which can be reflected in the exaggerated invasion into people's daily life, capturing every little corner of their privacy, and therefore jeopardizing their rights and liberties.

These surveillance programs have also shown that even the civil rights groups are considered as a tremendous threat on the security of the country, since they are under constant surveillance. This could be a hidden intention aiming at getting everybody in the line.

If these mass surveillance programs have shown anything, it certainly would be that it does not matter if you are innocent or not, suspected of doing something wrong or not, you are either way being monitored, and if you object to that it will only drag more attention to you.

So basically by intimidating citizens, governments and more exactly intelligence agencies can get their way and design surveillance programs as they please and exploit the data as they see fits, and all this under either the blessing of the oversight bodies such as the parliamentary, or their total ignorance.

PART TWO: MASS SURVEILLANCE, INDIVIDUAL LIBERTIES AND U.S NATIONAL SECURITY AFTER 9/11 EVENTS

Introduction

Following the 9/11 attacks, the government made huge efforts in order to establish bigger and more severe mass surveillance programs that intended to detect terrorist plots, and therefore prevents another catastrophe.

These events also contributed greatly in legislating laws and policies that reflected the need to put in place effective measures that aimed at securing the nation, but at the same time diminished a lot of the individuals' rights.

That is why, the 9/11 events are considered as the shifting point that contributed in the emergence of several issues. Among these issues was the controversy sparked between two conflicting groups, the ones that stand up for the civil rights and individual freedoms with the what they bear of human values, and the ones approving mass surveillance activities and accepting to restrict their liberties in exchange for a more secure nation and more stabilized society.

CHAPTER ONE: MASS SURVEILLANCE IN THE U.S AFTER 9/11 EVENTS: MECHANISMS AND LEGAL FRAMEWORK

Mass surveillance activities existed long before the 9/11 attacks. However these crucial and defining events increased the amount of programs conducted by the U.S Government in fear of the occurrence of similar terrorist attacks.

These programs have once again targeted individuals whether inside or outside the country. What also characterized these programs was the fact that they evolved tremendously due to the progress in modern technologies, and with the increase in the mass surveillance programs, legislation had to be established or reformed to conform to the nature of the environment post the 9/11 events, and to meet with the requirements of the surveillance programs.

SECTION I. MASS SURVEILLANCE PROGRAMS AFTER 9/11 EVENTS

Since the 9/11 events, the United States government has dramatically increased the capacity of its intelligence community to gather and investigate data on both foreign and domestic subjects, and to do so the U.S has invested bigger than ever in mass surveillance programs.

These programs were designed to capture every little detail of the individuals' lives, whether by hacking into their computers or intercepting their phone calls, the U.S intelligence community didn't stop at anything to increase security measures.

Once again the programs cited below will be categorized according to whether targeting U.S citizens or both U.S and Non U.S citizens.

I. Programs Targeting U.S. Citizens

A. Stellar Wind

It is the code name for data gathered under the President's Surveillance Program launched in 2001, it was approved by President George W. Bush shortly after the 9/11 events and was revealed at first by William Binney few years after its establishment, and then by Thomas Tamm to the New York Times in 2008.[1]

This program created by the NSA and CIA operates through an extensive data mining of huge database of the communications of the US citizens, their e-mails, financial transactions, internet activity[2], which the NSA called 'contact chaining' that provided the study of the online records of people who communicated with people who communicated with targeted persons.[3]

Stellar Wind, just like other surveillance program after the 9/11 events, was operated under no oversight and required no warrants[4], and because of its extreme secrecy even within the US intelligence community, it proved to be a useless and an effective program.[5]

William Binney, one of the NSA whistleblowers, said that the outset of this program recorded 320 million calls a day, which represented about 73 to 80 percent of the entire amount of the NSA's worldwide intercepts.

The Stellar Wind program was discontinued after an interagency review in 2011, for operational and resource purposes.[6]

---

1 "PRISM and Stellar Wind Programs", *talkleft*, Jun 07, 2013, http://www.talkleft.com/story/2013/6/7/42840/79770/civilliberties/PRISM-and-Stellar-Wind-Programs

2 "Entire Stellar Wind (CIA/NSA 'president's surveillance program') document here", *undercoverinfo*, May 4, 2015, https://undercoverinfo.wordpress.com/2015/05/04/entire-stellar-wind-ciansa-presidents-surveillance-program-document-here/

3 Glenn Greenwald and Spencer Ackerman, "NSA collected US email records in bulk for more than two years under Obama", *The Guardian*, jun 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

4 Tim Cushing, "NSA's Stellar Wind Program was almost completely useless, hidden from FISA Court by NSA and FBI", *Techdirt*, April 27, 2015, https://www.techdirt.com/articles/20150427/11042430811/nsas-stellar-wind-program-was-almost-completely-useless-hidden-fisa-court-nsa-fbi.shtml

5 Joseph Fitsanakis, "Declassified report points to flaws in post 9/11 NSA wiretapping", *Intelnews.org*, April 29,2015, https://intelnews.org/2015/04/29/01-1687/

6 Liz Klimas, "New NSA Spying Info on Project Code Named 'Stellar Wind': Collected Data Akin to a 'Real-Time Map of Your Brain'", *the blaze*, jun 27, 2013, http://www.theblaze.com/stories/2013/06/27/new-nsa-spying-info-on-project-code-named-stellar-wind-collected-data-akin-to-a-real-time-map-of-your-brain/

B. Total information awareness

This program was amended in May, 2003 to Terrorist Information Awareness (TIA), under the initiation of the Information Awareness Office (IAO) led by John Poindexter. This office was established by the Department of Advanced Research Projects Agency (DARPA), a branch of the Department of Defense.

The purpose behind this program was to gather and disseminate huge amounts of data including credit card purchases, airline tickets, and medical records… about every individual in the United States and trace patterns of activity that could lead to terrorists groups.

As a result to the aggressive campaigns against this project, especially from the American Civil Liberties Union, the program was allegedly defunded by Congress and was eventually shut down. But the truth is that this program was only transferred to the Advanced Research and Development Activity (ARDA), a branch of the NSA.[1]

C. Mainway

It is an NSA database that has been working since 2001 but it wasn't known publicly until revealed on May 10 2006 by the 'USA Today'. It includes metadata of hundreds of billions of telephone communications collected through four largest telephone carriers in the United States: AT&T, BellSouth, SBC, and Verizon, in order to extract the duration of the sender and the receiver identity, the call location including GPS data, audio content.

This program is not just a database that stores raw metadata, but a system that also performs data quality, preparation and sorting functions, and then summarizes contacts represented in the processed data, to finally stores the resulting contact chains and provides analysts with access to these contact chains.[2]

1 Eliot D. Cohen, *Op. Cit.,* p. 14.

2 "Section 215 bulk telephone records and the MAINWAY database", *Electrospaces.net*, january 20, 2016, http://electrospaces.blogspot.com/2016/01/section-215-bulk-telephone-records-and.html

The Section 215 of the Patriot Act allows the FBI to compel production of 'business records' that is relevant to a specific terrorism investigation and to share those in some cases with NSA[1]. However, it is estimated that the database of this program contains more than 1, 9 trillion call-detail records of many citizens who have no conceivable link to terrorism[2].

II. Programs Targeting Both U.S. And Non U.S. Citizens

A. Trailblazer

It was a NSA project aimed at developing a capability to analyze information carried on communications network like the internet. This program was chosen over a similar program called THINTHREAD, a cheaper and more respective to privacy conditions program.

Trailblazer's main purpose when it was launched in November 1999 by then the NSA Director Michael Hayden, was to allow he NSA analysts to link the two million bits of information the agency gathers every hour.

After spending more than 1, 2 billion dollars over it, this program was eventually shut down in 2006 because of its budget.

B. Turbulence

It is the NSA's information-technology project established in 2005 but first revealed in 2007 by the "Baltimore Sun" which has for an annual budget 500 million dollars.

Turbulence is a collection of systems that is composed of nine smaller programs such as the Turmoil network surveillance system that feeds the NSA's Xkeyscore database.[3] The Turbulence program that was designed to avoid the maximum possible oversight includes offensive cyber warfare capabilities.

---

1 Kevin Drum, "Washington Post Provides New History of NSA Surveillance Programs", *Mother Jones*, jun 15, 2013, http://www.motherjones.com/kevin-drum/2013/06/washington-post-provides-new-history-nsa-surveillance-programs

2 Ellen Nakashima, "Call records of fewer than 300 people were searched in 2012, U.S. says", *Washington Post,* june 15, 2013, https://www.washingtonpost.com/world/national-security/call-records-of-fewer-than-300-people-were-searched-in-2012-us-says/2013/06/15/5e611cee-d61b-11e2-a73e-826d299ff459_story.html

3 Sean Gallagher, "NSA's automated hacking engine offers hands-free pwning of the world", *Ars technica*, mars 12, 2014, http://arstechnica.com/information-technology/2014/03/nsas-automated-hacking-engine-offers-hands-free-pwning-of-the-world/

The project was criticized in 2007 by the US congress for having the same bureaucratic issues as the Trailblazer project.

C. Tempora

This program first tried in 2008 and established in 2011, is used jointly between the NSA and GCHQ to buffer most internet communications that are extracted from the fiber-optic cables which represent the backbone of the internet to gain total access to vast amounts of internet user's personal data, in order to be analyzed at a later time.[1]

The personal data includes recordings of phone calls, the content of e-mail messages, entries on Facebook and the history of any internet user's access to websites.[2]

According to Snowden's leaked documents in which he called this program "the largest program of suspicionless surveillance in human history", Tempora has two main elements "Mastering the Internet" and "Global Telecoms Exploitation" which are provided thanks to the collaboration with some commercial companies that are alleged to have been paid for their services.

Though it is one of the most effective surveillance tools for intelligence agencies, Tempora violates the fourth amendment and also articles 8 and 10 of the European convention on human rights.[3]

D. Mystic

It is a program operated by the NSA Special Source Operations division to digitally record and gather METADATA of phone calls from many countries since 2009, and by 2011 it was ready to be rolled out at fully capacity[4], but publicly acknowledged in March 2014.

---

1 Esther Kursley, "Briefing paper: Mass surveillance: security by "remote control"-consequences and effectiveness", remote control project, August 2016, p. 2, http://www.oxfordresearchgroup.org.uk/sites/default/files/Mass surveillance briefing paper.pdf.

2 Ewen MacAskill et al, "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, june 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

3 Owen Bowcott,"GCHQ surveillance hearing to begin", *The Guardian,* July 14, 2014, http://www.theguardian.com/uk-news/2014/jul/14/court-gchq-surveillance-tempora-ipt-nsa-snowden

4 "NSA recording '100 %' of another country's phone calls", *Russia Today*, mars 18, 2014, https://www.rt.com/usa/nsa-mystic-retro-leak-630/

Mystic scrapes mobile networks for so-called "metadata" which reveals time, source, and destination of calls.[1] This program performing under the executive order 12333 can gather every single conversation nationwide and stores billions of them in thirty days.

Mystic has also another feature which is called "the call buffer" also know as «retrospective retrieval"[2], which opens a door into the past, allowing the NSA to retrieve audio of interest that was not tasked at the time of the original call.[3] The calls are stored for thirty days in a database named "NUCLEON", during which the NSA can choose to disseminate at any time the content of the calls.

In its defense the NSA said that US citizens are not the targets behind this program. However their calls are incidentally tapped in the process of filtering foreign intelligence services, or criminal targets.[4]

E. Prism

It is a massive clandestine surveillance program also known as US-984XN, established in 2007 in the wake of the passage of the Protect America Act, through which the NSA gathers stored internet communications that were encrypted when they traveled across the internet backbone, by using front doors access to data from at least nine US internet companies including Microsoft in 2007, Yahoo in 2008, Google, Facebook and Paltalk in 2009, YouTube in 2010, AOL and Skype in 2011 and Apple in 2012. A although these companies have denied any participation in this program and have refused allegations that the NSA had a direct access into their user's data.[5]

1 Barton Gellman and Ashkan Soltani, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls", *The Washington Post*, March 18, 2014, 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

2 "NSA recording '100 %' of another country's phone calls", ibid.

3 Ryan Devereaux, Glenn Greenwald, Laura Poitras, "Data Pirates Of The Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas", *The Intercept*, may 19, 2014, https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

4 "NSA recording '100 %' of another country's phone calls", ibid.

5 Esther Kursley, ibid.

Nevertheless, government officials and the leaked slides concerning this program made it clear that the NSA regarded the identities of its private partners as Prism's most sensitive secret, fearing that the companies would withdraw from the program if exposed, since 98% of this program is based on Yahoo, Google and Microsoft.[1]

The existence of this program that cost 20 millions dollar per year was only acknowledged due to the leaked documents of Edward Snowden published by the Guardian in 2013, which showed that the world's electronic communications pass through the U.S.

This program which belongs to the Special Source Operations division of the National Security Agency is known as the number one source of raw data used for NSA analytical reports. According to some materials obtained by the Washington Post, Prism accounts for nearly one in seven intelligence reports.[2]

The actual collection process is done by the Data Intercept Technology Unit of the FBI, which reaches the internet service providers and then sends them to the NSA where they would be stored.

This program was supposed to be operated conformingly with section 702 of the Foreign Intelligence surveillance Act Amendments of 2008, which provides that the U.S citizens won't be targeted. However, any analyst could gain access to the whole data bases with the so-called "reasonable belief" which is known as the 51 percent confidence which leaves much room for error.

Basically, thanks to this surveillance program the U.S intelligence community has a total access to e-mails, videos, voice chat, photos, browsing histories, Microsoft Word documents, social networking details…which is known as data mining.[3]

Even though the US government insists that the data is only gathered with court approval and for specific targets. However, because only little is known about how this program performs and because FISA court works in secret, and doesn't require the government to show any probable cause to believe that the target of surveillance has

1 Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", *Washington Post*, jun 7, 2013, 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

2 Ibid.

3 Eliot D. Cohen,*Op. Cit,* p.20.

committed a crime[1], no one could know whether Prism is violating the constitutional rights of the citizens[2]. This idea is well expressed in the words of "Jameel Jaffer", deputy legal director of the American Civil Liberties Union: "This is a court that meets in secret, allows only the government to appear before it, and punishes almost none of its opinions. It has never been an effective check on government".[3]

Prism remains the most controversial of the warrantless surveillance orders issued by President George W. Bush after the 9/11 attacks.

This figure here below shows that the prism program cooperates with the internet service providers, and extract from them data concerning individuals.

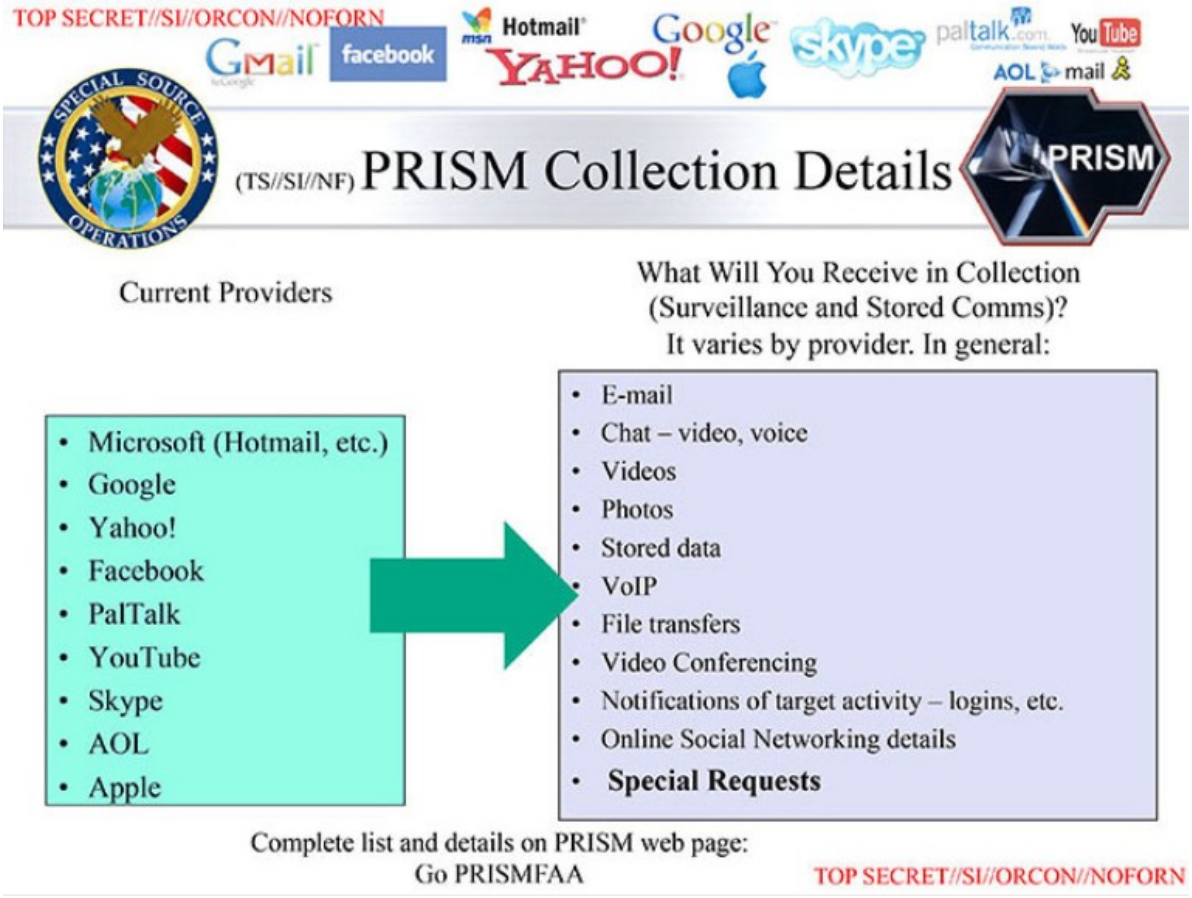

Figure 2: representing the Prism program[4]

1 Timothy B. Lee, "Here's everything we know about PRISM to date", *washington post*, jun 12, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

2 T.C. Sottek and Joshua Kopstein, "Everything you need to know about PRISM : A cheat sheet for the NSA's unprecedented surveillance programs", *The Verge*, July 17, 2013, http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

3 Barton Gellman and Laura Poitras, ibid.

4 Glenn Greenwald, *No Place To Hide: Edward Snowden, the NSA and the Surveillance State* (USA: Pinguin Group, 2014), p. 109

F. Muscular

It is the code name for the program jointly conducted by GCHQ and NSA from undisclosed interception points, which allows them to copy entire data flows across fiber-optic cables that carry information among the data centers[1], and within a month only the NSA copied more than 180 million data sets from the internal networks of Google and Yahoo[2].

Conforming to Edward Snowden's leaked documents, this program which belongs to a collection of other programs like WINDSTOP, works by secretly breaking into the principal communications links that connect the data centers of Yahoo and Google, since they are the two largest internet companies in the world[3], via an access point known as DS-200B in order to infiltrate and mine private data stash.[4] The tapping of these communication fibers provides the NSA with a full access to millions of users' data, including both metadata and content, regardless of whether or not they are were suspected terrorists or criminals.[5]

Once again, both Google and Yahoo denied any involvement with this program, and as a counteract they both planned to encrypt their data to stop the NSA from acquiring access to the users information.

According to the Washington Post, MUSCULAR gathers more than twice as many data points compared to PRISM, and unlike this latter, MUSCULAR does not need a warrant to perform.

The Washington Post reported that this program has proved itself effective for the government, because much of the data mining conducted under this program takes place overseas where the Foreign Surveillance Intelligence Court has no jurisdiction,

---

1 Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, washington post", October 30, 2013, 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

2 Eliot D. Cohen, Op. Cit., p. 24.

3 Marty Biancuzzo, "The Shocking Truth Behind the NSA's "Project Muscular"", *Wall Street Daily,* November 2, 2013, http://www.wallstreetdaily.com/2013/11/02/nsa-project-muscular/

4 Ibid.

5 Ben Hayes, "state of surveillance : the NSA files and the global fightback", *Statewatch*, 2014, p. 2 http://www.statewatch.org/news/2014/jan/state-of-surveillance-chapter.pdf

and also due to the lack of visibility of the method used in this program to tech companies, which allows the NSA to collect huge amounts of data without caring about privacy policies.

G. Dishfire

It is a covert global surveillance collection system and database operated by the NSA and GCHQ in order to gather automatically vast amount of text messages everyday from all around the world and therefore put together detailed reports for these agencies.

This program revealed in 2014, uses an analytical tool named the "Prefer Program", which processes text messages to extract data including contacts, location, financial information, phone number, the sender the receiver, serial number of SIM card, the serial number of the device time and date, detailed meeting information from calendar invites, missed calls, passwords…, and all these data would provide the NSA with a portrait on every user's habits[1].

An agency presentation in 2011, subtitled "SMS Text Messages: A Goldmine to Exploit", stated that Dishfire gathered about 194 million text messages a day in April that year.[2]

H. Marina

It is an NSA database and analysis toolset for intercepted internet metadata, which tracks a user's browser experience, collects content such as IP address, size of e-mail, and then develops summaries of targets. This program has the ability to export the data in a variety of formats[3]; it can even look back on the last year worth of metadata without apparent justification.

1 Josh Lowensohn, "NSA's 'Dishfire' program said to capture nearly 200 million texts a day," *the verge*, january 16, 2014, http://www.theverge.com/2014/1/16/5316178/nsas-dishfire-program-said-to-capture-nearly-200m-texts-a-day

2 James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep", *The Guardian*, january 16, 2014, http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

3 James Ball, "NSA stores metadata of millions of web users for up to a year, secret files show", *The Guardian*, january 16, 2014, http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

I. Upstream

Known as an "umbrella program", Upstream is a collection of programs which includes BLARNEY, FAIRVIEW, OAKSTAR and STORMBREW. These exploitation systems that target about 80% of the telecommunications of both domestic and foreign individuals, intercept massive mounts of international internet traffic by gathering communications on fiber cables and infrastructure as data flows passes by.[1]

The Upstream collection allows access to very high volume of data as a result o the NSA several agreements with internet providers paid in exchange for their services. Under upstream surveillance, an American sending an e-mail or making a video call to someone in another country could have the content of their correspondence gathered by the NSA.[2]

Upstream surveillance is legal under section 702 of the 2008 FISA Amendments Act if it any way relates to national security or foreign affairs, but at the same time violates the internet users' first and fourth Amendment rights.[3]

J. Xkeyscore

Referred to by the NSA as its "widest-reaching" program[4], Xkeyscore previously considered as a secret computer system used by the NSA in order to collect and analyze global internet data on a daily basis, came into light for the first time thanks to the leaked documents of Edward Snowden in 2013.[5]

1 Eliot D. Cohen, Op. Cit., p. 20.

2 "An 'Upstream' Battle As Wikimedia Challenges NSA Surveillance", *National Public Radio*, march 15, 2015, http://www.npr.org/2015/03/15/393190252/an-upstream-battle-as-wikimedia-challenges-nsa-surveillance

3 Giuseppe Macri, "Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance", *Inside Sources*, october 23, 2015, http://www.insidesources.com/federal-court-dismisses-aclu-wikipedia-case-against-nsas-upstream-surveillance/

4 Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", *the guardian*, july 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

5 Ben Hayes, *Op. Cit*., p. 2.

The Xheyscore database is fed a constant flow of internet traffic from fiber optic cables that make up the back of the world's communication network.[1] This program first revealed by the Guardian, sweeps endless individual's internet searches, e-mails, documents, usernames, passwords, and also private communications.[2]

Xkeyscore is a complicated system which consists of a series of user interfaces, backend databases, more than 700 servers at about 150 sites and software that chooses certain kinds of data and metadata. Since only 2008, this surveillance program boasted about 150 field sites in the United States, Mexico, Brazil, Australia, and several other states.[3]

This program is a surveillance tool that builds a searchable database of both metadata which is stored for thirty days and communications content which is stored for one day, gathered from around the world by collecting data from many sources.[4]

Xkeyscore can even conduct broad surveillance on persons according to certain perceived patterns, such as location or nationality or visited websites.[5]

In an interview on January 26, 2014, Edward Snowden described the capacity of XKEYSCORE as it follows:

"You could read anyone's email in the world. Anybody you've got email address for, any website you can watch traffic to and from it, any computer that a individual sits at you can watch it, any laptop that you're tracking you can follow it as it moves from place to place throughout the world. It's a one stop shop for access to the NSA's information. And what's more you can tag individuals using XKEYSCORE. Let's say, I saw you once and I thought what you were doing was interesting or you just have access that's interesting to me, let's say you wok at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I

1 Cale Guthrie Weissman, "It turns out the NSA was collecting voice calls, photos, passwords, documents, and much more", *Business Insider*, july 1, 2015, http://www.businessinsider.com/nsa-xkeyscore-surveillance-program-details-revealed-in-new-snowden-documents-2015-7

2 Morgan Marquis-Boire, Glenn Greenwald, Micah Lee, "XKEYSCORE: NSA's Google for the World's Private Communications", *The Intercept*, July 1 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

3 Ibid.

4 Joe Kloc, "The definitive guide to NSA spy programs", *the daily dot*, august 14, 2013, http://www.dailydot.com/politics/nsa-spy-prgrams-prism-fairview-blarney/

5 Morgan Marquis-Boire, Glenn Greenwald, Micah Lee, ibid.

can track associations with your friends and I can build what's called a fingerprint which is network activity unique to you which means anywhere you go in the world anywhere you try to sort of hide our online presence hide your identity, the NSA find you and anyone who's allowed to use this or who the NSA shares their software with can do the same thing"[1]

This surveillance program is considered a 'passive' program, because it listens but does not transmit anything on the networks that it targets. However it can trigger other systems which perform 'active' operations through Tailored Access Operations.

Xkeyscore has indeed succeeded in tracking down many terrorist like 'Shaykh Atiyatallah', an al Qaeda senior leader; however this program has been also operated to spy on non terrorists' targets such as The U.N Secretary General 'Ban Ki-moon' to track down his talking points before a meeting with President Obama.

Even tough it is considered to be a huge violation for the fourth amendment protection against "unreasonable search and seizure", but given the amount of information gained through Xkeyscore, the US government and its surveillance allies, depends on it greatly.[2]

This figure here below demonstrates how the Xkeyscore program extracts and collects data from users' devices.

1 Eliot D. Cohen, Op. Cit., p.p. 21-22

2 Morgan Marquis-Boire, Glenn Greenwald, Micah Lee, ibid.

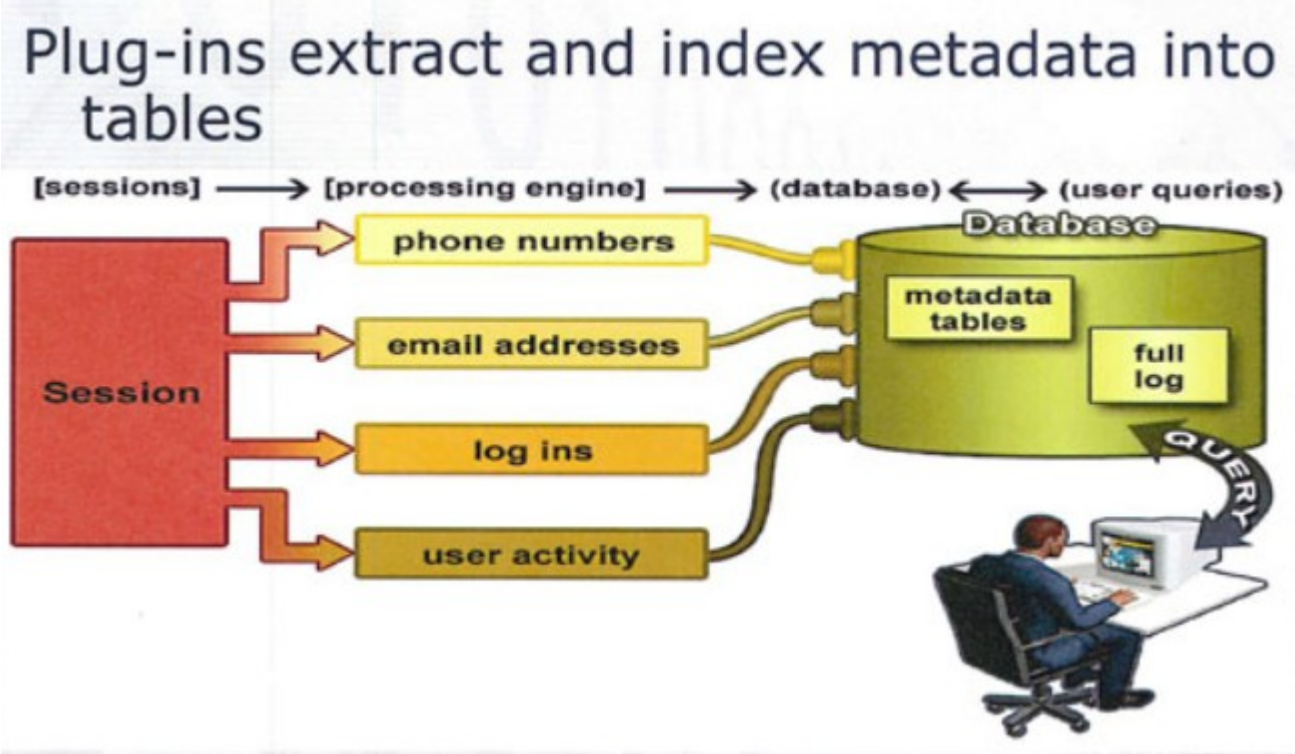

Figure 3: representing XkeyScore program[1]

K. Turbine

It is the code name for an automated system which enables the NSA to covertly hack into computers on a mass scale and reduces the level of human oversight in the process. The Turbine infrastructure which is classified among the Turbulence system allows the current implant network to scale to large size by creating a system that does automated control implants by groups instead of individuals.[2]

This program can automate functions of Turbulence systems to corrupt data in transit between two internet addresses. Since it went online in 2010, Turbine has allowed the NSA to conduct millions of hacking operations.[3]

L. Bullrun

It is a clandestine and highly classified decryption program run by the NSA that uses several sources including computer network exploitation, collaboration with other intelligence agencies.

---

1 Glenn Greenwald, *No Place To Hide*, p. 94.

2 Ryan Gallagher and Glenn Greenwald, "how the NSA plans to infect 'millions' of computers with malware", *The Intercept*, march 12, 2014, https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

3 Sean Gallagher, ibid.

This massive surveillance program is considered to be the second choice for the US Government after failing in placing a back door or to disclose related encryption keys to have an access into the data.[1] According to the documents leaked by Edward Snowden, the NSA has been working under this program that cost 254, 9 million dollars a year, for 10 years.[2]

In order to enforce this program, the NSA covertly influenced tech companies to insert vulnerabilities into commercial products that would allow this intelligence agency access without consumers' knowledge[3]. It is not clear whether these products include online communications services[4], but if this was true, it would mean that the internet companies compromised the guarantees they've given to reassure their consumers.

For the sake of defending their methods, the NSA said that the ability to defeat encryption is crucial to all of their counter-terrorism and foreign intelligence operations.[5]

M. Boundless Informant

First revealed on June 8, 2013, Boundless Informant is a huge analysis and data visualization tool used by the NSA in order to organize and index the data by country or program.[6] This data mining tool provides its operator a graphical insight by detailing and mapping the enormous amount of information it gathers from computer and telephone networks in each country and the methods used in the process.[7] According to a snapshot of a Boundless Informant heat map, the NSA gathered 97 billion pieces of intelligence from computer networks worldwide in March 2013 alone.

---

1 Pierluigi Paganini, "NSA Bullrun program, encryption and false perception of security", *security affairs*, september 7, 2013, http://securityaffairs.co/wordpress/17577/intelligence/nsa-bullrun-program-false-perception-security.html

2 Ben Hayes, *Loc. Cit*.

3 Ryan W. Neal, "Edward Snowden Reveals Secret Decryption Programs: 10 Things You Need To Know About Bullrun And Edgehill", *International Business Times*, september 6, 2013, http://www.ibtimes.com/edward-snowden-reveals-secret-decryption-programs-10-things-you-need-know-about-bullrun-edgehill

4 Dan Auerbach and Kurt Opsahl, "rucial unanswered questions about the NSA's Bullrun program", *Electronic Frontier Foundation*, september 9, 2013, https://www.eff.org/fr/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program

5 James Ball, Julian Borger and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", *the guardian*, september 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

6 Ben Hayes, *Loc. Cit*.

7 Glenn Greenwald and Ewen MacAskill, "Boundless Informant: the NSA's secret tool to track global surveillance data", the guardian, jun 11, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

The amount of mass surveillance programs operated by the law enforcement agencies after the 9/11 events reached an incredible rate. This proved that mass surveillance became more dragnet, aggressive, and ubiquitous as a result to the enhancement of technologies.

These surveillance methods captured literally every detail of the citizens' lives, making of privacy just an illusion. Virtually everything one communicates through any traceable device, or any record of one's existence in the electronic sphere, which these days is everything, will become the property of the government to deal with as it sees fit.

SECTION II. THE LEGAL FRAMEWORK OF MASS SURVEILLANCE IN THE U.S.

The 9/11 events were a defining, apparent and crucial moment in the U.S history, so crucial that it is still being felt until the present day. Proof of this is the huge amount of laws and executive orders passed to strengthen U.S National Security, and to launch the so called 'Global War on Terrorism'.

Nevertheless, the US Government was criticized for compromising and sacrificing civil rights and individual liberties during the process.

I. Acts

A. The USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)

It is an Act of Congress, signed by President George W. Bush on October 26, 2001 in response to the 9/11 attacks, expanding the definition of terrorism to include domestic terrorism, and legislating grants law enforcement and intelligence agencies more authority to detain and question suspects for longer periods.[1]

Several legal challenges were raised towards this act that minimized restrictions that were placed on law enforcement agencies and provided them with greater abilities to search phones, e-mails, and all kind of records, to detain and to deport in secret without providing a probable cause and with no need for a warrant...[2]

1 encyclopedia of espionage, intelligence and security, ibid., sv. "patriot act".

2 Shun-Jie Ji, "Civil liberties vs. national security: lessons from september 11th attacks on america", p. 141, http://www2.tku.edu.tw/~ti/Journal/8-2/824.pdf

The provisions included in the USA Patriot Act consist of measures that aim at enhancing domestic security against terrorism and surveillance procedures. For instance, this act expands the ability of the government in both anti-terrorism and routine criminal investigations to use so called "sneak and peek" and "black bag" secret searches without the individuals' knowledge or consent, which means that citizens could have their cars, houses, and offices searched without even realizing that.[1]

Under this act, the government could also designate advocacy groups like "Greenpeace" as terrorist groups and subject them to invasive surveillance, wiretapping, harassment. In addition to that, the government may monitor federal prison jailhouse conversations between attorneys and clients and deny lawyers to US citizens accused of crimes, the government could even jail anyone without a trial.[2]

Another controversial section in this act is section 215 which allows the government to store bulk of metadata. This generates risks to public trust, personal privacy, and civil liberty[3], and that is because section 215 does not require a showing of probable cause, and also due to the fact that this section is used to obtain records that implicate the privacy interests of persons whose private data are contained in records kept by a third party, which means that for instance if a government obtains a certain financial information about a person from a bank, it is not considered as a violation to the fourth amendment since that person revealed those information voluntarily.[4]

The government explained this section as follows:"One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools is this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States…

---

1 Bryan Johnson, "Top 10 U.S. Government Changes Since 9/11", *Toptenz*, september 7, 2011, http://www.toptenz.net/top-10-u-s-government-changes-since-911.php

2 "The USA Patriot Act: legislation Rushed into Law in the Wake of 9/11/01", *9-11 Research*, http://911research.wtc7.net/post911/legislation/usapatriot.html

3 United States, White House, "liberties and security in a challenging world", december 12, 2013, p. 17, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

4 Ibid., p.p. 82-83.

… By analyzing telephony meta-data based on telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States…In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks"

This implies that service providers have to hand over call records for every phone call made in, from or to the United States, about all their clients on an ongoing basis.[1]

The Patriot Act was extended in 2011 by President Barack Obama, expanding the capacity of the government agencies to gather data about the citizens, however the public didn't know about this expansion until it was revealed by Edward Snowden in 2013.[2]

B. The Homeland Security Act

This 484 pages act that passed on November 25, 2002, described the biggest transformation in the federal government in more than fifty years through the consolidation of over 20 existing federal agencies into a single Homeland Security Department. This consolidation aimed at detecting, fighting against terrorists, and reducing damages by removing data firewalls between government agencies.

One of the most controversial of the Act's provisions was the "Total Information Awareness", which required creating a file about every single American including detailed data on financial, medical and educational records. Later on May 20, 2003 the Information Awareness Office changed the name of the Total Awareness to Terrorist Information Awareness, to indicate that the targets are not US citizens, however the description of the program's activities remained the same.

Even though this program was eventually cut of funding due to its violation to the Fourth Amendment, Congress ruled that some data mining technologies may be continued.

Another disputed provision under this act states that it would be illegal to cut government-funded programs if any US jobs will be lost as a result of the cuts.

1 Ibid., p.p. 96-97.

2 Ewen Macaskill and Gabriel Dance, "NSA files decoded: What the revelations mean for you", *the guardian*, november 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

Like any other act after the 9/11 attacks, the Homeland Security Act was strongly refused by civil liberties groups on the grounds that it reduced privacy and increased government secrecy.

However, the intriguing part about this act is its ambiguous origins. Though The American citizens were told that this act was established as a consequence to the 9/11 events, it's known that the US Commission on National Security for the 21 century published under Clinton in 1998 the "Road Map for National Security: Imperative For Change", in which it talked about an independent "National Homeland Security Agency" that would incorporate several US government agencies, which, for the sake of the nation, could work in secrecy.

Vice President Dick Cheney said at that time that the goal behind this was to protect America in a better way, but one might wonder whom he wanted to protect, since this act allowed his highly secretive Energy Task Force of maps of Iraqi oil fields and pipelines, to meet and generate any sort of document in total secrecy.[1]

C. Intelligence Reform and Terrorism Prevention Act of 2004

It is 236 pages Act of Congress, signed by President George W. Bush[2] that incorporated multiple separate titles with different subject issues which included the creation of the position of the Director of National Intelligence[3], the National Counterterrorism Center, and the Privacy and Civil Liberties Oversight Board.

This report released on July 22, 2004, was the most significant legislation affecting the U.S Intelligence Community, since its main goal was to reform some of its missions[4]. For instance, under this act interagency centers were established to foster collaboration and ensure closer coordination by sharing information.[5] This act also aimed at reinforcing immigration security and the border patrol by increasing investigations.[6]

---

1 "The Homeland Security Act: Legislation Predicated on the Official Story of the 9/11/01 Attack", *9-11 Research*, http://911research.wtc7.net/post911/legislation/hsa.html

2 United States, the Congress, "intelligence reform and terrorism prevention act of 2004", *U.S. government publishing office*, december 17, 2004, https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf

3 Ibid.

4 Ibid.

5 Aki J. Peritz and Eric Rosenbach, *ibid.*

6 Bryan Johnson, ibid.

Some believe that the Intelligence Community was more effective before this act that added only more complexity and obscurity to it. One of the arguments given to criticize this reform was the terrorist attack on a Detroit-bound airline in December 2009, which proved that the intelligence community failed to effectively to share and analyze available information.[1]

D. The military Commissions Act

This Congress act signed on October 18, 2006, aimed at redefining the category of unlawful enemy combatant to insert all irregular opposition to US imperialism which could engage in hostilities against the United States.

This act intended to authorize trial by military commission for violations of the law of war, and for other reasons, that resulted of the Supreme Court's decision on Hamdan vs. Rumsfeld, in which it ruled that the combatant status review tribunals as established by the Department of Defense didn't benefit from the protection of the Geneva Conventions; denying them from the right to a speedy trial, considering that such rights do not exist when national security is compromised.[2]

This act gave absolute power to the president to designate enemy combatants and to set his own definitions for torture and gives US officials full immunity from prosecution for torturing detainees and permit, in violation of international law, the use of evidence extracted under inhuman treatment, and also allows the military commissions to hand down death sentences, and all this happened as part of "war on terror".

E. Protect America Act

This act signed by President George W. Bush was passed on August 5, 2007, in order to update the Foreign Intelligence Surveillance Act to provide additional procedures for authorizing certain acquisitions and other purposes.[3]

---

1 United States, The White House, "White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack", January 07, 2010, https://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack

2 "The Military Commissions Act: Legislation Predicated on the Official Story of the 9/11/01 Attack", *9-11 research*, http://911research.wtc7.net/post911/legislation/mca.html

3 Department of Justice, "What is the Protect America Act?", https://www.justice.gov/archive/ll/

Conforming to the other acts, the Protect America Act authorizes massive untargeted gathering of international communications by installing permanent back doors without any court order or a congress oversight.[1]

Under this act, communication service providers are paid to cooperate with the government agencies and can not be sued for divulging their clients' private information.[2]

F. The Homegrown Terrorism Prevention Act

This Homegrown Terrorism Prevention act passed on October 23, 2007, to amend the Homeland Security Act to fight homegrown terrorism and violent radicalization, by establishing a commission that would study the phenomenon of people with radical beliefs who turn into people who would use violence.

This bill intended to broaden the definition of terrorism so that it would encompass several first amendment activities. For example, under this act anti-war activists could be considered as criminals.

The legislation clearly included research from the Rand Corporation, which published a study in 2005 entitled "Tends in Terrorism" that inserted a chapter named "Homegrown Terrorist Threats to the United States". [3]

This act was criticized for targeting civil liberties groups, Muslims and for defining the internet as a weapon. The Homegrown Terrorism Prevention act also came under fire for giving vague definitions for words like extremism and terrorism.[4]

G. Foreign Intelligence Surveillance Act Amendments of 2008

First signed in 1978 and then updated in 2008, this act of Congress was established to intentionally engage in electronic surveillance under the appearance of an official government act, which gives the intelligence community the flexibility and agility it needs to identify and respond to terrorist and other threats.

---

1 "aclu fact sheet on the "police america act"", *Aclu*, https://www.aclu.org/aclu-fact-sheet-police-america-act

2 "What is the Protect America Act?", *Rupture Ready*, https://www.raptureready.com/faq/faq737.html

3 "The 'Homegrown Terrorism Prevention' Act: Legislation Predicated on the Official Story of the 9/11/01 Attack", *9-11 Research*, http://911research.wtc7.net/post911/legislation/htpa.html

4 Homegrown Terrorism Prevention Act Raises Fears of New Government Crackdown on Dissent, Democracy Now, november 20, 2007, http://www.democracynow.org/2007/11/20/homegrown_terrorism_prevention_act_raises_fears

The FISA act provides the government agencies a statutory framework by which they could collect foreign intelligence information after obtaining authorization to conduct wiretapping by the Foreign Intelligence Surveillance Court.

This act prohibits any individual from illegally intercepting, disclosing, using or divulging phone calls; it also prohibits the individual states from investigating, sanctioning, or requiring disclosure by large telecoms and protects them from lawsuits.

The FISA Amendments requires the government to keep records on surveillance for a period of 10 years and increases the time for warrantless surveillance from 48 hours to 7 days.[1]

Section 702 of this act raised many concerns since it stated that 'No U.S. citizens currently in or out of the country may be "intentionally" targeted. This statement left the possibility for a loophole which could be later on used to justify any targeting against U.S citizens.[2]

The American Civil Liberties Union filed a lawsuit against this act, on the grounds that it may compromised their jobs which rely on private communications.[3]

H. President' Surveillance Program

The President's Surveillance Program is a series of secret intelligence activities authorized by President George W. Bush after the 9/11 attacks, as a part of the War on Terrorism and issued to the Secretary of Defense directing that the signals intelligence capabilities of the NSA be used to detect and prevent future attacks.

This program is unknown for the public; the only section that has been revealed is the one about the warrantless wiretapping of international internet and phone communications of both U.S and non- U.S individuals.

On July 10, 2009, the Inspectors General of all intelligence agencies published a court ordered report showing that the program involved activities that went beyond the scope of the Foreign Intelligence Surveillance Act, which led to the questioning about the legal authorization of this program in addition to the lack of oversight and excessive secrecy.

---

1 Bryan Johnson, ibid.

2 Eliot D. Cohen, *Op. Cit*., p. 35.

3 Bryan Johnson, ibid.

This program raised more controversy when former NSA employee "Bill Binney" revealed that the communications' wiretapping was more widespread domestically.[1]

I. Communication Assistance for Law Enforcement Act

This Congress act was passed on October 25, 1994, and aimed at preserving the capacity of law enforcement officials to operate electronic surveillance programs more effectively by forcing phone companies to redesign their network architectures so that it would be easier for accessibility even with the deployment of new digital technologies.

Then this act was expanded in 2005 by the Federal Communications Commission to include internet service providers and issued a second order on May 2006 asking for broaden facilities to access internet with the help of the internet companies that would cooperate in compliance with this act obligations.[2]

Once again in 2014, the department of justice, the FBI and the Drug Enforcement Administration asked for another expansion that would include more internet providers.[3]

J. The USA Freedom Act: (Uniting and strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act)

This act passed on June 2, 2015, modified many provisions of the Patriot act that had expired the day before. The US Freedom act came to impose boundaries on the bulk collection of the communications metadata on the American population established by the intelligence community under Section 215 of the Patriot act[4], and to concord with the U.S citizens' rights as stated in the Fourth Amendment by placing real restrictions and oversight on the intelligence agencies surveillance authorities.

---

1 Ibid.

2 United States, Federal Communications Commission, "Communications Assistance for Law Enforcement Act", https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

3 The Communications Assistance for Law Enforcement Act (CALEA) of 1994, *Electronic Frontier Foundation*, https://www.eff.org/fr/issues/calea

4 United States, house of representatives, Judiciary Committee, "USA Freedom Act", Chairman Bob Goodlatte, https://judiciary.house.gov/issue/usa-freedom-act/

Some believe that this act fixes at the margins and only deals with one small slice of the mass surveillance, especially that the section 702 under the FISA amendments is still effective until 2017. In addition to that, even if the government agencies are no longer able to intercept communications, they are still capable of collecting metadata which is in a way more effective to them, since it doesn't require a labor-intensive human analysis, even the law is still requiring companies to hold, search, and analyze certain data at the request of the government, and many other aspects of U.S mass surveillance remain unaccountable under this act, including the mass surveillance of populations outside the U.S.[1]

II. Executive And Judicial Orders

A. Secrecy of Immigration Hearings

A memo issued by the Chief Immigration Michael Creppy on September 21, 2001 to all immigration judges demanding the closure of all deportation proceedings to the public and press when directed by the Department of Justice.

B. Attorney-Client Privilege

This regulation established by the Justice department on October 31, 2001, allows prison officials to supervise conversations between detainees and their attorneys without needing a court order, which was illegal before the 9/11 events.

C. Secret Military Tribunals

An order issued by President George W. Bush on November 13, 2001, which authorizes him to effectively decide who will be entitled to constitutional rights and who will not, when being in a military trial that could be held in secret, which no federal, state, foreign or international court is allowed to review.

According to this order, every detainee in the war in Afghanistan was considered as enemy combatant and therefore was not entitled to the Geneva Conventions.

1 "Two years after Snowden :protecting human rights in an age of mass surveillance", *Privacy International*, p. 3, https://www.privacyinternational.org/sites/default/files/Two Years After Snowden_Final Report_EN_0.pdf

D. Domestic Spying: New FBI Guidelines

Announced by Attorney General John Ashcroft on May 30, 2002, these guidelines allow the FBI to monitor any private activity of the citizens, including infiltrating mosques, churches, and gather private data online or from phone calls.[1]

These guidelines also permit the FBI to conduct investigations for a whole year with no need to prove that a crime is being committed.

E. Finger Printing Immigrants from Muslim Nations

Established on August 12, 2002 by the Justice Department. This plan involved providing fingerprints by Muslim immigrants to authorities upon arrival, and whoever fails to do so will face fines or even deportation.[2]

The 9/11 events opened the door for many laws and policies that restrained freedoms and civil liberties more than ever. During this period, terrorism after the 9/11 events became the catch-all phrase used to legitimatize unlawful practices and to justify the violation of several laws.

Though some acts declared that they were only targeting Non U.S citizens, they turned out to search through everyone's data; they even compelled tech companies to give personal information about their clients.

Basically after the 9/11 attacks, everything became permitted for the intelligence community to search through a pile of communications which may have been incidentally or accidentally collected without a warrant.

The changes resulting the 9/11 events demonstrate that after this period of time everything became legal and authorized, even the most unlawful actions became allowed and justified and were found perfectly reasonable in the light of an oversight looser than ever.

---

1 "Executive Orders: The Post 9/11/01 Attack on Civil Liberties Through Executive and Judicial Orders", *9-11 Research*, http://www.911research.wtc7.net/post911/executive/index.html

2 Ibid.

The mass surveillance programs conducted by the U.S Intelligence Community after the 9/11 attacks gathered literally every little data about everyone inside or outside the country, and the revealed programs are just the tip of the ice burg and if it wasn't for the disclosures of several whistleblowers, people would never even know about this collection of programs.

The insane part of these programs is that some of them stated that even in times of economic step backs, these programs had to be funded even at the expense of the society's welfare. And what is even more disturbing is that the bills of some of these acts existed long before the 9/11 events, which could only mean that they were only a pretext to enlarge the intelligence community's authorities.

CHAPTER TWO: THE DIALECTICS OF NATIONAL SECURITY AND INDIVIDUAL LIBERTIES

The 9/11 events have contributed heavily in sparking the controversy between those objecting to mass surveillance abuses in the name of protecting Individual Rights and Freedoms, and those defending mass surveillance activities for the sake of the National Security.

The never-ending debate has been in the core of local, regional and international legislations, which handled important matters such as the right to have a private life, the necessity to safeguard the national security (ect), and between defending the most fundamental rights an individual could enjoy, and securing the nation, the answer never seems to be clear.

Section I. Individual Liberties as a Boundary for Mass Surveillance

Following the 9/11 events, surveillance which is growing since then by leaps and bounds, became paramount to security.[1] Intelligence agencies have made of mass surveillance an everyday activity.

The message sent by the U.S Government was clear: in order to preserve the way of life in the land of the free, freedom had to be curtailed[2]. By saying that it appears as if freedom became a problem that had to be managed rather than a fundamental right[3], and liberties became regarded as optional.[4]

Since then, the public has gained conscience about the increasing surveillance systems that collected tremendous scale of information held by governments which don't always consider their interests as priorities, especially during a time when technology is raising more and more privacy concerns of individuals who are not

1 David Wright et al, sorting smart surveillance", *Computer Law & Security Review*, 26:4, (july 2010): p. 343

2 John Kampfner, *Freedom for Sale: How We Made Money and Lost Our Liberty* (Great Britain: Simon & Schuster, 2009), p. 228.

3 Ibid., p. 263.

4 Ibid., p. 262.

suspected of having any links to terrorism or other forms of crimes[1], whereas surveillance should only be allowed on the basis of a probable cause which makes an individual worthy of attention followed by judicial authorization for any intrusive procedures, and not based on speculations [2].

I. Challenges To Individual Liberties Posed By Mass Surveillance

Surveillance challenges the most fundamental rights and liberties that individuals could enjoy, their dignity and autonomy,[3] their right to protest, their right to association, and their right to free speech. Since the state keeps records on those who confess in public to a certain belief, or who choose to associate with those who are considered to be a threat by the state; this will lead citizens to disincline from engaging in these legitimate activities, and these are the « chilling effects »[4] that influence eventually the way the individuals behave, think and associate with others.

Another right is consequently violated due to mass surveillance, which is the intellectual ownership of the data[5], publishing their data online does not mean that the right holders have waived his right or given their approval to use their information[6] for other reasons than those for which they were published[7], especially that the copyright protection comes into existence automatically as soon as the work is made available and does not require any registration, which means that e-mails, communications, and pictures posted online; are all protected under copyright. And like copyrights, the use of databases; which refer to a collection of independent data arranged in a systematic way and are individually accessible by electronic or other means, can only be used on the grounds of both explicit and implicit licensing, therefore the right holder's permission[8].

1 Esther Kersley, Op. Cit., p. 2.

2 Ben Hayes, Op. Cit., p. 7.

3 David Wright et al, "Questioning surveillance", *Computer Law & Security Review*, 31:2, (April 2015): p. 282.

4 Kevin Macnish, University of Leeds, UK, Surveillance Ethics

5 Colette Cuijpers, "Legal aspects of open source intelligence – Results of the VIRTUOSO project", *Computer Law & Security Review*, 29:6, (December 2013): p. 642.

6 Ibid., p. 647

7 Ibid., p. 646

8 Ibid., p. 648

A. Privacy as the most threatened human value

In addition to the previous rights jeopardized because of the use of ubiquitous surveillance, the most controversial and disputed is the right of privacy which was defined in the United Nations General Assembly report of 2014 as :(the presumption that individuals should have an area of personal autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals)[1].

Privacy in the informational context is defined as the state of not sharing one's private information which includes physical and mental aspects. And there is often a difference between one's public persona which involves what the individual wants to reveal in front of others, and one's private self. For instance, a person may seem in the presence of others as a caring individual, when in fact he's a selfish one.[2] Privacy can also be seen as a moral right, meaning that individuals have a morally justified claim that others don't gain access to their private information without their informed knowledge.[3]

Privacy as a concept has always captured the attention of many legal commentators, philosophers and many others. Warren and Brandeis were perhaps the first to advocate the recognition of the right to privacy among legal commentators at the end of the 19 century, conceiving it as the right to be left alone, an important tool to combat the intrusion of privacy by newspapers[4], by considering that stealing someone's privacy was a crime of a deeply different nature than the theft of a material belonging.

US Supreme Court Justice Louis Brandeis said once again in the case of Olmstead v. U.S.: "the makers of our constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans

1 The United Nations, General Assembly, "Promotion and protection of human rights and fundamental freedoms while countering terrorism", september 23, 2014, http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

2 Eliot D. Cohen, *Op. Cit.,* p. 2.

3 Ibid., p. 3.

4 Sophie Stalla-Bourdillon, Joshua Phillips, Mark D. Ryan, *Privacy vs. Security*, (Berlin: Springer, 2014), p. 6

in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be left alone, the most comprehensive of rights and the right most valued by civilized men".[1]

In 1967, the concept of privacy was handled by Katz v., who considered surveillance as a violation to the fourth amendment. Then in 1972 Eisenstadt v.Baird related the right to privacy with the right to make important decisions without government's intervention. And in 1975, Judith Jarvis Thomson argued that the right to privacy includes a number of other rights such as the right to property and the right of the person, and therefore the violation of someone's privacy only happens when his other rights are being violated.

B. Privacy in the core of legislations

Privacy could also be understood as a legal right, which is enshrined in laws and constitutions as illustrated below.

The Bill of rights, or the first ten amendments to the constitution passed by the Congress, which represents a list of some basic protections to which all Americans are entitled[2]. Among these amendments the ones that focus on the right to privacy are, the first one, which preserves the right of free speech, the fourth amendment which clearly states that:"the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"[3] , and the fifth amendment which provides for due process under law.

Then in 1948, The Universal Declaration of Human Rights dealt with the concept of privacy in the article 12 stating that "No one shall be subjected to arbitrary interference with his privacy"[4]

1 Courtney Bowman et al, *The Architecture of Privacy: on engineering technologies that can deliver trustworthy safeguards*, ed. Elissa Lerner *(USA:* O'REILLY, 2015), p. 6.

2 Stephen Currie, *How Is the Internet Eroding Privacy Rights?* (USA: incontrevercy, 2014), p. 11.

3 Glenn Greenwald, *No Place To Hide*, p. 10

4 Courtney Bowman, Op. Cit., p. 4

Once again the rights to privacy and personal data protection are both embedded as fundamental human rights in articles 8 of the European Convention on human rights[1]. The article 8 stated that:

1-Everyone has the right to respect for his life and family life, his home and his correspondence.

2-There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[2]

In addition to the previous legislation, the right of privacy was dedicated in article 17 of the international covenant on civil and political rights, which clearly states:

- No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation.
- Everyone has the right to the protection of the law against such interference or attacks.[3]

As for the paragraph number eight of the General Comment No.16: Article 17 adopted by the UN Human Rights Committee in April 8, 1988, that even in case of interference with the provisions mentioned in article 17 of the covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be allowed.[4]

Even during times where threats like terrorism had reached their peak, privacy always remained in the core of laws and policies. For example, on 9 March 2004, the European Parliament declared that any kind of mass surveillance wasn't permitted,

1 Colette Cuijpers, ibid., p. 644.

2 Sophie Stalla-Bourdillon et al., ibid., p. 9

3 United Nations, office of the high commissioner for Human Rights, "International Covenant on Civil and Political Rights", http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

4 UN Human Rights Committee, "The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", 8 april 1988, http://www.refworld.org/docid/453883f922.html

except when targeting specific individuals based on reasonable suspicion with the respect to appropriate safeguards such as the requirement of search warrants or court orders.[1]

The United Nation's General Assembly stressed once again on the importance of privacy in its sixty ninth session by releasing a report in September 23, 2014, under the title of "Promotion and protection of human rights and fundamental freedoms while countering terrorism" , which examined the impact of modern technologies on the evolution of digital mass surveillance, and the use of this latter to fight terrorism and other forms of crimes, which should only be conducted against suspected individuals on the basis of a prior judicial or executive authority, and shouldn't be exploited for other purposes such as inspecting every communication made by all users. [2]

C. The importance of privacy in the individuals' lives:

All the cited above laws and studies dedicated to protect the individuals' private life against any unreasonable invasion or interference have shown that privacy is a crucial element in the development of our personal identities; it is the most important part of what it means to be a free individual, it generates the feeling of being safe in public, knowing that our weaknesses are not exposed, it is the intimate sphere of existence which must be concealed from the knowledge of other people and shielded from their curiosity[3]because it includes things about our selves that we don't want to share with others, and if we lose this space of privacy, anything embarrassing or disputed in our private lives becomes a weapon that might be exploited against us[4], and our most personal decisions become submitted to the manipulation of politics, media, business…[5]

1 Marie-Helen Maras, "The social consequences of a mass surveillance measure: What happens when we become the 'others'?", *International Journal of Law, Crime and Justice*, 40:2 (April 2012), p. 65.

2 "Promotion and protection of human rights and fundamental freedoms while countering terrorism", ibid., p. 4-6

3 European Parliament, "development of surveillance technology and risk of abuse of economic information", vol. 1, December 1999, http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf

4 Ben Woodfinden, "Government Sponsored Blackmail? : Mass Suveillance and the threat to Persona Privacy",*Canadian Student Review*, (Winter 2016), p. 18

5 Eliot D. Cohen, *Op. Cit.,* p. 2.

That's why privacy is vital for the individual's liberty because people completely change their behavior when they know that they are being watched. Trying to avoid shame and embarrassment, they stay within imposed boundaries[1] and only when they know that no one is watching them, that they feel free to experiment limits, to explore new ways of thinking[2].

II. Issues Posed By Mass Surveillance

By conducting their mass surveillance programs, the governments have unlimited access to our personal data without any specific suspicion and without giving any regard for the most fundamental rights of any constitution[3]. And once this private data about the citizens is collected, it will be stored forever.

Government defend themselves by saying that all they conduct is a "bulk collection" which doesn't interfere with anyone's right to privacy, but what they don't declare is that these mass surveillance programs gather everything, mine it, take advantage of it, build portrays about individuals from what they say, who they talk to, when, where, by starting from the fact that everyone is a suspect.[4]

Bruce Schneier explained metadata in a simple way. Imagine if you hired a detective to eavesdrop on someone, he would plant bugs in that person's house, and give you a detailed report about his conversations. Now imagine if you asked the detective to put the person under surveillance, he would tell you with whom he spoke, for how long, where, and that's largely enough to know a lot about a person.[5] So basically, the aim of the NSA's massive surveillance is as captured in their disclosed presentations:"collect it all", "know it all", "exploit it all".[6]

Another side-effect of these surveillance programs is that many detainees were subjected to coercive interrogations, and many were not advised of their right to retain an attorney, many had their personal property confiscated and not returned, many were being investigated not because of certain evidence of wrongdoing but on the basis of

1 Glenn Greenwald, *no place to hide*, ibid., p. 164

2 Ibid., p. 165

3 Sigmar Gabriel, "How NSA Spying, Google and Chlorinated Chickens Are Pitting Germans Against Americans—And What to Do About it", *New Perspectives Quarterly*, 32:1 (january 2015), p. 49.

4 "Mass Surveillance", Privacy International, ibid.

5 Bruce Schneier, *Data and Goliath*, p. 20.

6 Ibid., p. 50.

their racial or religious background[1]. Though The statement issued by the United Nations High Commissioner regarding the Guantanamo detentions clearly gives the right to the protection of international human rights and humanitarian law, especially those concerning the provisions in the Covenant on Civil and Political Rights and the Geneva Conventions of 1949, to all detainees[2], the U.S. Government considered those detainees not as prisoners of war, but as enemy combatants[3], which denies them from these rights.

III. Local, Regional, And International Reactions Towards Mass Surveillance Abuses

In response for the abuse of these outragous programs operated by the governments, a series of national, regional, and international bodies and experts opposed to mass surveillance programs, which they considered as violations to individual liberties. For instance, the President's Review Board of December 2013 judged that the government should not be allowed to gather and store personal data about individuals to enable future queries. This review was later on studied By the UN General Assembly which found that interception of communications has a negative influence on human rights activities. Another report from the Privacy and Civil Oversight Board accused the bulk collection of being a huge violation for the Electronic Communications Privacy Act and also the fourth Amendment. Another body that found the mass operations to be extremely indignant to human rights was the European Parliament Committee on Civil Liberties, Justice and home affairs, arguing that terrorism shouldn't be a pretext to justify mass surveillance. The UN High Commissioner for Human Rights also said in report written in July 2014 under the title of "The right to privacy in the digital age", that mass surveillance interfered with the right to a private life, this was reinforced by the UN Special Reporter on counter-terrorism and human rights in October 2014, in April 2015, the Parliamentary Assembly of the Council of Europe adopted a resolution in which it was stated that "The surveillance practices disclosed so far endanger fundamental human rights, including

1 Shun-jie Ji, Op. Cit., p. 146.

2 Shun-jie Ji, Op. Cit., p. 145.

3 Ibid., p. 147

the rights to privacy, freedom of information and expression, and the rights to a fair trial and freedom of religion…these rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law"[1].

The UK House of Lords stated that the expansion of the mass surveillance programs are directly affecting personal privacy and individual freedom, therefore they recommended that this negative impact should be taken into account before conducting any surveillance activity.[2]

As for the national reactions, in UK for example, the Investigatory Powers Tribunal ruled in February 2015 that intelligence sharing between UK and US was unlawful. In the US, the US Court of Appeals for the Second Circuit ruled in favor of the American Civil Liberties Union, considering mass surveillance to be unauthorized under the section 215 of the Patriot Act. Another case ongoing in Canada where a lawsuit was filed against the Canadian signals intelligence by the British Columbia for Civil Liberties; accusing it of being unconstitutional. In Australia and New Zealand , the Inspector-General of Intelligence and Security investigated in the spying actions of both countries.[3]

Even the tech companies involved in mass surveillance programs, have publicly spoken out against US mass surveillance programs to reform the laws underpinning bulk data collection, since these dragnet activities have shaken the trust of their clients in them. For instance, Microsoft, Facebook, Yahoo, and Google had filed a lawsuit in the USA asking to be able to reveal how many times they were compelled to cooperate with the US Government under the FISA Act; this request was granted in February 2014. These companies launched in December 2013 the reform Global Government Surveillance Coalition, in which they urged the US Government to sin the USA Freedom Act. This Coalition was broadened in March 2015 to include privacy advocates and human rights groups[4] asking for an effective, transparent and clear bulk collection permitted only under legal authorization.

1 "two years after Snowden : protecting human rights in an age of mass surveillance", *Privacy International*, June 2015, p. 8. https://www.privacyinternational.org/sites/default/files/Two Years After Snowden_Final Report_EN_0.pdf.

2 David Wright, "Sorting out smart surveillance", ibid., p. 348.

3 "two years after Snowden", ibid., p. 9

4 ibid., p. 16

In addition to the legal reforms, many companies worked to increase the default security and encryption provided to users on their platforms and services; such as Apple and Whatsapp. [1]

Polls also have shown the public's refusal against the mass surveillance programs. An international poll commissioned by Amnesty International in February 2016, which questioned 15,000 people from 13 countries across every continent, found that 71 percent of people are strongly opposed to their governments spying on their internet and phone communications[2].

Another poll was made by Fox News in 2013 showed that forty-five percent of respondents said that they are not willing to give up their liberties to fight terrorism.[3]

IV. Defending Individual Liberties

If these reactions and the resulting measures taken reflect anything, it would be that the government's exploitation of its authorities broke the social contract between the ruler and the ruled[4], because the use of mass surveillance essentially implies that everyone is considered as a threat by the government which doesn't trust anyone; this consequently leads to the loss of the citizens' trust in their governments[5] , because the public will only return the amount of trust invested in him.

In spite of the abuses resulting from the ubiquitous surveillance imposed on the daily life of all citizens, some people seemed not to mind these unlawful practices invoking all kinds of arguments.

The defenders of mass surveillance usually say that they find these activities acceptable since they are not hiding anything, but would they accept if the government installed cameras in their living room? Would they accept to put a tracking device around their ankle so that these agencies could locate them at all times? Would they accept if someone breaks into their house, read through their files, and snoop through

1 ibid., p. 17

2 ibid., p. 3.

3 Stephen Currie, Op. Cit., p. 9.

4 Shun-jie Ji, *Op. Cit.,* p. 144

5 Esther Kersley, Op. Cit., p. 6.

their personal belongings? The answer is obvious: they would be furious. Why should digital surveillance make them react any differently? The only difference would be that in the latter case, it's happening without their knowledge.

The people who use this argument also say that since they are not doing anything wrong, then these intelligence agencies are probably not watching them, so they don't feel threatened even in the presence of mass surveillance programs. Well, they are right! Of course the government is not going to pay attention to those loyal citizens who don't pose a challenge for the state, those who stay in line. However the real measurement of a society that respects freedom can be illustrated in the manner with which it deals with the opposing groups and people shouldn't kneel to the government so that it leaves them alone. [1]And even if they are not doing something wrong, they are being watched and recorded. Falling under suspicion is enough for these agencies to go back in time and scrutinize every decision they have ever made, everyone they have ever spoken with.[2]

Saying that they are not afraid of these programs because you have nothing to hide, is the same as saying that they don't care about freedom of speech because you don't have anything to say.

Some argue that there is a difference between informational privacy which deals with the gathering, exploitation and disclosure of private information, and the decisional one, which involves the freedom of making decisions about one's body and family. However, if information is really considered as a form of power, then the capacity of keeping information about oneself consequently influences the freedom of thinking and acting and that's why we can't separate informational privacy from decisional one.[3]

1 Glenn Greenwald, *no place to hide*, ibid., p.185

2 Ben Hayes, Op. Cit., p. 1

3 Courtney Bowman, p. 5.

Other people who are pro mass surveillance say that they don't mind it, because this latter prevents crimes. Let's say that a smart criminal would never use a device that could in anyway be traced back to him, he would either steal someone else's phone or buy a burnout phone that can't be tracked down [4]and can easily be thrown away without ever detecting the location of the criminal.

Besides, if these measures that restrain civil liberties were only established in a time of a crisis and as the crisis is solved they would be abolished, then that's perfectly understandable. However a lot of the procedures taken in such times lasted more than expected. For instance in the United Kingdom, the Prevention of Terrorism Acts, which were meant to be temporary provisions, became a permanent statute with the passage of the Prevention of Terrorism Act of 1989.

History also shows that such procedures had a way of spreading; they are first established to fight terrorism, but after that they would be exploited to combat other ordinary forms of crimes. This is called "the risk of mission creep", where measures to combat terrorism become used in other cases. For instance in the United Kingdom Regulation of Investigatory Powers Act initially aimed at fighting crimes and terrorism, but targeted later on minor offences, like detecting neighborhood nuisance.

"In 2005, a White house spokesman responded to the mass surveillance programs conducted under Bush's administration saying that:" This is not about monitoring phone calls designed to arrange little League practice or what to bring to a potluck dinner. These are designed to monitor calls from very bad people to very bad people" [1]. Well one might wonder who these bad people are. Is Martin Luther King considered one of the bad people? Are anti-war activists' bad people? Are civil rights defenders bad people? Even the genuine emergency is no excuse to target people because of their political views[2].

Invoking an external threat to justify the choice of keeping citizens submissive to government's powers is more of a slogan than a real argument, since most of the data collected by the NSA has nothing to do with terrorism. In addition to that, for those

4 Kiril Mitov, "Influence of mass surveillance on business and society", *Robopartans Group*, p. 6, https://robopartans.com/wp-content/uploads/2014/03/MassSurveillance.pdf

1 Glenn Greenwald, *no place to hide*, ibid., p.172

2 Russell A. Miller, *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror* (London: Routledge, 2008), p. 127.

who claim that bulk collection helps in getting information quicker to prevent attacks sooner, in December 2013, an advisory panel stated that preventing the attacks was possible to achieve in a short time through conventional court orders which haven't in any way slowed down the process of preventing attacks[1].

Democratic senators Ron Wyden, Mark Udall, and Heinrich stated in the New York Times: "the usefulness of the bulk collection program has been greatly exaggerated. We have yet to see any proof that it provides real, unique value in protecting national security. In spite of our repeated requests, the N.S.A has not provided evidence of any instance when the agency used this program to review phone records that could not have been obtained using regular court order or emergency authorization."

In fact the bulk collection did nothing to detect the 2012 Boston Marathon bombing, or the Detroit bombing, or the attacks over Brussels or Paris.[2]

Lawrence Wright, the NewYorker's al-Qaeda expert said the following about the C.I.A:"It had a warrant to establish surveillance of everyone connected to al-Qaeda in America. It could follow them, tap their phones, clone their computers, read their e-mails, and subpoena their medical, bank, and credit-card records. It had the right to demand records from telephone companies of any calls they had made. There was no need for a meta data-collection program. What was needed was cooperation with other federal agencies, but for reasons both pretty and obscure those agencies chose to hide vital clues from the investigators most likely to avert attacks"[3]

John Mueller an Ohio State University professor said in 2011, that the number of people who die drowning in the bathtub each year is more than the number of people who die from terrorist attacks[4]. So basically we are restricting our liberties for something which is far from being a frequent threat[5], a risk that is not likely going to happen, and even if it could happen at the rate that the government is claiming, physical values are as important if not less as other values.[6]

1 Glenn Greenwald, *no place to hide*, ibid., p.190

2 Ibid., p. 191.

3 Ibid., p. 192.

4 Ibid., p. 193.

5 Sophie Stalla-Bourdillon et al., *ibid*., p. 72.

6 Glenn Greenwald, op. Cit., p. 195.

Terrorism should never be used as a Trojan horse to justify the use of indiscriminate surveillance on a massive scale[1], and as Benjamin Franklin said in a historical review of Pennsylvania in 1759:"Those that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety".[2]

Now for the ones that claim they don't need privacy, well Glen Greenwald; a journalist in the Guardian responded to that by saying "Only when we are able to do things without external judgment being cast upon us, without external eyes watching, are we able to experiment with new forms of thought and behavior: To explore the realms of dissent, to question and challenge orthodoxy. It is only when we don't fear that people will be judging us and condemning us are we really free to do things, beyond just what conformity requires. It is really the area in which dissent and creativity and exploration reside. And when you take away privacy both at a state and society level or at an individual level what you are really doing is destroying that crucial human opportunity to be able to own one's away from the prying eyes of others decide for one self who one is, who one wants to be, what one wants to think about and you really subject yourself to this monitoring that forces you into a box of conformity and its destructive on the society level and on the individual level as well".[3]

While privacy opponents give every argument in the book to devalue this concept, they protect their own privacy as much as they can. For instance, a lot of people who deny the importance of privacy have passwords on their social media accounts, locks on their doors, sealing on their envelopes, they tell their lawyers, their psychologists, their close friends, what they don't want anyone else to know about. When the Senate Intelligence Committee's chair said that the NSA was only gathering meta data which was not revealing, would officials ever reveal the names of the individuals she contacted? Would they reveal the duration of those communications?[4] Would they give the location of where those calls were occurring? The answer is NO! And why is that? Because that information can say a lot about their relationships, their habits, and could create a whole portrait of their personality. The idea behind that is that privacy is a concept valued by every one of us, even those claiming the contrary.

1 "Promotion and protection of human rights and fundamental freedoms while countering terrorism", ibid., p. 9

2 Shun-jie Ji, *Op. Cit.,* p. 134.

3 Kiril Mitov, Op. Cit. p. 7

4 Glenn Greenwald, *no place to hide*, ibid., p.163

Just because people enjoy their privacy doesn't mean that they are doing something wrong. There are many acts that people need to keep private which are not linked to illegal activities. For example, if someone is getting treatment for a disease, they probably don't want that to be disclosed even if it has nothing to do with a wrongdoing.

Having presented all these arguments, it is safe to say that national security even if in danger should not jeopardy fundamental rights and freedoms for which men have fought throughout history, and the definition of national security given by Walter Lippman in 1943 explains that loud and clear:

"*A nation has security when it does not have to sacrifice its legitimate interest to avoid war, and is able, if challenged, to maintain them by war*".

If we looked at democratic societies as societies where citizens where able to formulate plans for their lives, make their decisions with no pressure what so ever, where there is a distinction between effective or positive freedom where a person could make his own decisions without the interference of others[1]; surveillance is considered to be a threat to the values within these societies, because it endangers one's autonomy that permits people to avoid justifying themselves and their personal preferences[2], since individuals instantly change their behavior when knowing that they are being monitored, and therefore will become unable to develop the subjectivity that makes them unique among others, this will eventually lead to a stereo type society where everyone is alike.

Section II. National Security as a Purpose from Mass Surveillance

"Desperate times call for desperate measures", this proverb sums up the fact that surveillance is sometimes required by the circumstances[3], and one of the most urgent circumstances is safeguarding security and combating crimes.

Among the cases where national security is threatened is when facing a terrorist attack. This threat can destabilize communities, threaten social and economic development, fracture the territorial integrity of countries, and undermine international peace and security.[4] And mass surveillance was one of the requirements needed by the U.S Government to safeguard national security.

I. Mass Surveillance, A Necessary Requirement To Fight Terrorism

The risk of terrorism increased greatly after the 9/11 events, this threat became flexible, adaptable, decentralized, transitional, diversified, easily infiltrated, blended and assimilated into societies. Bottom line terrorists could be anyone and anywhere,[5] and because Intelligence agencies are considered as an important part of the security sector

1 Bryce Clayton, "the massive metadata machine: liberty, power, and secret mass surveillance in the u.s. and europe", *A Journal of Law and Policy for the Information Society* (january 2014), p. 23.

2 Marie-Helen Maras, Op. Cit., p. 75.

3 Kevin Macnish, ibid.

4 "Promotion and protection of human rights and fundamental freedoms while countering terrorism", ibid., p. 14.

5 Marie-Helen Maras, "How to Catch a Terrorist: Is Mass Surveillance the Answer?", *Journal of Applied Security Research* 5:1 (january 2010), p. 26.

in any society, their main functions in the process of fighting the threats challenging the national security and the stability in the country, are to prevent and detect any terrorist activity or plot by collecting as much data as they can[1], for the sake of achieving a greater good and creating more stability in the state, the law enforcement agencies need the haystack to find the needle.

Under these circumstances and as Dick Cheney's doctrine known as "One Percent Doctrine" dictates, if there was even a one percent chance of terrorists getting a weapon of mass destruction, and there has been a small probability of such an occurrence for some time, the United States must now act as if it was a certainty[2], on the grounds that preemptive procedures are justified on the assumption that if the governments wait until the damage is done, then risks will eventually increase.[3]

Thus, for the state to counter-terrorism, it doesn't need the approval or the consent of criminals and those who are considered to be a threat to the country's security, to monitor and collect data about them. So if one is not a criminal, if one has nothing to hide, if one did nothing wrong, there is no reason to oppose data gathering and mass surveillance[4].

Besides, if an individual knows that he's being watched at all times, he will think deeply before engaging in any illegal activity, and if we apply that on the whole society we will eventually prevent crimes. As Ellul once said in 1964: "to be sure of apprehending criminals, it is necessary that everyone be supervised"[5].

The hostile towards the use of mass surveillance programs need to understand that precautionary measures are taken in cases where there is a lack of scientific uncertainty and a possibility of a serious and irreversible harm, and the procedures set in place by the U.S. Government in response to the 9/11 attacks fell into this logic. [6]

---

1 Bert-Jaap Koopsa, Jaap-Henk Hoepmanb and Ronald Leenes, "Open-source intelligence and privacy by design", *Computer Law & Security Review* 29:6 (December 2013), p. 677

2 Marie-Helen Maras, "How to Catch a Terrorist", *ibid*., p. 22.

3 Ibid., p. 24

4 Hagai Bar-El, "Against the collection of private data: The unknown risk factor", *Hagai Bar-El on Security*, august 3, 2012, https://www.hbarel.com/analysis/policy/against-the-collection-of-private

5 Marie-Helen Maras, "The social consequences of a mass surveillance measure", ibid., p. 69.

6 Marie-Helen Maras, "How to Catch a Terrorist", *ibid*., p. 22.

So in pursuance of making the terrorist threat known, to detect it, to make it visible, to conceal its activities and identities[1], taking these measures is inevitable, because the success of these criminal groups depends on the fact that they are unknown to the authorities.[2]

II. Legal Authorities To Conduct Mass Surveillance:

It is within the President's "inherent powers" that extreme measures such as monitoring the population could be justified. The President has congressionally irreducible power to "repel sudden attacks"[3]and the court has often referred to the president as the sole organ of foreign affairs in the circumstances of a genuine national emergency which was created due to the Pearl Harbor attack[4].

It is in times like that, that the President can take immediate action necessary to protect national security, even if the action violates statutory restrictions, which is embedded in the context of "special needs" that often excuse ordinary Fourth Amendment requirements. [5]

Besides, the goal behind safeguarding national security is survival, which without it the other values like freedom could never be preserved, since survival includes the protection of citizens, of the territorial integrity and sovereignty. These agencies are in charge of making the nation safer by providing policy makers and military commanders with timely and accurate intelligence in accordance with numerous legal authorities, such as the executive order 12333[6]

There is also the article 6 of the Internatoinal Covenant on Civil and Political Rights, under which states are obliged to protect their citizens from terrorist threats, by using effective means, and since criminals use devices to communicate, states have no choice but to intercept all communications to prevent these illegal activities.[7]

---

1 Ibid., p. 31

2 Ibid., p. 33

3 Russel A.Miller, op. Cit., p. 122.

4 Ibid., p. 124.

5 Ibid., p. 125.

6 United States, NSA director of Civil liberties and privacy office, "NSA's Civil Liberties and Privacy Protections, for targeted SIGINT activities under executive order 12333", Rebecca J. Richards, October 7, 2014, p. 3. https://fas.org/irp/nsa/clpo-12333.pdf

7 "Promotion and protection of human rights and fundamental freedoms while countering terrorism", ibid., p. 14.

Even after establishing these legislations, terrorism has shown once again that states must take extreme measures to safeguard the nation, even if that means restricting civil liberties. Case in point is the Declaration on Combating Terrorism adopted by the European Council on the 25 of March 2004 right after the Madrid bombings that happened in March 2004, which called for the necessity to increase the security measures, among these procedures the "passenger name record" which examined the personal information of the passenger (visa, passport, communications, movement…). Another directive 2006/24/EC was adopted after the London bombings to search through the data including websites visited, phone calls made and their specific location of all EU citizens by service providers of electronic communications services and communications networks.[1]

III. Defending Mass Surveillance In The Name Of National Security

For those who say that mass surveillance is an obvious breach for the individuals right to privacy, well experts usually speak about two sorts of privacy, the informational one; which deals with the gathering, exploitation and disclosure of private information, and the decisional one; which involves the freedom of making decisions about one's body and family[2]. In this case, if the government is gathering our data, this can't be considered as an invasion of our freedom of thinking, of speaking, and of acting.

Additionally, Data processing usually doesn't involve private or sensitive data, but public and non-sensitive data like car ownership, postal codes…, so metadata does not invade anyone's reasonable expectations of privacy, because it is less intrusive than intercepting the content of communications.

Besides, by using the internet and knowing that it is one of the open sources means, individuals using it have voluntarily forfeited their right to have a private life, especially if the data is not protected by intellectual property rights or to be more specific under copyrights, other parties are free to use it[3].

For those who object to mass surveillance by invoking the fourth amendment, the limits to privacy are hinted in this latter, because not all searches and seizures are unreasonable, and because criminals are not going to shout out loud and declare their

1 Marie-Helen Maras, "The social consequences of a mass surveillance measure", ibid., p. 66.

2 Courtney Bowman et al, op. Cit., p. 5.

3 Colette Cuijpers, op. Cit., p. 647.

unlawful plans, law enforcement agencies should be allowed to infringe on someone's personal data to see if the person is breaking the law. Moreover the fourth amendment was written at a time when technology didn't exist, which technically implies that these searches are not applicable to internet messages and online communications[1].

As for the article 17 of the International Convent on Civil and Political Rights, it is clear that there is no consent on the extent of the right to privacy.[2]

The European legislation on data protection of 1995 does not also apply to processing operations concerning public security, defense, state security and the activities of the state in domains of criminal law[3].

Furthermore, privacy is not endangered by mass surveillance, since only trained employees are allowed to handle individuals' personal data which will not be later exposed to the public.

More than that, the bulk collection conducted by the government has been so stressed on, that it made people forget about such activities operated by private companies known as "data brokers" that gain access to the individuals' data and use them for commercial purposes.[4]And the reason why citizens always blame the government is because these companies even if they exploit their data, they don't have the authority to put them in jail.[5]

What must also be taken into account is that the massive intelligence-collection abilities enjoyed by intelligence agencies come within legal authorities and judicial oversight.[6]

So the right to privacy must not be understood as an absolute right, once an individual is suspected of a wrongdoing; he is instantly subjected to investigations by intelligence or law enforcement agencies.

---

1 Stephen Currie, op. Cit., p. 15.

2 "Promotion and protection of human rights and fundamental freedoms while countering terrorism", ibid., p. 13.

3 David Wright et al., "Sorting out smart surveillance", ibid., p. 350.

4 Robin Simox, *surveillance after Snowden : Effective Espionage in an Age of Transparency* (London: the Henry Jackson Society, 2015), p. 74.

5 Ibid., p. 75.

6 Ibid., p. 72.

Hence, instead of opposing to these programs that were in the first place established to watch over the population in the interest of securing the country, citizens have to cooperate and collaborate with the government to combat terrorism. Considering that terrorists blend in the crowds so that they won't be recognized, the law enforcement agencies have no choice other but to turn to these surveillance methods to tracks them down.

IV. Transparency In Mass Surveillance Activities

Intelligence agencies try as they can to be as transparent as possible by reporting to several entities like the Congress, the Department of Defense, the Department of Justice, the Office of the Director of National Intelligence, the President's Intelligence Advisory Board, and the Privacy, Civil Liberties Oversight Board.

Not to mention the Fair Information Practice Principles (FIPPs) which include principle of Individual Participation implying that the person whose information is being gathered, knows about that process and has the choice to contest against it[1].

Another example that could be given to show how much civil liberties are respected by the intelligence agencies is that the NSA incorporates six major staff organizations responsible for protecting civil liberties and privacy:

-The Office of the Inspector General (OIG): oversees the conduct of intelligence activities and investigates whether or not it interferes with civil liberties and privacy rights,

-The Office of General Counsel (OGC): provides legal advice to the NSA to ensure that all its activities are in accordance with the law, including those regarding civil liberties,[2]

-The Office of the Director of Compliance (ODOC): responsible for achieving reasonable assurance that the missions conform to laws,

-The Authorities Integration Group (AIG): provides a forum for integrating authority-related activities (changes, additions…),

1 "NSA's Civil Liberties and Privacy Protections, for targeted SIGINT activities under executive order 12333", ibid., p. 4.

2 Ibid., p. 6.

-The Associate Director for Policy and Records (ADPR): performs as the privacy advocate, by assessing intelligence activities in accordance with the Privacy Act and the Freedom of Information Act,

-The Civil Liberties and Privacy Office (CLPO): in charge of increasing transparency in NSA's activities, taking into account civil liberties and privacy considerations.[1]

Furthermore, NSA's concerns about the individuals' rights are not only obvious through its civil liberties and privacy program required by the ODNI and DOD[2], but also through its training and education programs that provide employees with the knowledge of the Privacy Act and intelligence oversight[3], each of these employees must take an oath of office to the Constitution that speaks not simply to national security, but to protection of civil liberties and privacy[4].

However, bearing in mind that the law enforcement agencies have a national security mission, people must understand that the principle of transparency is not fully implemented in the same manner in organizations with a more public-facing mission, otherwise foreign intelligence could know all their plans and technologies[5].

That's why secrecy is crucial in the conduct of mass surveillance programs by the law enforcement and intelligence agencies, because if every thing is revealed then the terrorists would know about the methods used by these services to track and catch criminals, and that's the negative side-effect of the disclosures made by Edward Snowden and many other whistleblowers. [6]

Even if these agencies are conducting secretive surveillance activities, people have to understand that it is for the greater good, seeing how not all forms of surveillance are bad, there are some surveillance systems that support law enforcement and don't violate the public interest[7].

1 Ibid., p. 7.

2 Ibid., p. 8.

3 Ibid., p. 9.

4 Ibid., p. 5.

5 Ibid., p. 1.

6 Robin Simox, op. Cit., p. 13.

7 David Wright et al, "Questioning surveillance", ibid., p. 281.

V. 9/11 Events… A National Tragedy

The public has to always remember the eleventh of September 2011, that day when the United States of America became a nation transformed and more than 2,600 people were killed at the World Trade Center[1]; 125 died at the Pentagon; 256 died on four different planes. The death toll surpassed that at Pearl Harbor in December 1941.[2] Do Americans want to wake up to the same nightmare of the 9/11 tragedy? The Americans should remember how they felt on 9/11 to make cooperation easier with the government in order to create a safer world and a better future.[3]

If a person gets to choose between getting killed and having his phone calls intercepted, the choice would be obvious. That's why when faced to terrorism threats; enhancing security measures must outweigh individual liberties. So if giving up a few of our rights and our civil liberties would mean achieving greater personal safety and security, then so be it. The desire to live in a peaceful and orderly society should favor greater tolerance of restrictions on personal freedoms and civil liberties[4], because any push back on surveillance compromises national security.

People must understand that In an uncertain world, driven by the pace of technological development and the transformation in the nature of threats, intelligence agencies and law enforcement services must adapt and adjust to safeguard the national security as rapidly as these events emerge.

These criminal organizations, pose a threat to U.S. citizens as well as U.S interests by potentially penetrating and corrupting strategically vital markets.[5] In order to avoid such catastrophes from happening, these agencies must monitor and conduct surveillance to detect and disrupt violent extremist groups that actively plot to inflict damage or harm to the United States and its citizens[6]. So when it comes to terror attacks, security trumps privacy.

---

1 "9/11 Commission Report", ibid., p. 1.

2 ibid., p. 2

3 ibid., p. 31

4 Darren W. Davis and Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", *American Journal of Political Science*, 48:1 (January 2004), p. 29

5 "The National Intelligence Strategy of the United States of America", ibid., p. 4.

6 Ibid., p. 5.

After having displayed both of the arguments of those favoring national security and those defending civil liberties and freedoms against the abuses of mass surveillance, the idea that comes in mind is that both parties have a point to a certain extent.

On one hand law enforcement agencies need mass surveillance programs in order to safeguard national security, but on the other hand civil rights and liberties have always been in the core of laws and policies, given their importance for human dignity and autonomy.

That is why National Security and liberty shouldn't be odds and don't need to be in conflict, but in fact they must be mutually supportive. The values of privacy and security can not simply be conceived as being in blunt opposition without any possibility of reconciliation. On the contrary, they should be understood as complementary rather than contradictory.

It is crucial to understand the interaction between the protection of privacy and the furtherance of security so that appropriate boundaries are set to surveillance practices, and the best way to balance between them is to implement verifiable measures of accountability that permits citizens to comprehend the degree and the nature of surveillance that is being conducted by the government on a case by case basis.

Conclusion of the Part Two

The fear of terrorism generated by the 9/11 events was exploited by the U.S. leaders to justify a large set of extremist policies, which led to unlawful detentions without any charges, unreasonable seizures and searches, by turning mass surveillance to the most aggressive tool of repression and intrusion ever seen.

Indeed mass surveillance is required under certain circumstances such as terrorist attacks to preserve the nation's security. However if not restricted, mass surveillance can be detrimental to individual liberties; it could chill the exercise of civil liberties like the right to free speech.

If anything could be concluded from these programs, is that the governments are willing to go as far as possible and by any means available to collect and store data about their citizens, even if it means denying them from their constitutional rights. This leads to think that mass surveillance is no longer limited to totalitarian systems but also a feature describing democratic systems.

GENERAL CONCLUSION

Intelligence and mass surveillance have always figured in the history of the United States' Intelligence community giving the significance of both of these activities in increasing the U.S power, in shielding its national security, as well as in protecting its citizens from any occurring or potential harms.

These mass surveillance activities have been established through a series of programs and operations, in which the U.S.A used all kind of techniques that were enhanced greatly due to the technological progress, from intercepting communications to deciphering e-mails to hacking into people's computers, the U.S intelligence agencies have done it all.

The mass surveillance programs have constantly posed several challenges to human rights and individual freedoms. However these threats increased even more after the 9/11 events, and that is because the mass surveillance conducted by the U.S intelligence agencies after this period became more blurred and ambiguous and their methods of gathering data became more aggressive. In addition to that the U.S intelligence services considered everyone as target and a probable suspect, and therefore they monitored people all around the world.

Mass surveillance became an obvious breach of human rights and a mean of domination and a tool of repression used to follow citizens in every move, to hear and record every call they make, to know about every time they send an e-mail, text, call, chat, and even though Americans generally have valued protection from terrorism over civil liberties, still they also have expressed concerns over government overreach on their privacy and that anti-terror policies will go too far in restricting civil liberties, arguing that civil liberties and constitutional rights should not be abused and violated in the name of security, because exposing terrorist plots does not require such mass violation of rights.

State reasons can not justify the intrusion into people's personal life on a daily basis not without their informed approval, and especially when the sacrifice turns out to be unnecessary, considering that the citizens who voted for a certain government and therefore provided it with certain authorities allowing them to make decisions, to introduce certain laws, and even to go to war, as long as there are few restrictions, red

lines that could never be crossed, civil liberties and human rights that will could never be crushed. That's why preserving the right of privacy is an example of society in which there are certain restrictions on the government.

By contrast to what is promoted in the official discourses that these mass surveillance programs are supposed to protect us, by misusing them they become a threat to the rights they were in the first place designed to preserve. If these agencies are using mass surveillance programs to violate citizens' most fundamental rights and to discredit political opponents, then they are not considered as a guardian of their people, but as a danger on their daily lives.

Nonetheless, that does not mean that individual liberties and national security should be in conflict, but in fact they ought to be fundamentally aligned, seeing how if we have no privacy, we feel exposed and vulnerable, we feel less secure, similarly if our private data are monitored and therefore less secure, we have no privacy. That's why framing the debate between security and privacy as a trade-off leads us to misguiding conclusions, we should rather preserve them together. Ronald Dworkin explores this idea further saying that even if there was a possibility for a trade-off, then it should be between our security and their liberty, and by their he was referring to the suspected groups.

The balancing between preserving national security and protecting individual liberties is indeed difficult, however it is not impossible, there are just some measures that must be taken, and one of the most important and beneficial procedures is transparency which is crucial for any open and free society because when decisions are made in the dark, their quality is reduced. If the government is keeping information about its citizens, they should at least know what they are gaining in return and who gets to conduct surveillance activities, in what cases and to what extent so that they could be sure that mass surveillance programs make them safer and guarantee that these agencies are not misusing their personal data, but keeping in mind that transparency should only be applied to a certain extent; otherwise the national security will be compromised if all its secrets are exposed.

In addition to implementing transparency policies, oversight is considered to be a vital element to assure that the power given to the government is not being abused. This question was raised by President Barack Obama in his January 17, 2014 speech on the

NSA surveillance program when he said «in the absence of institutional requirements for regular debate and oversight that is public as well as private or classified, the danger of government overreach becomes more acute".

Even though these agencies pretend that there is already an oversight by the congress, however they have always manipulated the rules governing congressional oversight to ensure that no actual understanding or critical review occurs, for instance the FISA court has a much lower standard of proof before it could issue a warrant; that is why it almost never refuses a warrant order from the NSA.

Oversight as a legislative framework should be adopted by a legitimate representative institution that sets out clear and open terms and this oversight body, such as a committee, must have enough power to obtain information and documents from the government and intelligence agencies, even about the covert activities. Bruce Scheiner said in his book "Data and Goliath" that in 2014 he was invited by six members of both parties of the congress to brief them about the NSA's activities since he had reviewed Snowden's leaked documents, wondering about how democracy could survive if the info came from him.

In order to implement effective oversight measures, some have suggested that the creation of more independent offices such as inspectors general, judicial commissioners or auditors to oversee the operations conducted by the security sector and assure that they concord with the legislation, with statutory authorities to access to data and staff.

Whistle-blowers and journalists could also be considered sorts of oversight mechanisms because they reveal information and disclose wrongdoings regardless of the consequences , that is why there has to be some laws that protect them. However that does not mean that anyone should leak anything he finds.

Among other procedures leading to creating a balance between national security and human rights is accountability, which implies that the government and more specifically intelligence agencies will be punished if they are misusing their authorities. There must not be a sort of impunity that let the government think it is free to do whatever they want.

Cooperates should also contribute in balancing between security and liberty, by giving access to data only conforming with international laws and human rights standards and develop measures to ensure better implementation of the international standards. These cooperates could also enhance awareness of their employees, focusing on their training and education of their responsibilities in handling the personal information of the users. In addition to that, by raising the cost of the privacy breaches, companies will be forced to make more effort to protect our data; in addition these companies could be compelled to comply with policies and laws like the 1973 Code of Fair Information Practices.

National laws should be reformed to concord with international human rights laws and standards, because this way, the government will be compelled legally to respect those conventions, otherwise they will be punished.

The citizens lost their seat at the government's table from the moment that these programs began to be conducted under their names and without their consent. For this reason, an open debate is also required to discuss the boundaries that should limit the government surveillance, through enforcing laws, and routine reports of government actions, and active press, because the more citizens communicate these matters to the government, the more the politicians will be aware that it is an important issue for them. For example they could try the public interest test whenever the government is about to establish a new program. These tests allow the public to gain access to information held by the government, and to participate in a debate, the public view will ultimately be taken into consideration.

We need also legislation that force the government to engage in targeted surveillance to limit the massive data gathering to only collecting the necessary information which only matters in safeguarding the national security.

Among the things ordinary citizens can do, is avoid surveillance; for instance by leaving cell phone home; by avoiding to speak about certain subjects online, by turning location services off on your Smart phone when they are not needed, by putting a sticker over their computer's camera to prevent someone who monitors it remotely from taking pictures of them. They can also learn some privacy enhancing technologies such as encryption to protect their data which is about regulating an authorized access and use of their data.

We are not arguing that the government should completely give up surveillance. Indeed, it is crucial for all states to have means of protecting themselves from foreign attacks. That is why citizens have to help the government surveillance, because as illogical as this could sound, we must admit that the government has to monitor internet activities in order to track down criminals, this way individuals could decide how much they want these agencies to get involved in their personal data.

Achieving security should be moral, preserved in a legal framework, controlled under the supervision of a higher and independent power to which all the parties will be held accountable.

The government control, monitoring and manipulation of the people's deepest and most private beliefs, feelings, and values can transform into an Orwellian reality and nightmare, and since individual liberties have always been the hall mark of the western societies and what distinguished them from dictatorships, then if that is gone, there will be no trace of democracy in this world, because as John Adams once said:"Liberty, once lost, is lost forever".

BIBLIOGRAPHY

Government Documents And Reports

1. "Homegrown Terrorism Prevention Act Raises Fears of New Government Crackdown on Dissent". *Democracy Now.* November 20, 2007. http://www.democracynow.org/2007/11/20/homegrown_terrorism_prevention_act_raises_fears

2. "The Communications Assistance for Law Enforcement Act (CALEA) of 1994", *Electronic Frontier Foundation*, https://www.eff.org/fr/issues/calea

3. "two years after snowden : protecting human rights in an age of mass surveillance". *Privacy International*, June 2015. https://www.privacyinternational.org/sites/default/files/Two Years After Snowden_Final Report_EN_0.pdf.

4. "Two years after Snowden :protecting human rights in an age of mass surveillance". *Privacy International.* https://www.privacyinternational.org/sites/default/files/Two Years After Snowden_Final Report_EN_0.pdf

5. Auerbach, Dan and Kurt Opsahl. "rucial unanswered questions about the NSA's Bullrun program", *Electronic Frontier Foundation*, september 9, 2013, https://www.eff.org/fr/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program

6. Becker, Peggy. European Parliament. "Development of Surveillance Technology and risk of abuse of economic information". Luxembourg. December 1999.

7. European Parliament. "development of surveillance technology and risk of abuse of economic information". vol. 1, December 1999. http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf

8. Hayes, Ben. "state of surveillance : the NSA files and the global fightback", *Statewatch*, 2014, http://www.statewatch.org/news/2014/jan/state-of-surveillance-chapter.pdf

9. The United Nations, General Assembly. "Promotion and protection of human rights and fundamental freedoms while countering terrorism". September 23, 2014. http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

10. The United Nations, office of the high commissioner for Human Rights, "International Covenant on Civil and Political Rights", http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

11. The United States of America, National Commission on Terrorist Attacks, "9/11 Commission Report".

12. The United States of America, the Congress, "intelligence reform and terrorism prevention act of 2004", *U.S. government publishing office,* december 17, 2004, https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf

13. The United States of America. American Army. "Joint intelligence". joint publication 2-0. 22 October 2013. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

14. The United States of America. Department of Justice. "What is the Protect America Act?". https://www.justice.gov/archive/ll/

15. The United States of America. Direction of National Intelligence. "The National Intelligence Strategy of the United States of America". August 2009. https://fas.org/irp/offdocs/nis2009.pdf.

16. The United States of America. Federal Communications Commission, "Communications Assistance for Law Enforcement Act", https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

17. The United States of America. house of representatives. Judiciary Committee, "USA Freedom Act". Chairman Bob Goodlatte. https://judiciary.house.gov/issue/usa-freedom-act/

18. The United States of America. Joint Services Command and Staff College. advanced command and staff course, *strategic intelligence study period*, sep 04 – Jul 05 (N. 8).

19. The United States of America. NSA director of Civil liberties and privacy office. "NSA's Civil Liberties and Privacy Protections, for targeted SIGINT activities under executive order 12333", Rebecca J. Richards, October 7, 2014. https://fas.org/irp/nsa/clpo-12333.pdf.

20. The United States of America. The White House, "White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack", January 07, 2010, https://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack

21. The United States of America. The White House. "liberties and security in a challenging world". december 12, 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

22. UN Human Rights Committee, "The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", april 8, 1988, http://www.refworld.org/docid/453883f922.html

23. United Kingdom. House of Lords. constitution committee. "surveillance: citizens and the state". London, January 21, 2009.

Books

1. Bowman, Courtney , et al. *The Architecture of Privacy: on engineering technologies that can deliver trustworthy safeguards*, edited by Elissa Lerner. USA: O'REILLY, 2015.

2. Clark, Ransom J. *Intelligence and National Security : a reference handbook.* London: Praeger Security International, 2007.

3. Cohen, Eliot D. *Technology of oppression: preserving Freedom and Dignity in an Age of Mass, Warantless Surveillance*. USA: Palgrave MacMillan, 2014.

4. Currie, Stephen. *How Is the Internet Eroding Privacy Rights?.* USA: incontrevercy, 2014.

5. Delesse, Claude. *Echelon et le renseignement electronique americain.* Rennes : Ed. OUEST-France, 2012.

6. Greenwald, Glenn. *No Place To Hide: Edward Snowden, the NSA and the Surveillance State*. USA: Pinguin Group, 2014.

7. Johnson, Loch K. *handbook of intelligence studies*. London : Routledge, 2007.

8. Kampfner, John. *Freedom for Sale: How We Made Money and Lost Our Liberty.* Great Britain: Simon & Schuster, 2009.

9. Laurent, Sebastien-Yves. *Atlas du renseignement : Géopolitique du pouvoir.* Paris: les presses de science po, 2014.

10. Miller, Russell A. *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror.* London: Routledge, 2008.

11. Rosenbach, Eric and Aki J. Peritz. *Confrontation or collaboration: congress and the intelligence community*. USA: Harvard Kennedy School, 2009.

12. Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York: W.W. Norton & Company, 2015.

13. Simox, Robin. *surveillance after Snowden : Effective Espionage in an Age of Transparency.* London: the Henry Jackson Society, 2015.

14. Stalla-Bourdillon, Sophie, Joshua Phillips and Mark D. Ryan. *Privacy vs. Security*. Berlin: Springer, 2014.

15. Tzu, Sun. *the art of war.* translated by Griffith Samuel. New-York: Oxford University Press, 1963.

Journal Articles

1. Appelbaum Jacob, Judith Horchert and Christian Stocker. “Shopping for Spy Gear: Catalog Advertises NSA Toolbox”, *spiegel online,* december 29, 2013.

2. Clayton, Bryce. "The Massive Metadata Machine: Liberty, Power, And Secret Mass Surveillance in the U.S. and Europe", *Journal of Law and Policy for the information Society*, 10:3 (2014), p.p. 481-522.

3. Clayton, Bryce. "the massive metadata machine: liberty, power, and secret mass surveillance in the u.s. and europe". *A Journal of Law and Policy for the Information Society* (january 2014).

4. Cuijpers, Colette. "Legal aspects of open source intelligence – Results of the VIRTUOSO project". *Computer Law & Security Review.* 29:6 (December 2013): p.p. 642-653.

5. Davis, Darren W. and Brian D. Silver. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America". *American Journal of Political Science*, 48:1 (January 2004), p.p. 28-46.

6. Gabriel, Sigmar. "How NSA Spying, Google and Chlorinated Chickens Are Pitting Germans Against Americans—And What to Do About it". *New Perspectives Quarterly* 32:1 (january 2015) : p.p. 48-55.

7. Koopsa, Bert-Jaap, Jaap-Henk Hoepmanb and Ronald Leenes. "Open-source intelligence and privacy by design". *Computer Law & Security Review* 29:6 (December 2013), p.p. 676-688.

8. Maras, Marie-Helen. "How to Catch a Terrorist: Is Mass Surveillance the Answer?", *Journal of Applied Security Research* 5:1 (january 2010): p.p. 20-41.

9. Maras, Marie-Helen. "The social consequences of a mass surveillance measure: What happens when we become the 'others'?". *International Journal of Law, Crime and Justice.* 40:2 (April 2012) : p.p. 65-81.

10. Nabbali, Talitha and Mark Perry. "Going for the Throat: Carnivore in an Echelon World - Part I", *computer law & security report.* vol. 20, 2004.

11. Nabbali, Talitha and Mark Perry. "Going for the Throat: Carnivore in an Echelon World - Part II". *computer law & security report.* vol. 20, 2004.

12. Power, Amanda. “under watchful eyes: the medieval origins of mass surveillance”, *Lapham's Quarterly*, (2012), http://www.laphamsquarterly.org/spies/under-watchful-eyes.

13. Woodfinden, Ben. “Government Sponsored Blackmail? : Mass Suveillance and the threat to Persona Privacy” *Canadian Student Review* (Winter 2016): p.p. 13-19.

14. Wright, David et al. “Questioning surveillance”, *Computer Law & Security Review*, 31:2 (April 2015): p.p. 280-292.

15. Wright, David et al. “sorting smart surveillance”. *Computer Law & Security Review*, 26:4 (july 2010): p.p. 343-354.

Newspapers

1. "Declassified NSA files show agency spied on Muhammad Ali and MLK". *The Guardian.* September 26, 2013. http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-anti-vietnam-muhammad-ali-mlk

2. “NSA recording ‘100 %’ of another country’s phone calls”, *Russia Today*, mars 18, 2014, https://www.rt.com/usa/nsa-mystic-retro-leak-630/

3. “The man who made Edward Snowden inevitable”. *The Eonomist.* December 19, 2015. http://www.economist.com/news/christmas-specials/21683975-man-who-made-edward-snowden-inevitable-black-chamber

4. Ball, James. “NSA stores metadata of millions of web users for up to a year, secret files show”, *The Guardian*, january 16, 2014, http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

5. Ball, James. Julian Borger and Glenn Greenwald, “Revealed: how US and UK spy agencies defeat internet privacy and security”. *the guardian*, september 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

6. Biancuzzo, Marty. "The Shocking Truth Behind the NSA's "Project Muscular"". *Wall Street Daily.* November 2, 2013. http://www.wallstreetdaily.com/2013/11/02/nsa-project-muscular/

7. Bowcott, Owen. "GCHQ surveillance hearing to begin". *The Guardian.* July 14, 2014. http://www.theguardian.com/uk-news/2014/jul/14/court-gchq-surveillance-tempora-ipt-nsa-snowden

8. Devereaux, Ryan, Glenn Greenwald and Laura Poitras. "Data Pirates Of The Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas". *The Intercept.* May 19, 2014. https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

9. Drum, Kevin. "Washington Post Provides New History of NSA Surveillance Programs". *Mother Jones.* June 15, 2013. http://www.motherjones.com/kevin-drum/2013/06/washington-post-provides-new-history-nsa-surveillance-programs

10. Farrell, Paul. "history of 5-Eyes-explainer". *The Guardian.* December 2, 2013. http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

11. Gallagher, Ryan and Glenn Greenwald. "how the NSA plans to infect 'millions' of computers with malware". *The Intercept.* March 12, 2014. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

12. Gellman, Barton and Ashkan Soltani. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". *washington post.* October 30, 2013. 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

13. Gellman, Barton and Ashkan Soltani. “NSA surveillance program reaches ‘into the past’ to retrieve, replay phone calls”. *The Washington Post.* March 18, 2014. 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

14. Gellman, Barton and Laura Poitras. “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program”. *Washington Post.* Jun 7, 2013. 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

15. Greenwald, Glenn and Ewen MacAskill. “Boundless Informant: the NSA's secret tool to track global surveillance data”. *the guardian,* jun 11, 2013. http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

16. Greenwald, Glenn and Spencer Ackerman. "NSA collected US email records in bulk for more than two years under Obama". *The guardian.* june 27, 2013. http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

17. Greenwald, Glenn. “XKeyscore: NSA tool collects 'nearly everything a user does on the internet'”, *the guardian,* july 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

18. Johnson, Jay. “ThinThread allows U.S Government to extract vast amounts of personal data”. *the voice of Russia*. January 24, 2013. http://sputniknews.com/voiceofrussia/2014_01_24/ThinThread-program-allows-US-Government-to-extract-vast-amounts-of-personal-data-former-NSA-employee-7099/.

19. Klimas, Liz. "New NSA Spying Info on Project Code Named 'Stellar Wind': Collected Data Akin to a 'Real-Time Map of Your Brain'". *the blaze.* June 27, 2013. http://www.theblaze.com/stories/2013/06/27/new-nsa-spying-info-on-project-code-named-stellar-wind-collected-data-akin-to-a-real-time-map-of-your-brain/

20. Kloc, Joe. "The definitive guide to NSA spy programs". *the daily dot.* August 14, 2013. http://www.dailydot.com/politics/nsa-spy-prgrams-prism-fairview-blarney/

21. Lee, Timothy B. "Here's everything we know about PRISM to date", *washington post*, jun 12, 2013. https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

22. Lowensohn, Josh. "NSA's 'Dishfire' program said to capture nearly 200 million texts a day". *the verge.* january 16, 2014. http://www.theverge.com/2014/1/16/5316178/nsas-dishfire-program-said-to-capture-nearly-200m-texts-a-day

23. Macaskill, Ewen and Gabriel Dance. "NSA files decoded: What the revelations mean for you". *the guardian.* November 1, 2013. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

24. MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Ball. "GCHQ taps fibre-optic cables for secret access to world's communications". *The Guardian.* June 21, 2013. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

25. Macri, Giuseppe. "Federal Court Dismisses ACLU, Wikipedia Case Against NSA's 'Upstream' Surveillance". *Inside Sources.* October 23, 2015. http://www.insidesources.com/federal-court-dismisses-aclu-wikipedia-case-against-nsas-upstream-surveillance/

26. Marquis-Boire, Morgan, Glenn Greenwald and Micah Lee. “XKEYSCORE: NSA’s Google for the World’s Private Communications”. *The Intercept.* July 1 2015. https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

27. Nakashima, Ellen. “Call records of fewer than 300 people were searched in 2012, U.S. says”. *Washington Post.* june 15, 2013. https://www.washingtonpost.com/world/national-security/call-records-of-fewer-than-300-people-were-searched-in-2012-us-says/2013/06/15/5e611cee-d61b-11e2-a73e-826d299ff459_story.html

28. Neal, Ryan W. “Edward Snowden Reveals Secret Decryption Programs: 10 Things You Need To Know About Bullrun And Edgehill”. *International Business Times.* September 6, 2013. http://www.ibtimes.com/edward-snowden-reveals-secret-decryption-programs-10-things-you-need-know-about-bullrun-edgehill

29. Norton-Taylor, Richard. "Not so secret: deal at the heart of UK-US intelligence". *The Guardian.* June 25, 2010. www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

30. Paganini, Pierluigi. “NSA Bullrun program, encryption and false perception of security”. *security affairs.* September 7, 2013. http://securityaffairs.co/wordpress/17577/intelligence/nsa-bullrun-program-false-perception-security.html

31. Paganini, Pierluigi. “ThinThread spy system secretly tested on New Zealand population”. *Security Affairs.* May 28, 2013. http://securityaffairs.co/wordpress/14749/intelligence/thinthread-us-spy-system-tested-on-nz.html

32. Perrone, James. “The Echelon Spy Network”. *The Guardian.* May 29, 2001. http://www.theguardian.com/world/2001/may/29/qanda.janeperrone

33. Shedd, David R. What guides the U.S Intelligence Community. *the daily signal.* March 28, 2016. http://dailysignal.com/2016/03/28/what-guides-the-us-intelligence-community/.

34. Sottek, T.C. and Joshua Kopstein. “Everything you need to know about PRISM : A cheat sheet for the NSA's unprecedented surveillance programs”. *The Verge.* July 17, 2013. http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

35. Weissman, Cale Guthrie. “It turns out the NSA was collecting voice calls, photos, passwords, documents, and much more”. *Business Insider.* july 1, 2015. http://www.businessinsider.com/nsa-xkeyscore-surveillance-program-details-revealed-in-new-snowden-documents-2015-7

Sites

1. “Members of the IC”. *Office of the Director of National Intelligence web site.* https://www.dni.gov/index.php/intelligence-community/members-of-the-ic.

2. "ECHELON : online surveillance". *what really happened.* http://whatreallyhappened.com/RANCHO/POLITICS/ECHELON/echelon.html.

3. "Top 10 Best intelligence agencie in the world". *ABC news Point*, December 15, 2014. http://www.abcnewspoint.com/top-10-best-intelligence-agencies-in-the-world-2015/

4. “aclu fact sheet on the “police america act"”. *Aclu.* https://www.aclu.org/aclu-fact-sheet-police-america-act

5. “An 'Upstream' Battle As Wikimedia Challenges NSA Surveillance”, *National Public Radio*, march 15, 2015, http://www.npr.org/2015/03/15/393190252/an-upstream-battle-as-wikimedia-challenges-nsa-surveillance

6. “Bernie Sanders on Privacy and digital rights”. *feelthebern.org.* http://feelthebern.org/bernie-sanders-on-privacy-and-digital-rights/.

7. “Entire Stellar Wind (CIA/NSA ‘president’s surveillance program’) document here”. *undercoverinfo.* May 4, 2015. https://undercoverinfo.wordpress.com/2015/05/04/entire-stellar-wind-ciansa-presidents-surveillance-program-document-here/

8. “Executive Orders: The Post 9/11/01 Attack on Civil Liberties Through Executive and Judicial Orders”, *9-11 Research*, http://www.911research.wtc7.net/post911/executive/index.html

9. “Mass Surveillance”. privacy international. https://www.privacyinternational.org/node/52.

10. “PRISM and Stellar Wind Programs”. *talkleft.* June 07, 2013. http://www.talkleft.com/story/2013/6/7/42840/79770/civilliberties/PRISM-and-Stellar-Wind-Programs

11. “Section 215 bulk telephone records and the MAINWAY database”. *Electrospaces.net*, january 20, 2016. http://electrospaces.blogspot.com/2016/01/section-215-bulk-telephone-records-and.html

12. “The Homeland Security Act: Legislation Predicated on the Official Story of the 9/11/01 Attack”. *9-11 Research.* http://911research.wtc7.net/post911/legislation/hsa.html

13. “The Military Commissions Act: Legislation Predicated on the Official Story of the 9/11/01 Attack”. *9-11 research.* http://911research.wtc7.net/post911/legislation/mca.html

14. “The USA Patriot Act: legislation Rushed into Law in the Wake of 9/11/01”. *9-11 Research.* http://911research.wtc7.net/post911/legislation/usapatriot.html

15. "the role of intelligence”, federation of american scientists, february 23, 1996.

16. “What is the Protect America Act?”, *Rupture Ready*, https://www.raptureready.com/faq/faq737.html

17. Bar-El, Hagai. “Against the collection of private data: The unknown risk factor”. *Hagai Bar-El on Security.* august 3, 2012. https://www.hbarel.com/analysis/policy/against-the-collection-of-private

18. Bimfort, Martin T. “a definition of intelligence”. *Cental Intelligence Agency.* September 18, 1995. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm.

19. Bryan Johnson, “Top 10 U.S. Government Changes Since 9/11”, *Toptenz*, september 7, 2011, http://www.toptenz.net/top-10-u-s-government-changes-since-911.php

20. Coeuré, Sophie. “the origins of mass surveillance”. interviewed by Ivan Jablonka. translated by Arianne Dorval. *books and ideas.* http://www.booksandideas.net/The-Origins-of-Mass-Surveillance.html.

21. Cushing, Tim. “NSA’s Stellar Wind Program was almost completely useless, hidden from FISA Court by NSA and FBI”. *Techdirt.* April 27, 2015. https://www.techdirt.com/articles/20150427/11042430811/nsas-stellar-wind-program-was-almost-completely-useless-hidden-fisa-court-nsa-fbi.shtml

22. Fitsanakis, Joseph. "Files reveal names of Americans targeted by NSA during Vietnam War". Intelnew.org. September 26, 2013. https://intelnews.org/2013/09/26/01-1348/

23. Fitsanakis, Joseph. “Declassified report points to flaws in post 9/11 NSA wiretapping”. *Intelnews.org.* April 29,2015. https://intelnews.org/2015/04/29/01-1687/

24. Gallagher, Sean. “NSA’s automated hacking engine offers hands-free pwning of the world”. *Ars technica.* mars 12, 2014, http://arstechnica.com/information-technology/2014/03/nsas-automated-hacking-engine-offers-hands-free-pwning-of-the-world/

25. Ji, Shun-Jie. “Civil liberties vs. national security: lessons from september 11th attacks on america”. http://www2.tku.edu.tw/~ti/Journal/8-2/824.pdf

26. kupcikas, Karolis. “the importance of intelligence to international security”. E-*Internatoinal Relations Student.* november 8, 2013. http://www.e-ir.info/2013/11/08/importance-of-intelligence-to-international-security/.

27. Kursley, Esther. “Briefing paper: Mass surveillance: security by “remote control”-consequences and effectiveness”, *remote control project*, August 2016, p. 2, http://www.oxfordresearchgroup.org.uk/sites/default/files/Mass surveillance briefing paper.pdf.

28. Maximus, Fabius. “How useful are our intelligence agencies? To what degree are they blinded by prejudice and institutional needs?”. *fabiusmaximus.com*. https://fabiusmaximus.com/2010/04/13/intel-2/

29. Mishra, Anant. “role of intelligence agencies in modern warfare”. *indian defense review*. October 29, 2014. http://www.indiandefencereview.com/spotlights/role-of-intelligence-agencies-in-modern-warfare/

30. Mitov, Kiril. “Influence of mass surveillance on business and society”, Robopartans Group, https://robopartans.com/wp-content/uploads/2014/03/MassSurveillance.pdf

31. Mitov, Kiril. “influence of mass surveillance on business and society”. robopartans group. https://robopartans.com/wp-content/uploads/2014/03/MassSurveillance.pdf.

32. Poole, Patrick S. "ECHELON: America's Secret Global Surveillance Network". *Echelon Research Ressources.* 1999/2000, http://www.web.archive.org/web/20070202171651/http://fly.hiwaay.net/~pspoole/echelon.html

33. Schneier, Bruce. “Project Shamrock”. *Shneier on Security.* December 29, 2005. https://www.schneier.com/blog/archives/2005/12/project_shamroc.html

34. Thompson, Chris. “the history of mass surveillance”. *Truthout.* June 21, 2013. http://www.truth-out.org/speakout/item/17139-the-history-of-mass-surveillance.

Dictoinnaries And Encyclopedies

1. encyclopedia of espionage, intelligence and security, Volume 2, ed. Lee Lerner and Brenda Wimoth, svv. “intelligence”, “intelligence and law enforcement agencies”, “Patriot Act”, “intelligence and espionage carreers”.

2. Manish, Kevin. "surveillance ethics", in *internet encyclopedia of philosophy*, http://www.iep.utm.edu/surv-eth/

3. Oxford Dictionnaries, sv. "intelligence", http://www.oxforddictionaries.com/definition/english/intelligence

4. The Free Dictionnary, sv. “intelligence”, http://www.thefreedictionary.com/intelligence.