RIGA GRADUATE SCHOOL OF LAW

Mass Phone Surveillance Programs – Security vs. Civil Liberties?

MASTER'S THESIS

Author: Miraziz Khidoyatov
LL.M 2016/2017 year student
student number M016083

SUPERVISOR: *(CHRISTY, KOLLMAR)*

(JD, LLM, MBA, MGM)

DECLARATION OF HONOUR:
I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …Miraziz Khidoyatov…….

RIGA, 2017

ABSTRACT

Following September 11 attacks, America has increased its intelligence and defense capabilities. In particular, a historic law named USA PATRIOT Act was passed by Bush administration together with President's Surveillance Program. Though the emotional trauma and immediate strategic need to defend the homeland is understandable as it is commendable that the law was passed relatively quick, the Constitution of the United States is what makes this nation so developed and great. This inquiry will take a deep look into the law in relation to unwarranted surveillance over phone activities of the people and assess its constitutionality. To support the assessment, the development of the relevant laws, Section 215 of USA PATRIOT Act and Section 702 of FISA Amendments Act, and the precedents will be analyzed leading us to assume a probable future verdict of the Supreme Court of the United States had it heard this case today. It will be shown that such encroachments on civil rights and liberties is not novel and precede terrorism. Thus, further appropriation and amendments shall be made to the laws to bring it to respect rights to privacy and warrant requirement for search and seizure as guaranteed by Fourth Amendment. Analysis of European Law will be made, using examples of UK and France, and a dangerous trend will be shown illustrating that some leading members of the Union are adapting draconian laws and through cooperation agreements aiding the US into doing things they cannot legally do in the US. Seven recommendations will be proposed to put the laws in question in line with the US Constitution and bring more legitimacy to the process.

Table of Contents

ABBREVIATIONS

1. AG – Attorney General
2. BR – Business Records
3. CIA – Central Intelligence Agency
4. DNI – Director of National Intelligence
5. DOD – Department of Defense
6. DOJ – Department of Justice
7. EU – European Union
8. FISA – Foreign Intelligence Surveillance Act
9. FISC – Foreign Intelligence Surveillance Court
10. FISCR – Foreign Intelligence Surveillance Court of Review
11. NSA – National Security Agency
12. NYT – the *New York Times*
13. ODNI – Office of Director of National Intelligence
14. OLC – Office of Legal Counsel
15. PCLOB – Privacy and Civil Liberties Oversight Board
16. PSP – President's Surveillance Program
17. RAS – reasonable, articulable suspicion
18. SCOTUS – Supreme Court of the United States
19. USA FREEDOM Act – Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act
20. USA PATRIOT Act – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

"[The makers of our Constitution] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men."[1]

INTRODUCTION

Niccolò Machiavelli in the beginning of the sixteenth century in *Prince* claimed that war is a constant state of human nature, peace is just a break.[2] In seventeenth century, Thomas Hobbes asserted that human society is in a condition of perpetual, or endless, war.[3] The same can be said today about crises in general. Even countries that have not been in war for centuries nonetheless fall victim to international calamities that befall humanity. For example, Switzerland was last in war in 1847[4] but refugee crises from wars in Africa or Syria did not go unnoticed for people of and in Switzerland. This study will look at a different type of crisis. It is one of our civil rights and liberties. It is one about, to put it with words of Justice Brandeis in *Olmstead v. United States* (1928)[5], "the most comprehensive of rights and the right most valued by civilized men" – "the right to be let alone".[6]

Dozens of innovative technologies, ideas and concepts, if not more, are being created every day. With regards to the level of human progress and population, it is not surprising. Nonetheless, the speed of life is faster than ever and it keeps accelerating. As any product humanity creates – it has ability to improve our lives as well as destroy it. An example of the latter can be seen from the Snowden leaks. After them, and future leaks that continue to come, people became more aware of what they speak, to whom and where. For example, numerous school and college students put tape over their web-cameras on their computers. People stopped feeling safe.

Evidently, laws and legal protections, unfortunately, do not move at the same pace as innovation does. Therefore, there is some buffer time in which a lot of things can and do happen. During this buffer time, mass surveillance of people, of what they do, say, discuss, like or share in secret could be conducted for it would fall in legal "gray area". And this could be done not only by governments. There are companies that could assemble and compile all the information available online about a person or group of people, this compilation is named Big Data. According to some representatives of one of Big Four Audit companies, financial institutions and

---

[1] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, L., dissenting)
[2] ***See*** Niccoló Machiavelli, *The Prince* (Robert M. Adams trans., W.W. Norton & Company, Inc. 1977) (1532)
[3] ***See*** Thomas Hobbes, *Leviathan* (Penguin 1985) (1651).
[4] Which was a Civil War effectively creating Swiss Federation. ***See*** *Charm Offensive — Switzerland's 'Polite War' of 1847*, Military History Now (January 18, 2013), http://militaryhistorynow.com/2013/01/18/charm-offensive-switzerlands-polite-war-of-1847/
[5] *Olmstead v. United States*, 277 U.S. 438 (1928)
[6] *Id*, at 478.

companies who provide services to them are already using Big Data and start involving them in their daily processes.[7]

Google Inc. is a company that uses Big Data by tracking where people go (through Google Maps), what they search for, what they like with clicks on ads. From these, now, simple processes Google might know everything about anyone. Starting from which food one likes ending with his/her sexual preferences and hidden desires. Below, an example will be given of how can one deduct all life events happening in a life of a target just by looking at his/her phone calling records, obtained through Section 215 of USA PATRIOT Act.

People would be rightly worried about their privacy. They would be rightly worried about whether this could be used against them. Though legally it cannot be, human history, American included, has seen governments or people in power abusing this very power for their own benefit. Sometimes, suppressing free press.

It must be noted that, contrary to some popular belief, right to privacy is not mentioned in the Constitution of the United States in contrast to European Convention of Human Rights and Constitutions of several European states.

With regards to the United States Constitution, though there is no written right to privacy in the Constitution, it exists as an implied right through Constitutional interpretation by the Supreme Court of the United States ("SCOTUS").

Because the study will be comparing the United States practice with European, putting great emphasis and analysis on American, the author of this study finds it prudent to give a brief introduction to the right to privacy in the United States and, later, explain origin of the issue together with its deeper importance.

a. Right to Privacy

In American law, the right to privacy exists under two main spheres/areas: (1) under tort law, affording tort damages for invasion of privacy, and (2) under constitutional law, protecting people's right to privacy against unlawful governmental intrusion.[8] This work will focus on Constitutional area of right to privacy.

As noted by the Supreme Court in a landmark case, *Roe v. Wade* (1973)[9]:

> "Although the Constitution does not explicitly mention any right of privacy, the United States Supreme Court recognizes that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution, and that the roots of that right may be found in the First Amendment, in the Fourth and Fifth Amendments, in

[7] More on Big Data and how the government is using it, *see* Chad Squitieri, *CONFRONTING BIG DATA: APPLYING THE CONFRONTATION CLAUSE TO GOVERNMENT DATA COLLECTION*, 101 Virginia Law Review 2011 (2015).
[8] ***See*** 1-1 Data Privacy, Protection, and Security Law § 1.02 (2017)
[9] *Roe v. Wade*, 410 U.S. 113 (1973)

> the penumbras of the Bill of Rights, in the Ninth Amendment, and in the concept of liberty guaranteed by the first section of the Fourteenth Amendment."[10]

This short subsection will give a brief overview of the development of the right to privacy through the Supreme Court. It shall be noted and reiterated that the overview is not comprehensive but serves solely an informative, and introductory, role.

The analysis starts with *Olmstead v. United States* (1928)[11], where government decided to wiretap the conversations of a suspect, Justice Brandeis, in his concurring opinion, declared that right to privacy is "the most comprehensive of rights and the right most valued by civilized men."[12] Nonetheless, the court found no violation of the Fourth Amendment. This case presents importance to the scholarly analysis and would be analyzed in detail further down the study.

Thirty-seven years later, the Supreme Court decided *Griswold v. Connecticut* (1965)[13], in which use of contraceptives was discussed. Majority opinion written by Justice Douglas presents utmost importance to the right to privacy in America. It took the argument of the petitioner and through use of, not one or two but a set of, six Amendments created the right to privacy and issued strict scrutiny standard pertaining to these issues.

Strict scrutiny is a legal standard that is most favorable to the individual. According to Black's Law Dictionary,

> "In due-process analysis, the standard [is] applied to suspect classifications (such as race) in equal-protection analysis and to fundamental rights (such as voting rights)."[14]

It was officially introduced by the Supreme Court in *Korematsu v. United States* (1944)[15]. The Supreme Court explained the test as follows:

> "In order to withstand strict scrutiny, the law must advance a compelling state interest by the least restrictive means available."[16]

Continuing with the case study of development of the Constitutional right to privacy, while *Griswold* was about use of contraceptives between married couple, in *Eisenstadt, Sheriff v. Baird* (1972)[17] the issue was of use of contraceptives between an unmarried couple. Without going in detail, the Court held that there can be no discriminate treatment between married and unmarried couples, for this violates Fourteenth Amendment's Equal Protection Clause. But most importantly, the opinion reaffirms the right to privacy. "If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."[18] It is true that arguably the decision limited the right to privacy to childbearing, it

[10] *Roe v. Wade*, 410 U.S. 113, 152 (1973)
[11] *Olmstead v. United States*, 277 U.S. 438 (1928)
[12] *Id*, at 478 (Brandeis, L., dissenting)
[13] *Griswold v. Connecticut*, 381 U.S. 479 (1965)
[14] STRICT SCRUTINY, Black's Law Dictionary (10th ed. 2014)
[15] *Korematsu v. United States*, 323 U.S. 214 (1944)
[16] *Bernal v. Fainter*, 467 U.S. 216, 219 (1984)
[17] *Eisenstadt, Sheriff v. Baird*, 405 U.S. 438 (1972)
[18] *Id*, at 453

nonetheless basically created a right not mentioned in the constitution. Further down the opinion, the implied character of the right was, however, noted.

Roe v. Wade (1973)[19] will be the case following *Eisenstadt*. In *Roe*, the Court applied the right to privacy to Fourteenth Amendment Due Process Clause and reaffirmed the standard of strict scrutiny pertaining to these issues.

Now the brief introduction to evolvement of right to privacy in America is finished, it is now prudent to continue with outlining the central issue of the study, explain its importance and relevance.

b. Coming to the issue, study's importance and structure

Returning to the idea of Machiavelli perpetuated earlier – world exists in the constant state of war. And this war might not always be fought with guns – it might be in the form of competition or constant struggle for dominance. That is indeed the political realism theory.[20] It must be noted though that that competition is probably the greatest force behind innovation and progress and thus has great benefits.

Starting just from the second wave of colonization, one can already note that there has always been a growing threat to either peace and security of Europe or existential threat to the Western way of life. It all started with Germany, followed by Soviet Union and spread of Communism, came back to Germany, after World War II returned back to Communism, and after the fall of the Iron Curtain, with almost 10 years of political vacuum, "civilized world" found a new existential enemy. This new adversary was found in September 11, 2001– Islamist radicalism and Islamist terror. Though arguably Russia, with the rule of Putin, recently returned back to being existential threat to international peace and security, this threat might be a bit exaggerated.

After September 11, 2001 attacks, the United States and the whole world ended the year with a state of shock. The countries were unanimous in their joint declaration of war against terrorism, or probably a more particular type of terrorism – Islamic radicalism.

In essence, this war is similar to Cold War for in the Cold War the ideology of Communism was as great of an adversary as the Soviet Union. Therefore, in the United States a rise of radical anti-Communist sentiment exemplified in McCarthyism is seen. One could see similar rise of Islamophobia exemplified with stabbings in MAX Light Rail or, more recent, homicide of 17-year old Nabra Hassanen. In contrast to Cold War, where the greatest enemy was a State-actor with real threat of nuclear attack, the Communism was just another weapon, this new form of war is different where the greatest enemy is an ideology, without clear face. It also is asymmetrical for the radical groups target civilians to instill fear, whilst the attacks of State-

[19] *Roe v. Wade*, 410 U.S. 113 (1973)
[20] ***See*** Richard K. Ashley, *Political Realism and Human Interests*, 25 International Studies Quarterly 204 (Jun. 1981).

actors against terrorists very often leaves numerous civilian casualties. The enemy is a non-State actor. Therefore, the foe is effectively invisible, for any person of any color could be member of such an organization and he/she does not have to wear any distinctive features[21]. Effectively, this war becomes more heavily reliant on counter-intelligence practices rather than preparations for war through weaponry development, like nuclear warheads in the Cold War. In such an environment, the time dictates for development and improvement of new communication interception, location pinning and individual identification technologies[22]. That is indeed what has taken place.

However, it is essential that States do not forget main goal of the war – to preserve liberal ways of life instead of falling to the status of police states. These liberties and civil rights are indeed what distinguishes the Western liberal societies and democracies from the regimes that Islamist radicals want to impose on the world. Therefore, the question on civil liberties this study analyzes is fundamental to commonly valued democratic and liberal way of life.

To narrow down the scope, the study selected phone surveillance to be the focal point. The reason is simple and self-evident – phones and electronic means communication became primary source of communication between people in distance. They are not solely means of communication anymore – together with most intricate details that our communications (be that voice, message or email) can reveal, they contain most private details of our lives through pictures, videos and other recordings. This view is shared by the United States Supreme Court too.[23]

Due to nature of the threat, the object of surveillance becomes undetermined. Clearly, terrorists are intended subjects but due to difficulty of determination of such the subjects become effectively everyone. The study will reveal specific techniques and criteria used to determine investigation objects in two most famous relevant provisions of counter-intelligence laws pertaining to electronic communication surveillance in the United States. More specifically, USA PATRIOT Act's Section 215 and FISA Amendments Act's Section 702. The study will analyze its constitutionality and compare them to practices in the European Union.

Again, assessment of constitutionality will be too complex for a limited space given. Therefore, the study will limit its focus to the Fourth Amendment, which reads as follows:

> "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."[24]

[21] ***See*** Andrew Campbell, *'Taqiyya': How Islamic Extremist deceive the West*, National Observer 11 (Winter 2005).
[22] Such as face recognition software
[23] ***See*** *Riley v. California*, 134 S.Ct. 2473, 2483 (1948)
[24] U.S. Const. Amend. IV

The structure of the work will be as follows. The introduction will be followed by Chapter I, which analyzes precedents pertaining to the issue of communication surveillance and the Fourth Amendment. Next, Chapter II will begin analysis of Section 215 of USA PATRIOT Act, track its development and analyze its constitutionality. The study will make a commentary trying to predict future movements of the court in this area. Chapter III will go in the same direction as Chapter II but with Section 702 of FISA Amendments Act. Following will be Chapter IV where analysis of the similar practices and legal developments in the European Union will be analyzed. Finally, Chapter V will offer author's recommendations to amend practices of intelligence agencies to conform with current and evolving civil standards.

CHAPTER I

CELL PHONE COMMUNICATION AND THE FOURTH AMENDMENT – INTERPRETATION BY THE SUPREME COURT OF THE UNITED STATES

To understand the evolvement of the constitutional interpretation and therefore of civil rights and liberty protections, in the course of our inquiry it becomes pivotal to review the case law most pertinent. This chapter will analyze the precedents most relevant to the study.

Unreasonable searches and seizures were subject to civil actions long before 1791 and landmark English cases, such as *Entick v. Carrington and Three Other King's Messengers*[25], can serve as evidence. However, these laws were intended and interpreted as non-trespass rules only, as was the Fourth Amendment for the Supreme Court of the United States for a long time. And it continued to be seen as such until *Boyd v. United States* (1886)[26].

Written by Justice Bradley the opinion recalls Lord Camden's judgment in *Entick v. Carrington* and presumes that "its propositions were in the minds of those who framed the fourth amendment to the constitution".[27] In there, Lord Camden reasoned that "[t]he great end for which men entered into society was to secure their property."[28] Explaining that property is an inviolable good and that instances where trespass, and seizure, is permitted must be clearly defined by law. If law is silent, then trespass is unlawful. Similarly, secrets in letters and documents are "[men's] dearest property" and therefore, even absent of physical intrusion of space, the violation of secrecy of these documents constitutes trespass.[29] This court has used the same logic and further emphasized the inviolability of personal property and papers, and gone even further by decreeing that courts have no right to order production of evidence from defendants, which might convict them.

Subsequently, the Court continuously condemned search and seizure of defendants' home or property without a warrant and continuously found those to be in violation of the Fourth Amendment. Among those were – *Weeks v. United States* (1914)[30], *ex parte Jackson* (1878)[31], *Silverthorne Lumber Co. v. United States* (1920)[32], *Amos v. United States* (1921)[33], *Gouled v. United States* (1921)[34].

Surely, *Boyd's* view did not last long, for it's a bit radical take, and in subsequent cases was indirectly overturned. Nonetheless, even taking these views into account, as propagated in

[25] *Entick v. Carrington and Three Other King's Messengers*, EWHC KB J98, 95 ER 807 (1765)
[26] *Boyd v. United States*, 116 U.S. 616 (1886)
[27] *Id*, at 626.
[28] *Id*, at 627.
[29] *Id*, at 628.
[30] *Weeks v. United States*, 232 U.S. 383 (1914)
[31] *ex parte Jackson*, 96 U.S. 727 (1878)
[32] *Silverthorne Lumber Co. v. United States*, 252 U.S. 385 (1920)
[33] *Amos v. United States*, 255 U.S. 313 (1921)
[34] *Gouled v. United States*, 255 U.S. 298 (1921)

Boyd v. United States, what approach should the government take with phone communication? First, nothing was ever mentioned or even thought about phones in Boyd and Entick, simply because they did not exist yet. Second, the letters are something that was sealed and sent, openly declaring that the contents of the letter are secret, while phone conversations are something that can be overheard – so are they really a "dearest property" of men?

First case to ask this question was *Olmstead v. United States* (1928)[35]. In their paper, *FIGHTING CYBERCRIME AFTER UNITED STATES V. JONES*, Gray, Citron and Rinehart gave a fascinating story about development of the telephone.[36] A year after Bell's and Watson's "famous first telephonically transmitted words" in 1876, there were 3,000 active telephones in the United States.[37] In 1902 "2,315,000 telephones were in service in the United States."[38] By 1908, New York City alone had 800,000 phones.[39] By 1927 telephone became an essential part of American life.[40] As with any great invention, it might be used in a criminal way, be that directly or indirectly.

Olmstead was suspected in violating the prohibition laws by importing and distributing the liquors. In the course of investigation police inserted wires into the telephone lines used by the suspect to listen to his conversations. Based on gathered information, or as a consequence of it, the prosecution had a strong case against the suspect. There was no trespass upon any property of the suspect. Nonetheless, Olmstead further appealed the decision of the district court arguing that law enforcement violated his Fourth Amendment rights.

However, the Court declined to accept that, an intangible, conversation was intended to be protected under the Fourth Amendment. They justified that by explaining that warrant requirement of the Fourth Amendment is on tangible things only. "The amendment itself shows that the search is to be of material things-the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or things to be seized."[41]

The Court here, though using *Boyd v. United States* (1886)[42], fails to tackle the logic of it – the reasoning used in the case. Instead, they just compare contrast fact situations, analyze approach and state the court's ruling. In *Boyd*, the Court intentionally made clear that Fourth Amendment protects privacy of the people and explained that the enumerated things there are

[35] *Olmstead v. United States,* 277 U.S. 438 (1928)
[36] David Gray, Danielle Keats Citron & Liz Clark Rinehart, *FIGHTING CYBERCRIME AFTER UNITED STATES V. JONES*, 103 Journal of Criminal Law and Criminology 745, 752 (2013).
[37] The History, Old Telephones, http://oldtelephones.com/the-history/ (last visited Apr 18, 2017); Talking Wires: The Development of the Telephone, Talking Wires: The Development of the Telephone, http://www.moah.org/talkingwires/talkingwires.html?KeepThis=true (last visited Jul 18, 2017).
[38] Jennifer H. Meadows & August E. Grant, Communication Technology Update, 16 (2012).
[39] Herbert N. Casson, History of the Telephone, 172-73 (1910).
[40] Claude S. Fisher, America Calling: Social History of the Telephone to 1940, at 52-52 (1992); David Gray, Danielle Keats Citron & Liz Clark Rinehart, *FIGHTING CYBERCRIME AFTER UNITED STATES V. JONES*, 103 Journal of Criminal Law and Criminology 745, 752 (2013).
[41] *Olmstead v. United States*, 277 U.S. 438, 464 (1928)
[42] *Boyd v. United States,* 116 U.S. 616 (1886)

just examples or different varieties available. Here, one sees clear reversal of the logic back to old common law non-trespass only understanding of the Fourth Amendment.

One thing one should notice by reading these precedents is their names – United States is always there as a side, not a State. There is a simple explanation for that – *Barron v. Baltimore* (1833)[43]. The Court held that the Fourth Amendment was applied exclusively to the Federal government, and not the States. Therefore, in *Olmstead* reasoning, how the Court compares the practice of State Supreme Courts with their Constitutional variation of the Fourth Amendment is seen. This was so until *Mapp v. Ohio* (1961).[44]

There truly an intellectual feast and eclipse of justice is seen. Justice Clark delivered the opinion and in there used *Boyd v. United States* (1886).[45] This time though, he used logic of the opinion instead of the bare facts of it. Though incredibly interesting, this case is relevant to the current study only to the extent that it applies the Fourth Amendment to the States and puts back the Amendment to the logic of liberty of the people from warrantless governmental intrusion into their privacy. This logic was summarized in another landmark case – *Katz v. United States* (1967)[46].

This case is probably most important to us today for it gives standard against which future cases were decided.

Due to previous continuous interpretation of the Fourth Amendment as non-trespass rule, in this case, the Court was asked whether a telephone booth is a constitutionally protected area and whether its physical penetration is required "before search and seizure can be said to [violate] the Fourth Amendment to the United States Constitution."[47]

The case concerned a man who was transmitting wagering information from Los Angeles to Miami and Boston, in violation of federal laws. FBI attached a listening and recording device to the outside of phone booth the petitioner was using to make calls for that illicit end. These recordings were then presented at the Trial Court, over petitioner's objections. Federal Court of Appeals rejected the petitioner's contention that these recordings, and evidences, were obtained in violation of the Fourth Amendment. The reason is the same as it was – there was no physical entrance. During oral hearings at the Supreme Court, both sides argued "strenuously" whether booth constituted a "protected area".[48] Majority Opinion of the Supreme Court, written by Justice Stewart, right away, claimed that the Court "decline[s] to accept this formulation of the issues." They reasoned that the Fourth Amendment problems are not promoted by the "constitutionally protected area" and that Fourth Amendment rights cannot be translated into right to privacy.[49] Regarding the latter point, the Court clarified that the protections of the Fourth Amendment go further than privacy protections "and often have nothing to do with privacy at

[43] *Barron v. Baltimore*, 32 U.S. 243 (1833)
[44] *Mapp v. Ohio*, 367 U.S. 643 (1961)
[45] *Boyd v. United States*, 116 U.S. 616 (1886)
[46] *Katz v. United States*, 389 U.S. 347 (1967)
[47] *Id*, at 350.
[48] *Id*, at 351.
[49] *Id*, at 350.

all."[50] Nonetheless, it was here the Court famously proclaimed, "The Fourth Amendment protects people, not places." [51]

The government contended that the booth was made of glass and therefore the petitioner was exposed to public and thereby voiding the protection of the Fourth Amendment. However, the Court responded saying that the petitioner still wanted to exclude unwanted ear and the glass was intended for that purposes. Following *Rios v. United States* (1960)[52] and *ex parte Jackson* (1878)[53], the Court contended that if a person intends to keep things private, even if done in an area accessible to public, Constitutional protection can still be applied.

"One who occupies [the telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[54] Here the court introduces the progressive interpretation of the Fourth Amendment allowing future courts to adapt to technological progress.

Next, the government contended that there was no violation of the Fourth Amendment for there was no physical penetration. The Court admitted that it did previously use such interpretation of the Fourth Amendment. Nonetheless, they noted that the property prerequisite has been waived already, in *Warden v. Hayden* (1967)[55]. In *Silverman v. United States* (1961)[56], the Court held that seizure of intangible items without warrant can also constitute a violation of the Fourth Amendment. Consequently, the Court concludes that "[o]nce this much is acknowledged, and once it is recognized that the Fourth Amendment protects people -- and not simply "areas" -- against unreasonable searches and seizures," the requirement of physical intrusion of space becomes irrelevant.[57] Furthermore, the Court precluded law enforcement agents from warrantless search on grounds of presence of a probable cause even when the least restrictive means were exercised.

Interestingly enough, the Court here seemingly introduces reasonable expectation of privacy standard but mentions it in relation to the individual only. Also, the court not only addresses specific exceptions to the judicial process of the search, the Court says "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment."[58] This means that all searches without judicial approval are in violation of the Fourth Amendment, except when they fall under "few specifically established and well-delineated exceptions."[59] These are three – if seizure is incident

[50] *Id.*
[51] *Id*, at 351.
[52] *Rios v. United States*, 364 U.S. 253 (1960)
[53] *ex parte Jackson*, 96 U.S. 727 (1878)
[54] *Katz v. United States*, 389 U.S. 347, at 352 (1967)
[55] *Warden v. Hayden*, 387 U.S. 294 (1967)
[56] *Silverman v. United States*, 365 U.S. 505 (1961)
[57] *Katz, supra note* 5, at 353.
[58] *Id.*, at 357
[59] *Id.*

to arrest, if it is conducted as a result of hot pursuit and if done by individual's consent. The case failed to apply to those three exceptions.

The Court unintentionally added another exception but this one was curiously not in the opinion itself. This exception was in the footnote of the opinion – famous footnote 23. "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." Some scholars asserted that "This footnote suggested the possibility that agents could conduct national security and foreign intelligence searches without obtaining a search warrant."[60]

At least two concurring opinions play significant role in our study today. Justice Douglas, whom Justice Brennan joins, clarifies that such electronic searches are unconstitutional even when "national security" interest is invoked and a member of executive branch (disconnected from the case and investigation) authorizes such search. They reasoned that the Constitution intentionally required that such warrants be given by another, independent, branch – judicial. They underlined that executive, no matter how detached from the case, cannot be independent.

Next concurring opinion, by Justice Harlan, is of special importance to us. Here, Justice Harlan introduces two-prong standard/test for cases concerning unwarranted searches and seizures. First prong is whether an individual had a subjective expectation of privacy. Second is if that expectation is one that the society can recognize as reasonable.

This case is important to us for the subsequent court decisions have taken Justice Harlan's standard in analyzing future cases. Therefore, for no new standard arose nor this was explicitly overturned, we will also use it for the analysis section.

National Security exception to the Fourth Amendment is often discussed by the government. *United States v. United States District Court for the Eastern District of Michigan et al*. (known as *Keith*)[61], though sided with the individual and found that government violated the Fourth Amendment by wiretapping conversations of White Panther Party who tried to bomb CIA office in Michigan, indirectly created the national security exception.

> "We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."[62]

Furthermore, the Court states that surveillance conducted on US soil should be subject to the Fourth Amendment requirements, because of the dangers of abuse of power. Thereby, the Court in *Keith* leaves door for unwarranted surveillance of foreign agents and of persons located outside the United States. The criticism for users of *Keith* to warrant national security exception is that the Court does not give a blank check for national security matters. In fact, the Court states, "constitutional basis of the President's domestic security role … must be exercised in a manner compatible with the Fourth Amendment."[63] Therefore, unwarranted wholly domestic

[60] Patrick Walsh stepping on (or over) the constitution's line
[61] *United States v. United States District Court for the Eastern District of Michigan et al.*, 407 U.S. 297 (1972)
[62] *Keith*, 407 U.S. 297, 321-322 (1972)
[63] *Id.* at 319

surveillance is unconstitutional. As it shall be seen, Section 702 of FISA Amendments Act will try to fit this framework. Nonetheless, as Senator Edward Kennedy was quoted in Justice Douglas' concurring opinion, there is "the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps years at a time. Even the most innocent and random caller who uses or telephones into a tapped line can become a flagged number in the Government's data bank."[64] As the world community discovered about Section 215 of Patriot Act and Section 702 of FISA Amendments Act through Edward Snowden leaks, this scenario is not a mere possibility anymore – it is, unfortunately, ongoing reality.

Four years later, 1976, the Court decided another case on Fourth Amendment. In *United States v. Miller*[65], the Court analyzed whether personal records obtained through a third party constitutes Fourth Amendment violation. In this case, Banks where respondent had accounts, upon receiving subpoenas, handed over to the government checks, deposit slips and financial statements of the respondent. Court affirmed that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[66]" With this case, the government received assurance from the Court that people had diminished expectation of privacy in cases when persons voluntarily conveyed personal information to a third-party, even if they had reasonable expectation that this information or these records remain private. In particular, this case emphasized that records conveyed "in the ordinary course of business" are no longer private and can be requested through subpoena or directive without warrant given on probable cause.[67] This will be further used by the government extensively. With our conversations becoming more electronic and being more dependent on a third-party (business), it basically leads to a state when none of our conversations would be protected for people always have an intermediary business recording our conversations or passing our conversations through their service as an ordinary course of business. This will be until the Court would recognize that electronic communications are protected under the Fourth Amendment. In *Kyllo v. United States* (2001)[68], the Court will put a cornerstone for such an interpretation, on which, in turn, the Court built the Constitutional understanding of *Riley v. California* (2014)[69], which would be vital for our analysis further on.

What is most important for this study's aim is that with *Katz*[70], the Court opened the door onto flowing interpretation of the Fourth Amendment, which can be compatible and adaptive to technological progress. This brought new questions about what exactly are the reasonable expectations of privacy of individuals and the society. Where do we draw a line?

---

[64] *Id.* (Sen. Edward Kennedy as quoted by Justice Douglas)
[65] *United States v. Miller*, 425 U.S. 435 (1976)
[66] *Id,* at 443.
[67] *Id,* at 442.
[68] *Kyllo v. United States*, 533 U.S. 27 (2001)
[69] *Riley v. California*, 134 S.Ct. 2473 (2014)
[70] *Id.*

A major Supreme Court case asking one such question was *Smith v. Maryland* (1979).[71]

Michael Lee Smith, after robbing Patricia McDonough, started to make obscene and threatening calls to her home. At some point, he asked her to step out to the porch. After doing so, Ms. McDonough observed a car she saw near the crime scene and later described to the police. Police also observed a man and a car matching victim's description in the victim's neighborhood. By tracking the license plate numbers, police, without a warrant, requested the telephone company to install pen register to record phone numbers dialed from the petitioner's phone. The company complied. Upon examination of the register, police learned that calls have been placed from petitioner's home to the victim's home. They obtained a warrant and searched Mr. Smith's home, where they have found a phone book folded on a page with Ms. McDonough's name and number. Mr. Smith was arrested and recognized as the robber by Ms. McDonough in a six-man line-up. On trial, petitioner requested all fruits from warrantless pen register be suppressed. Trial court rejected the motion. Court of Appeals also declined to accept that warrantless pen register constituted a violation of the Fourth Amendment for the lack of "reasonable expectation of privacy into numbers dialed into a telephone system."[72]

Supreme Court agreed with the lower courts' interpretation of facts. The opinion of the court rendered by Justice Blackmun reasoned that an individual does not have legitimate expectation of privacy of phone numbers dialed. The Court expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[73] People dial numbers they know will be transferred to the phone company to make the call. And even if, somehow, the petitioner had some reasonable expectation of privacy – it is not "one that society is prepared to recognize as 'reasonable'."[74] Many reasons were given. For example, the phone companies in their terms of service stipulate that they can record phone numbers for billing purposes or to inform clients on the source of unwanted calls.

Therefore, now it must accepted that pen register is outside the scope of the Fourth Amendment. It shall be noted, however, that court did comment on limited capabilities of pen register, "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed -- a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[75]

However, this also raises an important practical (constitutional) question – if these numbers are not protected because they are transferred to a third-party, can the government just intercept these numbers before they reach the company? The scholarly analysis leads to suggest that according to Smith the government should obtain the data "from and with the knowledge of

[71] *Smith v. Maryland*, 442 U.S. 735 (1979)
[72] *Smith v. Maryland*, 442 U.S. 735, 738 (1979)
[73] *Id*, at 742
[74] *Katz v. United States*, 389 U.S. 347 (1967)
[75] *United States* v. *New York Tel. Co*., 434 U.S. 159, 166 (1977);

the third party."[76] It is also suggested by *Smith* and by scholars that the third-party doctrine rests on *voluntary* disclosure. Today, it seems appropriate to ask how voluntary are our disclosures to the phone service or internet provider companies. Without these third-parties people would not have possibility to use technology. Therefore, if one takes *Smith* precedent as leading today, one is obliged to accept the reality that if one lives in the society of the 21st Century, he/she does not have Civil Liberties guaranteed by the Fourth Amendment.

This point was actually raised by Justice Sotomayor's concurring opinion in *United States v. Jones* (2012).[77] She pointed out that people are voluntarily giving up "a great deal of" personal information by performing mundane tasks. She noted that for that reason, it should not mean that only because a person is giving up personal information to a third person for a limited purpose – this person has limited expectation of privacy and is, therefore, disentitled from the Fourth Amendment's protection. Most importantly to the point of this study is that she noted that such, current, approach is ill suited for the digital age. This study agrees with this assessment.

Next, the study will analyze *Kyllo v. United States* (2001)[78]. It must be noted that the subject in this case is not directly related to the issue at hand. However, as it was stipulated at the page 15, the decision plays an important role in the subsequent relevant and important Court decision, *Riley v. California* (2014). Furthermore, it plays an important role in illustrating that the Court begins to adapt to the development of technology.

Danny Kyllo was suspected to be growing marijuana at his home. Usually, when marijuana is grown in home conditions, a certain technology is used – high intensity lamps.[79] Agents from US Department of Interior used thermal imaging scanner to observe thermal image of Kyllo's house. Using these images, the government obtained a search warrant into Kyllo's house. Kyllo, in District Court, filed motions to suppress evidence obtained through thermal imaging scanner on the grounds that the procedure violated the Fourth Amendment. District Court disagreed, Circuit Court remanded but District Court again denied motion to suppress and Circuit Court after change of composition agreed. The United States Supreme Court agreed with the arguments of the petitioner and ruled that use of thermal imaging is against reasonable expectation of privacy and constituted a search for it revealed to user the information not intended for public use. [80] This case is important to us in that the Court reaffirmed that Fourth Amendment interpretation should be adjusted to the emerging technology. "The Court recognized that it must sometimes confront the question of what limits there are upon this power of technology to shrink the realm of guaranteed privacy. In a case involving a thermal-imaging device aimed at a private home from a public street, which revealed details about the interior of the home that previously could have been known only by physical entry, the Court declared use

[76] Monu Bedi, *THE CURIOUS CASE OF CELL PHONE LOCATION DATA: FOURTH AMENDMENT DOCTRINE MASH-UP*, 110 Northwestern University Law Review 507, 512 (2016)
[77] *United States v. Jones*, 132 S.Ct. 945 (2012)
[78] *Kyllo v. United States*, 533 U.S. 27 (2001)
[79] *Id*, at 29
[80] *Id.*

of the device to be a search, rejecting a rigid interpretation of the Fourth Amendment that would leave the homeowner at the mercy of advancing technology."[81]

So, listening to one's conversations without a warrant violates the Fourth Amendment but installing the pen register to know what numbers one called does not. But what about searching one's phone digital information after arrest? Technically the phone is a fruit to the arrest.

In *Riley v. California* (2014)[82] the Court resolves this issue. Being more precise this opinion is a decision on two cases – *David Leon Riley v. California* and *United States v. Brima Wurie*. Both "raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[83]

In both cases, as it may be obvious, people were arrested, their phones then searched and later convicted of crimes using evidences obtained from, and as a result of, the information contained on the phones. Though not explicitly noted in the opinion, this case is related much more to *Johnson v. United States* (1948)[84] than just for the issue of warrantless search. In these cases, as it is in *Johnson*, officers gained evidence for conviction for serious crime only after the arrest. The big difference is that in *Johnson* the court found that the arrest was unjustified and therefore search of premises incidental to arrest was not either, while in *Riley* the Court agrees with justifiability of arrest without agreeing with the justifiability of search.

But back to Riley. The Court made a great remark that is hard to ignore or pass by:

> "In 1914, this Court first acknowledged in dictum 'the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime.' *Weeks v. United States*, 232 U.S. 383, 392, 34 S.Ct. 341, 58 L.Ed. 652. Since that time, it has been well accepted that such a search constitutes an exception to the warrant requirement. Indeed, the label "exception" is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant. See 3 W. LaFave, Search and Seizure § 5.2(b), p. 132, and n. 15 (5th ed. 2012).
>
> Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long."[85]

In particular, the Court noted, the scope of how far could law enforcement officers search the arrestee without a warrant was debated. The opinion informed us that, as of now, there are three cases that govern this issue: *Chimel v. California* (1969)[86], *United States v. Robinson* (1973)[87] and *Arizona v. Gant* (2009)[88].

---

[81] David Medine et al., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, Privacy and Civil Liberties Oversight Board, at 121 (2014) (internal quotations omitted).
[82] *Riley v. California*, 134 S.Ct. 2473 (2014)
[83] *Id*, at 2480
[84] *Johnson v. United States*, 333 U.S. 10 (1948)
[85] *Riley v. California*, 134 S.Ct. 2473, 2483 (1948)
[86] *Chimel v. California*, 395 U.S. 752 (1969)
[87] *United States v. Robinson*, 414 U.S. 218 (1973)
[88] *Arizona v. Gant*, 556 U.S. 332 (2009)

Chimel "laid the groundwork for most of the existing search incident to arrest doctrine."[89] In there, police after arresting a suspect at his home, without a warrant searched his house in entirety (including attic and garage)[90]. *Chimel* Court explained that search without a warrant upon arrest is justified on arrestee's person and as far as the area is reachable to him/her to gain possession of weapons or destroy evidence. Extensive search in this case was, therefore, not justified.

In *Robinson,* police officer arrested Robinson for driving with a revoked license and upon patdown search found a crumpled cigarette pack in one of his pockets. Removing and opening it, he found 14 capsules of heroin.[91] Appeals court found that the search was unjustified for Robinson was unlikely to have evidence for arrest on his person, nor was extracting and opening a cigarette package going to prevent danger to the life of the officer.[92] The Supreme Court found this search to be justified. "The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect. A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification."[93]

Therefore, as Riley court explained, the Court allowed search of arrestee without having reasonable threat to officer's life or destruction of evidence. But the Court clarified in *United States v. Chadwick* (1977) that "this exception was limited to 'personal property ... immediately associated with the person of the arrestee.'"[94]

Gant recognized that *Chimel* concern for officer safety and evidence preservation are essential to warrantless search. Applying the case to car circumstances, *Gant* Court explained that search of the car is justified if the suspect is unsecured and might get a hold of a weapon. The passenger compartment search might also be justified if there might be evidence relevant to the crime.[95] *Gant* Court determined that search-incident-to-arrest exception to the Fourth Amendment did not justify the search in this case.[96]

To decide this case, the court used balancing test of *Wyoming v. Houghton* (1999)[97] as, they clarified, it was used to decide *Robinson*. In this test, the Court "assess[ed], on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[98] Cellphone data and information, the Court explained, did not pose danger to the officers, nor was it likely that

[89] *Riley*, supra note 84, 2483
[90] *Id.*; *also see Chimel v. California*, 395 U.S. 752, 753-754 (1969)
[91] *United States v. Robinson*, 414 U.S. 218, at 220 and 223 (1973) as cited by *Riley v. California*, 134 S.Ct. 2473, 2483 (2014)
[92] *United States v. Robinson*, 414 U.S. 218 (1973) as cited by *Riley v. California*, 134 S.Ct. 2473, 2483 (2014)
[93] *United States v. Robinson*, 414 U.S. 218, at 235 (1973)
[94] *United States v. Chadwick*, 433 U.S. 1 (1977)
[95] *Id*, 15, as cited by *Riley v. California*, 134 S.Ct. 2473, 2484 (2014)
[96] *Arizona v. Gant*, 556 U.S. 332 (2009)
[97] *Wyoming v. Houghton*, 526 U.S. 295 (1999)
[98] *Id*, at 299

arrestee could destroy evidences without phone in his possession. The searches of person of arrestee is brief while search of the phone data intrudes on the most private information of the phone owner. Therefore, such search required a warrant. The Court admitted that search of the phone can be justified if only the physical aspects would be searched. On the arguments by the United States and California that evidence might be destroyed also remotely, the Court said that police had enough capabilities to prevent that. Furthermore, the data (evidence) could not be destroyed by the suspect himself remotely while being in custody.

Therefore, in practice, we have prohibitions of law enforcement agencies to search phones of suspects without a warrant be they in custody or just under investigation. Nor does the law enforcement have a right to read people's conversations without a warrant, unless it is based on legitimate, work-related justification.[99] Leading precedent for the latter is *City of Ontario, Cal. v. Quon* (2010)[100].

There an officer of police department was using his work pager for his personal matters and thereby going over the imposed character limit and paying the fine. While officer was, without objection, paying out the fines, the police department wanted to investigate if the character limited was too small, so that if they were these would be increased for workers to avoid fines, or the workers were using all those characters for personal means. For that end, they requested transcript of texts of officer Quon and found out that most of his texts were not work related. An internal investigation was conducted, where all messages sent of duty were redacted out, which found that most messages were not work related and thereby Quon was disciplined for violation of OPD rules. Quon sued on grounds of Fourth Amendment violation. Trial court found that he did have reasonable expectation of privacy but, citing plurality opinion of *O'Connor v. Ortega* (1987)[101], determined that investigation was justified and reasonable under work-related grounds. Court of Appeals did not agree that the investigation was reasonable even under legitimate work-related grounds. The Supreme Court assumed that Quon had reasonable expectation of privacy, though whether it was really so remained questionable. The Court noted rapid development of telecommunication and indicated that "[p]rudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."[102] Therefore, the assumptions were made to tailor the decision into this particular case. And then they examined the reasonableness of "search" made by the department of his text exchanges. They found that it, in fact, was reasonable for it was done under legitimate, work-related purposes, was not excessively intrusive and tailored to the specific purpose of the search. Furthermore, the Court noted that it would be a similar investigation would be normal if a private company conducted it on their own personnel.

To finally sum up, search of phone content as well as listening to conversations (be that text or voice) without a warrant is unreasonable under the Fourth Amendment, *Katz* and *Riley*. This applies to all situations, even if phone owner (suspect) is arrested, *Riley*. There are

[99] *City of Ontario, Cal. v. Quon*, 130 S.Ct. 2619 (2010)
[100] *Id*.
[101] *O'Connor v. Ortega*, 480 U.S. 709 (1987)
[102] *City of Ontario, Cal, v. Quon,* 130 S.Ct. 2619, 2629 (2010)

exceptions – the phone physically could be searched by an officer if it is incident to arrest, *Riley*. Also, the text conversations could be "searched" if government acts as an employer and acts under legitimate, work-related purposes and this search is not overly intrusive, *Ontario*.

Next, the study will analyze if provisions of PATIOT Act Section 215 together with FISA Amendments Section 702 are compatible with the Fourth Amendment, as currently interpreted by the Court.

CHAPTER II

SURVEILLANCE UNDER SECTION 215

This chapter will analyze the history of Section 215 of the USA PATRIOT Act, assess its value and constitutionality using the precedents analyzed in the previous chapter.

The discussion of Constitutionality of Sections 215 of the USA PATRIOT Act (Patriot Act) and 702 of FISA Amendments Act (FAA) requires us to discuss in detail what these sections entail. This is vital not only because it will be fundamental for reader's comprehension of the issue at hand but to avoid "value to national security" argumentation by possible critics. This sub-chapter intends, to the best of study's length constraints, to track the development of the circumstances around Section 215 and discuss its value to the war on terror. To this end, reports issued by Privacy and Civil Liberties Oversight Board (PCLOB) will be used and supplemented with further analysis and discussions.

> "The PCLOB is an independent bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007. The Board is comprised of four part-time members and a full-time chairman, all appointed by the President and confirmed by the Senate. The Board's authorizing statute gives it two primary responsibilities:
>
> To analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
>
> To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism." [103,104]

On January 23, 2014, PCLOB published a *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*. In this report, the PCLOB provides description and history of the NSA Section 215 Program, together with statutory and constitutional analysis thereof, concluding with recommendations regarding the program.

As it turned out, Section 215 is, actually, not the initiating statute of the phone surveillance – it was initiated by the President's Surveillance Program (hereinafter referred to as

[103] David Medine et al., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, Privacy and Civil Liberties Oversight Board (2014), 2; *See* Pub. L. No. 110-53, §801(a) (codified at 42 U.S.C. §2000ee)

[104] Notably enough, since August 2012 PCLOB did not function but was completely reconstituted merely "five days before news stories based upon the NSA leaks began to appear." ***See*** (PCLOB publication p.4)

"PSP"). In October 2001, President George W. Bush issued "highly classified" authorization "to collect certain foreign intelligence by electronic surveillance…without judicial warrants or court orders for limited number of days."[105] With this order NSA was authorized (1) to collect contents of "certain international communications" and (2) collect bulk metadata of telephone and Internet communications.[106] These authorizations were renewed "every thirty to sixty days" until 2007.[107]

Unclassified Report, prepared by the Office of Inspectors General of the DOD, DOJ, CIA, NSA and ODNI, stated that said "program became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool."[108]

In March 2004 after reassessment of the program by Office of Legal Counsel (hereinafter referred to as "OLC") and lengthy discussions within the Administration, President discontinued bulk collection of *Internet* metadata under PSP.[109]

It is imperative to understand what "metadata" means and entails in this context. Metadata can be described as "data about data" for it is basically information on communication without communication content in it. In regards to phone communication, metadata serves as information a pen register, discussed in *Smith v. Maryland* (1979)[110], would usually yield – numbers, dates, duration and time. In regards to Internet communication, metadata usually refers to information on senders and receivers of messages.

In December 2005, the *New York Times* (hereinafter referred to as "NYT") published a number of articles revealing interception of contents of international email and phone communication authorized by the PSP. These, as it shall be discussed later, will be transferred, through FISA Amendments Act, under authority of Section 702 of Foreign Intelligence Surveillance Act (hereinafter referred to as "FISA"). Though the concerns of the phone companies were calmed down after "white paper" issued by the government in response to the said articles, they were uneasy about pen registers not mentioned in the articles. *USA Today* began investigation on metadata collection in the beginning of 2006.[111] In May 2006, government started transition of metadata collection from PSP to FISA "business records" (hereinafter referred to as "BR") provision.

FISA BR provision, enacted in 1998, allowed FBI to apply for FISA court order requiring a business "to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism."[112] Orders could be applied to four types of businesses only – "a common carrier, public accommodation facility, physical

---

[105] David Medine et al., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, Privacy and Civil Liberties Oversight Board (2014), 37
[106] *Id.*
[107] *Id.*
[108] It should be clarified that report was issued in 2009. David Medine et al. *supra note* 104
[109] David Medine et al. *supra note* 104., *38*
[110] *Smith v. Maryland*, 442 U.S. 735 (1979)
[111] David Medine et al., *supra note* 104, at 40
[112] 50 U.S.C. §1862(a) (2000)

storage facility, or vehicle rental facility."[113] "Any application for such order was required to attest that there were specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[114]

Patriot Act's Section 215 expanded the FISA BR provision substantially. FBI was no longer limited to four types of businesses. Now, it could apply for an order requiring the production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism."[115] The law qualifies this rule stating that these can be done as long as the motive for it is not based "solely on the basis of activities protected by the First Amendment to the Constitution."[116] FBI also no longer needed to demonstrate "specific and articulable facts". Instead, they just needed to "specify that the records were being sought 'for an authorized investigation' conducted under guidelines approved by the Attorney General."[117] However, these measures were intended to be temporary and set to expire in 2005 (later extended to 2006).[118]

The debates on reauthorization of Section 215 of Patriot Act began in 2005. These were taking place at the same time as those regarding limitation of scope of Section 215 and transfer of metadata collection under PSP to Section 215.[119] Because PSP was classified, public discourse was evaded.

As a result, the Act was amended to require FISA courts to issue BR orders after determination that sought records were "likely relevant" to FBI investigation.[120] Also, the items that could be obtained were have to be "obtainable through grand jury subpoenas, administrative subpoenas, or court orders."[121] In March 2006, President Bush signed the amendments to the Act into law. By May of the same year, Congress renewed Section 215. At the same month, the government completed their application with supporting memoranda to the FISA court.

Referring to the word "relevant" in the law, the government argued that deference should be given to "the fully considered judgment of the executive branch" in assessing what is relevant.[122] They also argued that interpreting this word Supreme Court's 'special needs' jurisprudence must be used, "which balances any intrusion into privacy against the government interest at stake to determine whether a warrant or individualized suspicion is required."[123] This

---

[113] *Id.*
[114] (*Internal quotation marks omitted*) Report pages 40-41 (50 U.S.C. §1862(b)(2)(B) (2000)) (as cited by the PCLOB)
[115] Report page 41. 50 U.S.C. §1861(a) (1) (2002) (as cited by the PCLOB); ***see also*** Steven G. Stransky, *The Fourth Amendment and Bulk Telephone Metadata: An Overview of Recent Case Law*, 35 Saint Louis University Public Law Review 3 (2015).
[116] 50 U.S.C. § 1861(a)(1), (c).
[117] David Medine et al. *supra note* 104,. at 41; 50 U.S.C. §1861(b) (2) (2002) (as cited by the PCLOB)
[118] David Medine et al. *supra note* 104,. at 41
[119] *Id*
[120] *Id.*, at 42
[121] *Id.*
[122] *Id.*
[123] *Id*, at 44

means that if NSA says that the application is relevant the Court must take it as granted because NSA "knows better" and *any* intrusion into privacy is justified.

Furthermore, even though an immense amount of information is related to non-terrorist activities and persons, all information is still relevant for later analysis.[124] It must be admitted, this explanation is a bit confusing for we do not know why would they need so much information about innocent civilians for "later analysis". Is it to know with whom did those civilians communicate after they communicated with a terrorist they never knew he/she could be capable of such things? Or is it because potentially everyone can become a terrorist, so NSA better to know with whom they communicated before and after right away?

As duly noted by Stephanie Pell and Christopher Soghoian, from Stanford and Yale Law Schools respectively, "common sense" reading of the law, of Section 215, "does not, on its face, appear to permit collection on this scale."[125] They explain, as does the author of this study, that a great database with the metadata of virtually every American cannot be deemed relevant because only "*some* of the records in that database are actually relevant to an investigation."[126] David Medine, Jim Dempsey and Patricia Wald, from the PCLOB, also agree with this assessment and submit that practice of Section 215 does not comply to its own statutory language.[127]

It must be noted that these memoranda heavily relied on a past decision of FISC on internet metadata collection ignoring the fact that records were acquired only if they travelled through certain designated communications channels (likely to be) related to terrorist activity so to be "richly populated" with terrorism related communications.[128] What we do know, from the White Paper published by the Obama Administration in 2013, is that the program was designed to allow queries into the data be only on "identifiers" "that [are] associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court."[129] However, the approval of the Court looks more as formality before the Constitution rather than safeguarding mechanism. Also it ignored the discussion that it was FBI to apply for orders and obtain the records, under Section 215.

Judge Malcolm J. Howard signed an order approving the government application and in his order included the requirement that "records could be searched only with selections terms for which there already was 'reasonable, articulable suspicion' [(hereinafter referred to as "RAS"] of connection with terrorism."[130]

---

[124] *Id.*

[125] Stephanie Pell and Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 Yale Journal of Law and Technology 134, 138 (2013)

[126] *Id*, at 139 (the italics preserved from the original); ***see*** Orin Kerr, *The Problem With the Administration "White Paper" on the Telephony Metadata Program*, VOLOKH CONSPIRACY (Aug. 12, 2013, 2:34 PM), http://www.volokh.com/2013/08/12/problem-withthe-administration-white-paper-on-the-telephony-metadata-program

[127] David Medine et al., *supra note* 104, at 10

[128] *Id.*, at 39

[129] Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT ACT (Aug. 9, 2013) [hereinafter, "White Paper"], https://www.eff.org/document/administration-white-paper-section-215-patriot-act

[130] David Medine et al., *supra note* 104, at 46

So, collection of metadata under PSP continued without a break but now under Section 215 of Patriot Act.

Another fundamental thing to note is that FISA orders as they were operated (issued as blanket orders for 90 days subject to renewal) are questionable under the Fourth Amendment. Justice Douglas in *Katz v. US* concurring opinion noted that even in matters of "national security" members of the executive branch, be that President or Attorney General, cannot be an independent or detached magistrate. Therefore, applying it to this case, FISC was established to serve as such and issue orders on case-by-case basis. The most important reason is that rights under the Fourth Amendment belong to everyone in the United States and not the American society in general, as a unitary group. As it is and will be seen, the FISC has given the power of determination whether a person falls within RAS to the executive and the FISC serves as a mere formality. This also ignoring the fact that RAS is a generic standard that can be easily met having a decent legal advising and, especially, having all possible information on person and his/her contacts.

The acceptance of such practice by Courts leads to a dangerous precedent where any interception of communication that passes through a third-party by the sole decision of the executive can be acceptable if it does not intercept spoken or written words. "After the PATRIOT Act broadened the definitional section of the Pen/Trap statute, DOJ interpreted the statute to authorize the collection of nearly all non-content information exchanged between a mobile device and a cell tower and, accordingly, advised prosecutors to obtain a Pen/Trap order when employing IMSI-catchers in an investigation."[131] These IMSI-catchers are a more advanced technology used by law enforcement agencies to intercept in real time "unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier."[132] This technology can potentially send signals through the walls to locate and identify cell phones without service provider assistance or anyone knowing about that.[133]

It is also imperative for the reader to understand the chaining system, can also be called "hop" system. As soon as an analyst puts a search term into the system, he/she will get information on all numbers directly in contact with the target (first hop), he/she will get information on all numbers directly in contact with all those numbers (second hop) and then all contacts directly in contact with those (third hop).[134] As it stood since the beginning of operation of this program under Section 215, three hop search was permitted and any search beyond would be stopped by the software.

a. Noncompliance or just blunt violations of law

[131] Stephanie Pell and Christopher Soghoian, *supra note* 124, at 143
[132] *Id*, at 142
[133] *Id*, at 143
[134] David Medine et al., *supra note* 104, at 9

Contrary to sworn attestations of several executive branch officials who filed declarations with the FISC about NSA's program, NSA violated FISC orders regarding Section 215. In particular, NSA violated the requirement that analyst query only those who have been RAS approved.

At the time of PSP, NSA has developed and implemented a software system named "alert list". This system would scan new telephone records as soon as those would be input into the agency's database. There were thousands of numbers of interest for NSA analysts but most of those have never been RAS approved. "As of January 2009, fewer than 2,000 of the nearly 18,000 numbers on the alert list were RAS-approved."[135] This is whilst accepting the fact that it is not an independent magistrate that is approving the RAS but the NSA officials themselves.[136]

After NSA notified FISC of the problem, the problem was attempted to be fixed but for the lack of success of doing so it was shut down. The government reasoned that these problems were due to misunderstanding of personnel of FISC order. Judge Walton noted that "since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS approved telephone identifiers on its alert list against the BR metadata in order to identify any matches…It is difficult to imagine why the Court would intend the applicability of the RAS requirement – a critical component of the procedures proposed by the government and adopted by the Court – to turn on whether or not data being accessed has been 'archived' by the NSA in a particular database at the time of access…[Such an] illogical interpretation renders compliance with the RAS requirement merely optional."[137]

Furthermore, "[d]uring a five-day period in April 2008, the NSA determined, thirty-one NSA analysts queried the telephone records database without being aware they were doing so."[138] Then NSA created modified access tool, which had to be installed by every analyst. In December 2008 one such analyst failed to install it and "inadvertently queried the data using five identifiers for which NSA had not determined that the reasonable articulable suspicion standard was satisfied."[139] With further investigations, more violations of orders have been found by the NSA.

Responding to those violations, Judge Walton "wrote that he no longer had confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders."[140] Because the government insisted that this program is crucial to national security, he was hesitant to order its stop. So, instead, Judge ordered that every search

---

[135] *Id*, 47; Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harvard Journal of Law and Public Policy 757, 811 (2014).

[136] In other words, even though the Fourth Amendment's requirements were already ignored, the NSA managed to violate even this little formality.

[137] *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Mar. 2, 2009), Order at 5, *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf

[138] David Medine et al., supra note 104, at 50, quoting *In re Production of Tangible Things*, Order at 9 (Internal quotation marks omitted)

[139] *In re Production of Tangible Things, supra note* 136, Order at 5

[140] *Id*, Order at 12

should be approved by Court – an approach, in author's opinion, most appropriate in respect to the Fourth Amendment to the U.S. Constitution.

But NSA did not stop there. In violation of FISC orders and "generally applicable dissemination rules governing all of the NSA's activities[,]" the agency has inappropriately disseminated information to other intelligence agencies without minimization procedures.[141] NSA notified the Court that access to those records has been terminated.

In August 2009, Agency claimed to FISC that it was doing its best to minimize risks of further violations by imposing expanded rules and restrictions. And then, the Agency applied to be the one to determine if RAS standard has been satisfied or not, again. In September, Judge Walton granted the application and Section 215 program continued as before.

b. Value and USA FREEDOM Act

> "[W]e conclude that the Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program." [142]

In June 2015, USA FREEDOM Act (Freedom Act) was passed ending bulk collection of metadata. However, please do note that metadata collection by itself under Section 215 did not end. It means that now the intelligence community will not be acquiring and storing metadata in bulks in their archives. Beginning November 2015, government under authorization of FISC after identifying "specific selection term" reasonably associated with terrorism can acquire call detail records up to two hops from telephone companies.

c. Constitutionality

Seeing how the technology works it might be tempting to believe that Section 215 falls within the working precedent of the Fourth Amendment as regarding phone surveillance. After all, Section 215 does not record conversations and merely records numbers dialed by a user. These numbers, under precedent, are information transmitted to a third-party and, therefore, are

[141] David Medine et al. *supra note* 104, at 53
[142] David Medine et al., *supra note* 104, at 11

void of any protection of the Fourth Amendment. Inquiry for these numbers, subsequently, do not qualify as search. However, this subsection will try to illustrate that, despite little technical similarities, operations under Section 215 are different from pen-registry allowed under *Smith*, that they should be qualified as search, assessed its reasonableness and examined under reasonable expectation of privacy doctrine.

It is true that by not recording the actual conversations, Section 215 resembles pen-register. However, in such intricate matters, one assessing the constitutionality should look beyond first glance resemblance. This is primarily because the opinion given by the Court was detailed in outlining what pen-register did and, therefore, what they subsequently permit with their decision.[143]

> "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose *only the telephone numbers* that have been dialed -- a means of establishing communication. Neither the *purport* of any communication between the caller and the recipient of the call, their identities, *nor whether the call was even completed* is disclosed by pen registers."[144]

Compare that to Section 215. Under FISA orders, "all call detail records" are being collected by the NSA. These "typically include much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers."[145]

This methodology can be problematic and lead to inaccuracies in interpretation. To illustrate that, a hypothetical can be used. Suppose there is Mr. Bruce Wayne and law enforcement has an investigation on him relating to his suspected ties to terrorists. By using pen register on Mr. Wayne, the law enforcement could see only the numbers he dialed, without further knowledge if there was any conversation at all. Obviously, by using pen register only they will never find Mr. Wayne calling terrorists, for he is a superhero – the Batman. Under Section 215 Program, on the other hand, the NSA would know not only of the attempted calls "but also the precise duration and time of each call."[146] Furthermore, the Agency would be able to access the same records of all the numbers Mr. Wayne was in contact with, and of all those who were in contact with them. These all include not only outgoing but incoming calls too. Now suppose that Mr. Wayne contacted Mr. Luthor on some occasion asking about what he did to his significant other. Then, on a completely separate occasion, Mr. Luthor contacts an Arab prince negotiating a large oil deal. The mentioned prince then contacts a known terrorist. Then, hypothetically, NSA has a confirmation (significant or not) to their suspicions that Mr. Wayne has some indirect ties to terrorism.

---

[143] In *Smith v. Maryland*, 442 U.S. 735 (1979)
[144] *United States* v. *New York Tel. Co*., 434 U.S. 159, 166 (1977)
[145] David Medine et al., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, Privacy and Civil Liberties Oversight Board (2014), at 8
[146] *Id*, at 115

Another hypothetical will illustrate the "mosaic theory" problem. Forget about terrorism aims and just look at how much can metadata really give us. Suppose that looking at one's usual behavior, law enforcement (or anyone for that matter) can observe an unusual spike in gynecologist calls, followed by calls to or from husband. Later, records indicate calls from and to Mothercare store. Next, several months later, records indicate an unusual flow of calls to subject's and her husband's phones. These phone numbers belong to parents, supposed relatives and friends. We can also see calls from maternity home. Furthermore, we see unusual calls to a flower shop and delivery service. We note in both spouse's records spike in calls to their supposed place of employment. We note calls to and from an insurance company. We can also see an increase in calls to people either related to medical field or pediatricians themselves. Though records do not identify people's names, this can be done through reverse telephone directories for which a warrant is not required.[147] Thus, circumstances of a particular call, calls or pattern of calls can be highly suggestive of their content and, subsequently, reveal most intimate details of one's life – details for which a caller has a reasonable expectation of privacy. And the longer the surveillance is, the more it reveals. So, if surveillance were only a week, there would probably not be as many clues to suggest that the subject is having a child.

This problem is vividly illustrated in *United States v. Jones* (2012)[148]. However, for the illustration's purpose, the best explanation of the problem is given not by Justice Sotomayor's opinion[149] but in the opinion of Judge Ginsburg from D.C. Circuit Court:

> "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups--and not just one such fact about a person, but all such facts."[150]

In fact, a former general counsel of the NSA, Stewart Baker, was quoted saying, "Metadata absolutely tells you everything about somebody's life…[It's] sort of embarrassing how predictable we are as human beings…If you have enough metadata you don't really need content."[151] But why is it government's fault that all this metadata gives so much information? Government, after all, just does its job in protecting national security, in protecting us. But

[147] *Id*, at 22.
[148] *United States v. Jones*, 132 S.Ct. 945 (2012)
[149] ***See*** page 17 of the current study
[150] *United States v. Maynard(/Jones)*, 615 F.3d 544 (D.C. Cir. 2010)
[151] David Medine et al. supra note 104, at 158

"government's rampant misuse of its surveillance authority during the twentieth century to squelch domestic dissent in the name of national security was amply documented by the reports of the Church Committee, and was in fact the impetus for passage of the Foreign Intelligence Surveillance Act."[152] Therefore, to protect the constitutional rights the Framers wanted the People of the United States to have, practice of law enforcement should adapt to the new realities.

In *Riley*, the Court affirmed that with today's development of technology, phones became an irreplaceable part of human life. "[C]ell phones…are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[153] Court further noted the storage capacity of phones and found that access to one's phone data constitutes a search:

> "One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. […] Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant"[154]

In this case, we have not only log of messages but also log of calls supplied to the NSA every day and stored for five years. If we apply the metaphor used by the Court, then NSA is taking millions of pages' worth of log- and phonebooks, without warrant. Looking at violation statistics, these searches are many times of innocent people not connected to terrorism in any way.

Now that we have Freedom Act, bulk collection of metadata ceased. NSA is also not able to access or retain the record archives on their own servers. Nonetheless, records are still being provided on a daily basis. Thus, mosaic-theory problem persists. If we follow *Riley's* opinion's logic, then it is likely that even reformed practice[155] of Section 215 could be found in violation of the Fourth and Fourteenth Amendment.

A most practical solution would be to set a defined and short time limit for surveillance warrants, subject to renewal but only under a stricter standard showing the progress from the last warrant, explaining why is the individual still suspected and how much more time do they need to take action. This would stimulate law enforcement to limit the number and increase quality of searches, allowing only for result yielding pursuits, and decrease number people under constant surveillance. Another choice is for Court to apply strict scrutiny test on electronic surveillance cases such as this. Analysis of PCLOB found violations of First and Fourth Amendment with

[152] *Id*, at 160
[153] *Riley v. California*, 134 S.Ct. 2473, at 2484 (2014)
[154] *Id.*, at 2489.
[155] As with Freedom Act

Section 215. Discriminatory practice of searches based on race or religion are also observed.[156] Therefore, application of strict scrutiny seems fit for Section 215.

[156] Spied on for Being Muslim? NSA Targets Named in Snowden Leaks Respond to U.S. Gov't Surveillance, Democracy Now!, https://www.democracynow.org/2014/7/10/spied_on_for_being_muslim_nsa (last visited May 19, 2017).

CHAPTER III

SURVEILLANCE UNDER SECTION 702

Following the Chapter on Section 215, it is now pertinent to the study to analyze Section 702 of FISA Amendments Act in the similar fashion. Analogous to the previous one, this Chapter will discuss history, assess its value and constitutionality. While analyzing constitutionality, in contrast to the previous chapter, the author will use some cases from lower Federal courts.

Section 215, in fact, shares common history with Section 702. As we already saw, these operations conducted under them started with the PSP - long before they were codified in FISA or Patriot Act. And they continued to be untouchable as president was continuously renewing them "with some modifications and constrictions to the scope of the authorized collection, approximately every thirty to sixty days until 2007."[157] Justifying the renewal with constant and ongoing extraordinary emergency. The legislature and FISC were only briefed on the existence of the program.

As a reminder, in December 2005, the PSP was revealed through a series of articles in the NYT, which had international communications interception as the center of their attention. Though the government issued "white paper" outlining that the President had the authority to issue the PSP, it, nonetheless, went on to seek authorization for electronic surveillance through FISC. They requested FISC to issue the orders authorizing the surveillance with the *government* to make probable cause determinations. Court granted the order. This was "referred to as the 'Foreign Telephone and Email Order,' [which] in effect replaced the President's authorization of the [PSP], and the President made no further reauthorizations of the [PSP]."[158] But the Judge of the FISC changed, and the new judge modified the Foreign Telephone and Email Order, making the *court* to make probable cause determinations instead of the *government*. The government contested that these modifications created "intelligence gap". [159]

The government attempted to make another effort. They wanted to use FISC to obtain orders authorizing compelling private companies "to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States–based communication service providers."[160] Government contended that there were rigorous tests applied in order to gain FISA orders, showing that the targets were

[157] David Medine et al., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board (2014), at 16
[158] *Id.*, at 17
[159] *Id,* 18
[160] *Id*., Statement of Kenneth L. Wainstein (6-7) http://www.intelligence.senate.gov/070501/wainstein.pdf.

"agents of foreign power", located outside the United States and "communications being sought were frequently with other who were also located outside the United States."[161]

These new hassles "slowed and in some cases prevented the acquisition of foreign intelligence information."[162] Protect of America Act of 2007 and FISA Amendments Act of 2008, eliminated the need to seek individual authorizations for surveillance. These are of particular importance to our study today.

Report by the Director on National Intelligence to Congress reported that "Foreign Telephone and Email Order had resulted in degraded acquisition of communications, combined with reports of a heightened terrorist threat environment."[163] This was intended to speed up Congress in passing a more 'suitable' legislation. It succeeded. In August 2007, Protect America Act (PAA) was passed by Congress and signed by the President. PAA was "a legislative forerunner to what is now Section 702 of FISA."[164] The perk of the new law was that it was to live only for 180 days.

And suddenly, PAA united those both attempted forces that the government put into place into one. And PAA being only a temporary measure, Congress started working on the permanent one. In July 2008, FISA Amendments Act was signed into law, which "replaced the expired Protect America Act provisions with the new Section 702 of FISA."[165] Despite all the problems the reader already sees and the study will discuss below, FAA is more legitimate than PSP for the only reason that it was passed through legitimate legislative means.

What is the scope of Section 702? FISA sanctions Attorney General and the Director of National Security to jointly authorize:

1. "[T]argeting of persons who are not United States persons,
2. "[W]ho are reasonably believed to be located outside the United States,
3. "[W]ith the compelled assistance of an electronic communication service provider,
4. "[I]n order to acquire foreign intelligence information."[166]

As in any legislation there are definitions and limitations. Persons, mentioned, might be "groups, entities, associations, corporations, or foreign powers."[167] The foreign powers might be governments but not the whole nations. Accordingly, 50 U.S.C. §1801(i) defines what US person is – it is US citizen, permanent resident, virtually all US corporations and groups substantially composed of US citizens and permanent residents. Furthermore, no person located in the United States can be targeted, nor can the government target a foreign entity "if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United

[161] *Id*.
[162] *Id*.
[163] *Id,* 19 (internal quotations omitted)
[164] *Id*
[165] *Id*, at 20
[166] *Id*, at 20; 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi).
[167] David Medine et al., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board (2014), at 21

States."[168] Surveillance can be authorized only to acquire foreign intelligence information. "Foreign intelligence information concerning non-U.S. persons is defined in FISA as information that relates to the ability of the United States to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power."[169]

In contrast to FISA, FAA does not require the government to show probable cause to believe that the surveillance target is a foreign power or agent.[170] Actually, the mere fact that data in a device is encrypted already makes it a subject of collection, interception and storage of this data.[171] Also, though the targets should have been outside the United States, the interception location was never specified.[172] For example, the communication intercepted transited through the United States but the two persons targeted are non-US persons located outside the United States. Or the two targeted non-US persons in their intercepted communication are discussing a US person. Or because of a simple mistake, the target is a US person. But this US person cannot be intentionally targeted.[173]

Furthermore, the compliance oversight with the statutory requirements were effectively transited from the FISC to Attorney General or the Director of National Intelligence.[174] Thereby, Section 702 decreased the level of judicial monitoring.

Every year, the Attorney General and Director of National Intelligence make certifications to the FISC seeking authorization for targeting non-US persons reasonably believed to be located outside the United States to gather foreign intelligence information. It must be noted that specifics to what person(s) in particular, where and how is targeted are not required.[175] Instead, categories of foreign intelligence information are identified. But these procedures and certifications might be of no real legal use and just a mere formality, for the FISC does not determine if any of the standards were met. What the FISC determines is if minimization procedures have satisfied the set criteria and the "procedures are reasonably designed to ensure compliance with certain limitations."[176] These limitations include, but of course not limited to, intentional acquisition of wholly domestic communications. Minimization procedures are aimed to control "acquisition, retention, and dissemination of any non-publicly

---

[168] 50 U.S.C. § 1881a(b)(2)
[169] David Medine et al., supra note 166, at 22; 50 U.S.C. § 1801(e)(1)
[170] Patrick Walsh, *Stepping On (or Over) the Constitution's Line: Evaluating FISA Section 702 in a World of Hanging "Reasonableness" under the Fourth Amendment*, 18 NYU Journal of Legislation and Public Policy 741, at 758 (2015); *Amnesty Int'l USA v. Clapper,* 638 F.3d 118 (2nd. Cir. 2011), at 124; *The Supreme Court - Leading Cases*, 127 Harvard Law Review 298, at 299 (2013).
[171] Jeffrey L. Vagle, *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 Indiana Law Journal 101 (2015).
[172] Patrick Walsh, *supra note* 169, at 757
[173] ***See*** David Medine et al., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board (2014), 21 footnote 49
[174] *The Supreme Court - Leading Cases*, 127 Harvard Law Review 298, at 299 (2013).; Peter Beaudette Jr., *Compliance without Credit: National Security Agency and the International Right to Privacy,* 73 Air Force Law Review 25, at 31.
[175] *The Supreme Court - Leading Cases*, 127 Harvard Law Review 298, at 299 (2013).
[176] David Medine et al., *supra note* 166, at 27

available US person information acquired through the Section 702 program."[177]And after analysis, the FISC should determine if the acquisition meets Fourth Amendment requirements and issue a written opinion on why it does. Seeing that the program still exists even after Snowden leaks, the Courts might be really ones to blame for their traditional deference of national security matters to the executive. As we shall see below, there is a chance that this deference is slowly ending.

After order authorizing acquisition has been granted, the Attorney General and DNI send directives to communication providers to compel their cooperation in interception of these communications. These providers can protest and appeal the decision of FISC to the FISCR and then to the Supreme Court.

The process of surveillance is similar to one under Section 215 of Patriot Act. Here, too, the people are targets and their communication means (e.g. phone numbers or email addresses) are selectors (which are tasked). And though tasking process is individualized, in 2013 alone 89,138 persons were targeted under Section 702.[178] There are two types of acquisition under Section 702 – PRISM and "upstream" collection.

Under PRISM, the government (NSA on behalf of FBI) submits to communication service provider, that received the directive, the selector. In turn, the service provider should provide the government with all communications to or from the selector until the selector is "detasked". The raw data can then be provided to the FBI and CIA. In all agencies, the agents then are analyzing the data to ensure compliance with minimization processes and targeting requirements before surveillance is uploaded to database. External compliance oversight is further executed by the DOJ and ODNI. If any noncompliance is found, they need to report those to Congress.[179]

Under "upstream" collection, the government does not compel the service providers to submit data but instead the communication transit providers. "Upstream" is similar to the Olmstead case wiretapping. The government did not bug the phone itself, instead they took the contents of conversations from the wires, which connect the caller and receiver. However, in contrast to targeted wiretapping, "entire streams of Internet traffic flowing across major U.S. networks are acquired and searched."[180] In contrast to PRISM, FBI and CIA do not receive the raw data from upstream collection. The filters of tasking and minimization apply though too before the information is then uploaded to databases.[181]

In addition to seeing what emails were sent from or received to the selector, the NSA is collecting "about" communication, which means that NSA can intercept communication of

[177] *Id*, at 26; 50 U.S.C. § 1881a(e)(1), (g)(2)(A)(ii), (g)(2)(B).
[178] Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, The Washington Post (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.
[179] David Medine et al., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board (2014), at 8, 52
[180] *United States v. Mohamud*, 843 F. 3d 438 (2016)
[181] David Medine et al., (Section 702) *supra note* 166., *at* 35-41

persons in the United States who just mention the target or selector. But the enforcement agencies and the PCLOB claim that special minimization measures are applied there too not to obtain strictly domestic communication, such as IP filter.[182] But, according to the government and the PCLOB, the system is not perfect and there are tens of thousands wholly domestic communications intercepted per year. Though it is tempting to discuss more, there is no need for that for as of May 1, 2017 (while this work is being written) the "about" collection has been discontinued by the NSA.[183]

Also, there are Multi-Communication Transactions. These are communications initiated by a targeted non-US person outside the United States but then sent to the United States persons. These messages may further be exchanged exclusively between US persons and the target may no longer be even involved in the communication.

Unfortunately, unlike with Section 215, PCLOB did not report extensive violations of public trust and compliance. They report that less than one percent of all inquiries are incidents of noncompliance since the inception of Section 702. Not wanting to commit a fallacy of composition, the nature of said violations should at least be noted, as reported by the PCLOB. Most common types were just delay in reporting of tasking and detasking to the DOJ and ODNI, or wrong selectors due to typographic errors. They also noted only two instances of reverse targeting. Other incidents, which were noted to be rare, involve systemic errors, such as those involving MCT or technological malfunction, and analysts targeting individuals without approval. However, the latter one is an important and dangerous noncompliance instance. Council on Foreign Relations reports that it is estimated that millions of Americans are targeted through Section 702. The interception of President Trump's campaign workers' communications that tie them to Russia, generated further concern that Section 702 can be used for political gain.[184] Therefore, the real objectivity of PCLOB, in assessing the noncompliance and unconstitutionality of Section 702, is questionable. If anything, the estimates and facts that are seen today with "Russia hacking the U.S. election" fiasco, Section 702 has shown itself to be a dangerous unregulated weapon in the hands of the executive without any check.

The most important part of Section 702 is 50 U.S.C. §1881a(b)(5). It stipulates that surveillance acquisition "shall be conducted in a manner consistent with the Fourth amendment to the Constitution of the United States." Therefore, the next step of the study will do that indeed.

a. Constitutionality

[182] *Id., at* 36-37

[183] Adam Klein, *The End of "About" Collection under Section 702*, Lawfare (May 1, 2017, 10:07 AM), https://www.lawfareblog.com/end-about-collection-under-section-702.

[184] Laura K. Donohue, *THE CASE FOR REFORMING SECTION 702 OF U.S. FOREIGN INTELLIGENCE SURVEILLANCE LAW*, COUNCIL ON FOREIGN RELATIONS (JUNE 26, 2017), https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law; Dustin Volz, *Trumps Russian imbroglio prompts Republican rethink on surveillance law*, Reuters (March 21, 2017, 3:52 AM), http://www.reuters.com/article/us-usa-trump-russia-surveillance-idUSKBN16R2O1.

There are few cases up to date, or as far as it was found, that analyze the constitutionality of Section 702. It must be noted that they none of them ended up in the Supreme Court, at least yet.[185] Nonetheless, they are of interest for our analysis, for even the Supreme Court narrates the precedents.

Analysis of this section would be more extensive and complex than the previous one. There are many reasons for that. One is the complexity of Section 702 with all the safeguards put in place. Another is that the targets of Section 702 are foreigners located outside the United States who do not have Fourth Amendment protection.

In the beginning of the first story there is a 19-year-old young man. In February 2009, Mohamed Osman Mohamud, naturalized US citizen from Somalia, began exchanging emails with, now deceased, al-Qaeda member.[186] He was also in communication with a convicted terrorist in Saudi Arabia. In the latter communications, both discussed Mohamud's trip to Pakistan and terrorist training. The trip never happened and FBI began their undercover operation. Mohamud and undercover agents made trial trips to detonate bombs and then FBI agents asked "what he hoped would happen to those attending the Portland holiday ceremony, a family event that includes people of all ages." "I want whoever is attending that event to leave ... either dead or injured," said Mohamud. FBI implanted a fake bomb into the van, that Mohamud believed would blow up in the most public place in Oregon.

Evidence presented at the trial hearing, as it is evident from the retelling, was obtained through Section 702 surveillance. The problem is that the government "failed to notify the defendant that there was section 702 evidence against him, but provided notice only of evidence collected pursuant to other section of FISA."[187] In appeal of this decision, argued in U.S. Circuit Court of Appeals for Ninth Circuit, Mohamud pushed for recognition of many Constitutional encroachments on behalf of the government and Section 702 in particular, including separation of powers, First and Fourth Amendment violations. Due to space constraints, only Fourth Amendment aspect will be discussed.

The Court found no violation of the Fourth Amendment *in this case*. "Although § 702 potentially raises complex statutory and constitutional issues, this case does not. […] the initial collection of Mohamud's email communications did not involve so-called "upstreaming" or targeting of Mohamud under § 702, more controversial methods of collecting information. It also did not involve the retention and querying of incidentally collected communications."[188] This is important because for now it is the highest federal court that cast a doubt on constitutionality of Section 702 (and of pre-Freedom Act Section 215). The court, with this decision, codified the worries of the PCLOB. Up to date, it is the largest and most important recognition of the fact that collection of US persons' communication under Section 702 are not accidental, infrequent or

[185] There is a case of *Clapper v. Amnesty International* but the Supreme Court ruled that appellant does not have a standing, *see Clapper v. Amnesty International*, 568 U.S. ___ (2013)
[186] *USA V. MOHAMED MOHAMUD*, No. 14-30217 (9th Cir. 2016), at 423
[187] Patrick Walsh, *Stepping On (or Over) the Constitution's Line: Evaluating FISA Section 702 in a World of Hanging "Reasonableness" under the Fourth Amendment*, 18 NYU Journal of Legislation and Public Policy 741, at 759 (2015).
[188] *USA V. MOHAMED MOHAMUD*, No. 14-30217 (9th Cir. 2016), at 438

inconsequential. "[C]ommunications between foreign targets and U.S. persons was specifically contemplated and to some degree desired.…'incidental' collection of communications is not accidental, nor is it inadvertent…the term should not be understood to suggest that such collection is infrequent or that it is an inconsequential part of the Section 702 program"[189] The court, nonetheless, analyzed the reasonableness of the search under the Fourth Amendment. Using the legitimate balancing test (which resembles rational basis test[190]), where the legitimate government interest is balanced against "the degree to which [the search] intrudes upon an individual's privacy."[191] The only related criticism the author has on their analysis now is their implication that electronic communications, though recognized by this court equal to letters, have reduced expectation of privacy. But the quintessential aspect for Court's decision was that Mohamud's communication was sent to a third party, thereby diminishing Mohamud's expectation of privacy. But the Court did not address whether the disclosure of mails to a third party was voluntary one and whether that mattered. But we shall go on.

The other case involved two Uzbek refugees to United States (Jamshid Muhtorov and Bakhtiyor Jumaev). Ironically, one of the convicts of this case, Jamshid Muhtorov, was the head of human rights organization in Jizzakh who fled from prosecution (unrelated to terrorism) in Uzbekistan because of protection from lieutenant colonel of regional counter-terrorism squad.[192] These defendants were charged with provision of material support to a designated terrorist organization. Mr. Muhtorov, furthermore, was arrested on his one-way trip to Turkey due to surveillance information obtained through Section 702.

Here too, the U.S. District Court for the District of Colorado, recognized that "FAA is susceptible to unconstitutional application as an end-run around the Wiretap Act and the Fourth Amendment's prohibition against warrantless or unreasonable searches."[193] But, again, argued that in this case Section 702 was not unconstitutionally applied. Furthermore, it opened for discussion issue whether Section 702 violates Article III "case or controversy" requirement but did not discuss it, only stating that in this case it did not. And the collection of Mr. Muhtorov's communication was incidental to surveillance of Islamic Jihad Union (IJU), an international terrorist organization. Therefore, statutory and constitutional.

Even from the detached point of view, the analysis of Section 702 becomes too complex. This is for this very reason Supreme Court's ruling is needed.

In *Riley*, the Court already recognized the fast development of modern technology and that Constitutional protections should try to move with them. Even for an originalist this

---

[189] *Id*, at 440, citing PCLOB Report at 82 and 114 (internal quotations omitted)

[190] This test is of the same penumbra as strict scrutiny test. But in contrast to strict scrutiny, which is highest level of scrutiny and most deferential to the individual, this is a test most deferential to the government with lowest level of scrutiny. "The rational basis test contains two substantive limitations on legislative choice: legislative enactments must implicate legitimate goals, and the means chosen by the legislature must bear a rational relationship to those goals." *Lyng v. Int'l Union*, 485 U.S. 360, at 375 (1988)

[191] *USA V. MOHAMED MOHAMUD, supra note* 185, at 441, quoting (*Maryland v. King*, 133 S.Ct. 1958, 1970, 186 L. Ed. 2d 1 (2013))

[192] Uzbekistan: Jamshid Mukhtorov arrested in the USA and a former police officer from Uzbekistan used to be friends, Fergananews.Com, http://enews.fergananews.com/articles/2744 (last visited May 22, 2017).

[193] *United States v. Jamshid Muhtorov et al*., No. 12-cr-00033-JLK

argument seems plausible for people rarely send written letters to each other. Physical written communication is conducted usually for business matters. This is compared to, and in stark contrast to, extensive and, probably, exclusive use of letters in the 18th Century. The intent of Framers was to protect the privacy of communications and, therefore, it must be accepted that people receiving or sending electronic messages or using any other electronic communication have reasonable expectations of privacy – that the society has such reasonable expectation of privacy. This is true especially taking into account that FISA Court and 6th Circuit Court already treated electronic communication as letters ("Whether they are transmitted by letter, telephone or e-mail, a person's private communications are akin to personal papers").[194]

Also, there seems to still remain a question on whether US persons located abroad remain under Fourth Amendment protection (*see.* Walsh). However, this question was long settled with *Katz*. "The Fourth Amendment protects people, not places."[195] Therefore, targeting of US persons still remains unavailable under Section 702.

The next question comes to warrants. Fourth Amendment reads "and *no*[196] Warrants shall issue, *but upon*[197] probable cause." It remains a mystery to the author why do the Courts still debate on reasonableness of judicial procedure under FAA for it clearly violates the Fourth Amendment. Under FAA Section 702, government is not required to illustrate probable cause to FISC. Therefore, question raised by Muhtorov's case is viable one. As the Court itself recognized, "There would have been no "case or controversy" in *Tortorello* without Arthur Tortorello, and no "case or controversy" in *Camara* without Roland Camara."[198] This was said in relation that there is no judicial determination as to whether a person of interest can be subject to surveillance. Unfortunately, this Court did not analyze this issue extensively, for Muhtorov's communication was incidental to surveillance conducted on recognized terrorist organization.

We see similar language in the First Amendment, one might say, "Congress shall make *no*[199] law…abridging the freedom of speech, or of the press" but still not *all* speech is protected, such as incitement or defamation. Answering this reasonable objection, these are Court ruled exceptions to the law, while the Court allowed only few defined exceptions to warrant requirement and one still remains unaccounted for – national security. This study suggests that "national security" interest is vague and general, which renders the exception to become exception of the Fourth Amendment in general, for basically everything can be argued to be of national security matter.

In regards to reasonableness of Section 702 search, it remains always reasonable in cases that really have gone to Courts. This is because, at least most of the times, these cases involve crimes committed or conspired to be committed, which have strong evidence of connection of suspects with alleged crimes. Plus, great majority of such cases are public and subject to Fifth and Fourteenth Amendment's Due Process Clause. This study excludes cases conducted on

[194] 2011 U.S. Dist. LEXIS 157706, 2011 WL 10945618, at *26 (FISA Ct. Oct. 3, 2011)
[195] *Katz v. United States*, 389 U.S. 347 (1967)
[196] Emphasis added
[197] Emphasis added
[198] *United States v. Jamshid Muhtorov et al*., No. 12-cr-00033-JLK (2015), 22
[199] Emphasis added

terrorists litigated in military courts or even without litigation at all. Nonetheless, the reasonableness standard cannot be applied to cases where there are compliance issues or where government did not find any evidence for terrorism ties. In any other scenario where communication is targeted on non-US person outside the United States, or at least involves such person or organization – an argument can legitimately be made that the communication of US person obtained was "incidental" to permitted Section 702 surveillance.

A problem law enforcement may encounter is evidence of terrorism plot or ties obtained through Section 702 but through communication that was exclusively in the United States. This would make the interception of communication a violation of the Fourth Amendment and inadmissible in Court.

The only viable solutions author sees for these problems is bringing back the FISA warrant requirement back to its original form – to require presentation of probable cause for each target, or at least for those that have a slightest suspicion, or in the course of investigation was found, to be connected to US persons. Thereby, executive branch would increase its constitutional legitimacy with Section 702 and put itself within the requirements of the Fourth Amendment to the Constitution. Additionally, it will be prudent to cancel "upstream" collection of data for its great threat that most of the communication intercepted would be of US Persons unrelated to terrorism. Constitutionally, this "incidental" interception might justifiably be argued to be unreasonable search. Adaptation of these recommendations would slow down the intelligence work, as the government already argued. Nonetheless, this could be easily dealt with by increasing number of judges of FISC and their assistants, clerks. Allowing 24 hours of review would not put the nation in much greater danger. In case of emergency need, a process of expedited review can be devised and requested. Furthermore, technological modifications should be made to guarantee that analysts would not be able to insert selectors without FISC approval/warrant.

CHAPTER IV.

RIGHT TO PRIVACY AND THE COUNTER-TERRORISM EFFORTS IN THE EUROPEAN UNION

This Chapter will analyze the privacy rights and the counter-intelligence methods of two of the most populous, economically developed and politically influential countries in the European Union – France and the United Kingdom[200].

It is vital to note that, in contrast to the United States, the right to privacy in the European Union is codified and not implied or interpreted through precedents, like it is in the U.S. One can find the right to privacy in **Article 8 of European Convention on Human Rights**:

> 1. Everyone has the right to respect for his private 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.[201]

It is only prudent to give a brief introduction to the Convention and how applicable to individual European States it is.

As a response to horrendous experience of fascism and Nazism in Europe in the middle of the twentieth century, European States decided to bind themselves to an agreement establishing minimum standards of human rights in the continent. Furthermore, they set out to establish a judicial structure "whereby they could insure the identification and security of those rights."[202] European Nations drafted European Convention on Human Rights ("European Convention") during 1949 and 1950s. It came to force in 1953 when eight out of thirteen signatory States ratified the convention.[203]

Today, all 47 members of the Council of Europe are members to the European Convention. They are all subject to binding decisions of the European Court of Human Rights (ECHR) and the Committee of Ministers of the Council of Europe (Committee of Ministers). What is vital for the interest of this study is that the Council of Europe consists of States not members to the European Union, including Russia. And though the ECHR cannot invalidate the laws, as the SCOTUS can, they can make a declaratory judgment that the State is in breach of the

[200] Accepting the fact that United Kingdom is going through process of leaving the European Union, at the time of writing of this study, the nation has not yet passed through this process and remains a member of the European Union.
[201] Convention for the Protection of Human Rights and Fundamental Freedoms article 8, 1950 OJ C 103.
[202] John Hedigan, *The European Convention on Human Rights and Counter-Terrorism,* 28 Fordham Int'l Law Journal 392, at 396 (2005).
[203] Mark W. Janis et al., European Human Rights Law: Text and Materials 3 (1995).

Convention. The Committee of Ministers, in turn, can require contracting States to comply with the decision of the Court and with the language of the convention.

There is relevant case law on the Article 8, that is applicable to the study today. It is *Silver v. United Kingdom*[204] and *Klass v. Germany*. In *Klass*, the court found that the interference with the private and family life is reasonable when: it is in accordance with law,

> "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 freedom of others."[205]

Silver v. United Kingdom clarified what the term "necessary" means:

> "a) Necessary is not synonymous with "indispensable" nor has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" .
>
> b) The contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention.
>
> c) The phrase "necessary in a democratic society" means that, to be compatible with the Convention, the interference must, [*inter alia*], correspond to a "pressing social need" and be "proportionate to the limited aim pursued.
>
> d) Those paragraphs of Articles of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted."[206]

In *James v. United Kingdom*[207], the court created a proportionality test, whereby the proportionality requirement, as seen in the point "d)" above, will be assessed by the Court. The test requires that the law must have a "reasonable relationship of proportionality between the means employed and the aim sought to be [realized]." [208] In effect, this standard is similar to rational basis test, discussed above.[209] But one may argue as to which one of those test gives a stricter scrutiny and liberties protection. Rational basis, *inter alia,* requires that the aim must be legitimate. Whereas, the proportionality test requires no such thing. On the other hand, proportionality test taken together with the standard put in *Silver* create higher liberty protection because the law should "correspond to a pressing social need." Which of them end up giving more protections is a matter of discussion and maybe another separate study.

Right to privacy can also be found in **Article 8 of EU Charter on Fundamental Rights**:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

---

[204] *See Silver v. United Kingdom*, [1981] 3 Eur. H.R. Rep. 475
[205] *See* Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Restructuring the Control Machinery Established Thereby, May 11, 1994, Eur. T.S. No. 155, art. 8(2); Hedigan, *supra note*, at 422
[206] *Silver*, *supra note* 203, at P.97; Hedigan, *supra note,* at 422.
[207] *James v. United Kingdom*, [1986] 8 Eur. H.R. Rep. 123.
[208] *Id*, at P 50;
[209] *See* page 39, footnote 189

> Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[210]

The real power of the EU Charter on Fundamental Rights is under challenge. The Charter itself, when created and ratified, took a non-binding force. Maybe that is the reason indeed why all members and institutions of the European Union are parties to it. What is crucial to the study is that people cannot take their governments to the court for not upholding their obligations under the Charter. Therefore, the Charter has a framework nature and it is up to individual member states to ascend to the standards set by it or not.

These are to keep in mind. Now the study will begin analysis of counter-intelligence practice. The first country will be France.

In Chapter II, a technology was briefly mentioned – IMSI-catchers. To refresh, the study explained that IMSI-catchers are:

> [A] more advanced technology used by law enforcement agencies to intercept in real time "unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier."[211] This technology can potentially send signals through the walls to locate and identify cell phones without service provider assistance or anyone knowing about that.[212]

Analysis in this chapter will start with France. The right to privacy in France is an incredibly complicated issue. Article 9 of the Civil Code, Article 226 of the Criminal Code, Data Protection Act 78-17, Postal and Electronic Communication Code, UN Declaration of Human Rights 1948 (Article 12), European Convention on Human Rights (Article 8) and the Charter of Fundamental Rights of the European Union (Article 7) – these all, in principle, guarantee the right to privacy to French citizens and persons. However, France does not have such stringent rules on warrants like the United States.[213] And, in essence, the law enforcement agencies have broad liberty on search, especially if the matters concern counter-terrorism efforts.[214]

After events at Charlie Hebdo terrorist attack that left 12 people dead, French passed a controversial mass surveillance law.[215] With this law, the law enforcement received a carte blanche to surveil the entire French population, without an effective oversight. Reason why

---

[210] Charter of Fundamental Rights of the European Union article 8, 2000 O.J. C 83/02
[211] Stephanie Pell and Christopher Soghoian, *supra note* 124, at 142
[212] *Id*, at 143
[213] Myria Saarinen & Julie Ladousse, *PRIVACY IN FRANCE: OVERVIEW*, PRACTICAL LAW UK (FEBRUARY 1, 2017), https://uk.practicallaw.thomsonreuters.com/7-573-6346?source=relatedcontent&__lrTS=20170510095814251&transitionType=Default&contextData=%28sc.Default%29&firstPage=true&bhcp=1.
[214] ***See*** Richard S. Frase, *Comparative Criminal Justice as a Guide to American Law Reform: How do the French do it, How can we Find out, and Why Should we Care*, 78 California Law Review 539 (1990).
[215] Angelique Chrisafis, *France passes new surveillance law in wake of Charlie Hebdo attack*, The Guardian (May 5, 2015), https://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack.

effective was added as a qualifier is because National Commission for Control of Intelligence Techniques (CNCTR) was created as an oversight body.[216] However, it does not have a hard power to veto or stop any techniques – it is effectively an advisory board.[217]

This law authorized interception of phone calls and emails without judicial warrant. Additionally, the law sanctions bulk collection of metadata and use of IMSI-catchers.[218] Through the law, intelligence agencies will be able to use keyloggers to track every key stroke on a computer as well as implant microphones and video surveillance cameras into private property premises.

It is safe to say that human rights groups, judges, tech companies and international human rights bodies, such as UN Human Rights Committee, have extensively criticized the new law for its vagueness, lack of oversight or even power to review from any other branch and its discriminatory nature.[219] Nonetheless, as discussed above, one can take France to the ECHR on the basis of failing the proportionality test. It would be unreasonable to assume that such overboard personal data interception with explicit exclusion of any judicial or legislative oversight is proportional or even reasonable in the democratic regime for the narrow aim of war against terror. Nonetheless, it may be argued, that if rational basis test is applied then the French surveillance program might see another day. Compare that to strict scrutiny standard, which would strike down the law.

The other side of la Manche did not fall behind either. On November 2016, a new intelligence law was passed, which authorized mass surveillance and bulk collection of metadata – the Investigatory Powers Act (IPA).[220] The law has great resemblance to the Section 215 and Section 702 of the Patriot Act and FAA respectively. It consists of nine parts plus schedules. The bill distinguishes between targeted and bulk surveillance and collection. Part 2 talks about targeted interception of communication content. It is to be done through a "double lock" oversight mechanism, where the Secretary of State signs off the warrant subject to Judicial

---

[216] Nicolas Boring, *Foreign Intelligence Gathering Laws: France*, Library of Congress (2016), https://www.loc.gov/law/help/intelligence-activities/france.php (last visited Aug 2, 2017).

[217] Kim Willsher, *France approves 'Big Brother' surveillance powers despite UN concern*, The Guardian (July 24, 2015), https://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers; Arik Hesseldahl, *France Has a Powerful and Controversial New Surveillance Law*, Recode (November 14, 2015), https://www.recode.net/2015/11/14/11620670/france-has-a-powerful-and-controversial-new-surveillance-law.

[218] Arik Hesseldahl, *France Has a Powerful and Controversial New Surveillance Law*, Recode (November 14, 2015), https://www.recode.net/2015/11/14/11620670/france-has-a-powerful-and-controversial-new-surveillance-law.; *French parliament approves new surveillance rules*, BBC News (May 6, 2015), http://www.bbc.com/news/world-europe-32587377.; Steve Dent, France gets its own 'Patriot Act' in wake of 'Charlie Hebdo' attack Engadget (July 7, 2015), https://www.engadget.com/2015/07/24/france-surveillance-act/.;

[219] *France: New surveillance law a major blow to human rights* , AMNESTY INTERNATIONAL (JULY 24, 2015), https://www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights/; *France: Parliament must reject law that gives carte blanche to mass surveillance globally*, Amnesty International (September 30, 2015), https://www.amnesty.org/en/press-releases/2015/09/france-must-reject-law-that-gives-carte-blanche-to-mass-surveillance-globally/.

[220] Natasha Lomas, *UK PARLIAMENT RUBBERSTAMPS MASS SURVEILLANCE LAW*, TECHCRUNCH (November 17, 2016), https://techcrunch.com/2016/11/17/uk-parliament-rubberstamps-mass-surveillance-law/.; Joseph Cox, *The UK Just Legalized Mass Surveillance*, Motherboard (November 29, 2016), https://motherboard.vice.com/en_us/article/nz7kvm/mass-surveillance-in-the-uk-is-now-legal.;

Commissioner's approval.[221] However, the bill's language is structured in such a way that it practically makes the Judicial Commissioner to give deference to the Secretary's judgement. Please note, similar to FISC in its deference to the executive. The difference between the two bills in that aspect, more particularly between this bill and Section 702 of the FAA, is that surveillance over American persons, that is citizens, permanent residents and everyone on the territory of the United States, is statutorily prohibited, whilst here it is indiscriminate. Furthermore, even if the Judicial Commissioner refuses to approve the warrant, the intelligence body should stop the surveillance "as soon as possible", rather than immediately.[222] The law also authorizes maintaining databases of personal communications data, as well as interception of data from electronic equipment and the bulk collection of overseas communications. The problem with the latter is that it is also vague as the rest of the bill as is Section 702 of FAA – the exact definition and nature of overseas communication is not defined. Therefore, potentially anyone who would send an email or call abroad can become subject of surveillance without being suspected and involved in terrorism. Also, similar to the FAA and Patriot Act, the telecommunication companies are directed to retain the communication data of their customers for a period of time of 12 months.[223]

The study is discussing only officially recognized government surveillance programs. It must be noted that a large number of those are known only because of the leaks Edward Snowden gave to the world. Besides these there are still those, which are unrecognized. These programs include "Nosey Smurf", "GUMFISH", "Dreamy Smurf", "Tracker Smurf", "Paranoid Smurf" and "Foggybottom". These all are allegedly used by the GCHQ with the cooperation and coordination from the NSA, according to Edward Snowden and the documents he revealed.[224] To illustrate how problematic these programs are, the study will briefly mention what they entail. "Nosey Smurf" is a technology that allows listening to people's conversations through their devices even if they are turned off.[225] "Dreamy Smurf" allows turning on and off a device without user's knowledge.[226] GUMFISH is the technology that scares people into taping over their web-cameras – it allows GCHQ to access any webcam and film or take pictures of things the web-camera sees.[227] Edward Snowden reports that there are cooperation agreements with the leading EU powers and the intelligence agencies in the United States for information and

[221] Lorna Woods, *Draft Investigatory Powers Bill*, 2 European Data Protection Law Review 203 (2016).
[222] Investigatory Powers Bill 26(2)
[223] Natasha Lomas, *supra note 219*;
[224] Jason Murdock, *Edward Snowden: No smartphone is safe from GCHQ spying*, V3 (October 6, 2015), https://www.v3.co.uk/v3-uk/news/2429187/edward-snowden-no-smartphone-is-safe-from-gchq-spying.
[225] Ian Burrell, *Nosey Smurf, Gumfish and Foggybottom: The snooping tools that may have got GCHQ in hot water*, The Independent (May 13, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/nosey-smurf-gumfish-and-foggybottom-the-snooping-tools-that-may-have-got-gchq-in-hot-water-9362642.html.
[226] Jason Murdock, *Edward Snowden: No smartphone is safe from GCHQ spying*, V3 (October 6, 2015), https://www.v3.co.uk/v3-uk/news/2429187/edward-snowden-no-smartphone-is-safe-from-gchq-spying; Sherif Elsayed-Ali, *10 spy programmes with silly codenames used by GCHQ and NSA Amnesty International* (March 18, 2015), https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa/.
[227] Ian Burrell, *supra note 224*;

technology sharing.[228] Therefore, it must be of no surprise that NSA will have access to the information GCHQ will gather, or request GCHQ to obtain desired surveillance, or use the very same technology but claim British hand.

But return back to exclusive British surveillance. Because the United Kingdom is part of European Convention of Human Rights, the right to privacy of British citizens is protected by Article 8 of the said convention. In 2016, European Court of Justice gave a major blow to the IPA, ruling that forceful retention of communications data by telecommunication companies of all their customers is unlawful. Earlier, European Court of Human Rights delivered an opinion over Hungarian mass surveillance program ruling that indiscriminate mass surveillance is in violation of people's right to privacy. Therefore, the only thing that is left from these blows is the targeted surveillance, assuming that the U.K. government will follow the court's interpretation of the Convention and, thereby, uphold its obligations under it.

In the beginning of the chapter, the author presented the two main privacy provisions in the human rights mechanisms of the European Union. The flaws of the presented laws in regards to civil liberties the study is discussing are clear but still they are different in nature. Beginning with the European Convention on Human Rights, the flaw is the national security exception. The problem of such an exception, as discussed in the sections about the American law, is that, in effect, it grants a full discretionary power to law enforcement agencies. *Inter alia*, such an exception permits surveillance in conflict to guaranteed civil rights and liberties, potentially allowing law enforcement crackdown on such freedoms as freedom of speech and association. As it was seen in the American practice and it is seen by plain look over the counter-intelligence laws in France and the U.K. Furthermore, accepting that these laws are a requirement of time in the wake of terrorist attacks by Islamist radicals, it opens up an opportunity for discrimination against religious minorities.

Only proportionality test under *James* may give hope to the plaintiffs in cases against their governments over their mass surveillance programs. Hope is not assured power to win though, for an argument can be made that terrorism is a constantly unknown threat to which any such restrictive measure is proportionate if the end goal this method is sought for is the ultimate safety of the people and the stability of democratic system. And this argument satisfies the *Klass* and, maybe even, the *Silver* standards, as analyzed above.

The second flaw is in the EU Charter on Fundamental Rights, in the second clause of Article 8. The problem is the expression – "some other legitimate basis laid down by law."[229] Counter-intelligence and security interests of a nation are legitimate government interest and the mass surveillance is put in paper as a law. Therefore, it is greatly plausible that in case of a Court hearing, the state can argue that it does not violate the Article for the law sets down the standard for being able to violate the right to privacy – either by consent or for legitimate governmental interest. Therefore, satisfying one will be enough to be within the parameters of the Article. To

[228] ***See*** Julian Borger, *GCHQ and European spy agencies worked together on mass surveillance,* The Guardian (November 1, 2013), https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.
[229] Charter of Fundamental Rights of the European Union article 8, 2000 O.J. C 83/02

resolve the first flaw, the Members of the Union should amend the Article 8, as well as any other article that gives national security exceptions to civil rights and liberties, to define the limits to these exceptions and list prohibited practices. The second flaw's resolve is also in the definition and clarification of what is the legitimate basis, where are its limits, what types of laws can governments not pass.

However, a sum-up is needed. In essence, the practice of the United States in Patriot Act and the FAA is not much different than practice of the intelligence agencies in the European Union, even when the people of the E.U. have statutory protections of their right to privacy. What is surprising and worrying is that even if the United States does not have written right to privacy in the Constitution, it is protected by it because of the Supreme Court. Furthermore, the United States has the Fourth Amendment. But France having the right to privacy does not specify the right to privacy from government surveillance. The United Kingdom was found to have the right to privacy only because of ratification of the EU Human Right mechanisms discussed above. The passage of laws authorizing such mass surveillance is evidence that these rights are not properly protected and these European states are much closer to a verge on becoming official police states. The United States, on the other hand, has working mechanism of checks on the executive. These working mechanisms and standards, though not foolproof as seen by failure of the Supreme Court to start analyzing the counter-intelligence laws, do work and in effect give much higher protection to the people, on its face, than do the mechanisms and standards of the E.U. Recent changes to the practice of the NSA are illustrative enough.[230]

[230] *Statement - NSA Stops Certain Section 702 "Upstream" Activities*, National Security Agency (April 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml; Ellen Nakashima, *NSA halts controversial email collection practice to preserve larger surveillance program*, The Washington Post (April 28, 2017), https://www.washingtonpost.com/world/national-security/nsa-halts-controversial-email-collection-practice-to-preserve-larger-surveillance-program/2017/04/28/e2ddf9a0-2c3f-11e7-be51-b3fc6ff7faee_story.html; Adam Klein, *The End of "About" Collection under Section 702*, Lawfare (May 1, 2017, 10:07 AM), https://www.lawfareblog.com/end-about-collection-under-section-702.

CHAPTER V.

RECOMMENDATIONS FROM FINDINGS

As with any analytical work, it was important for the study to have a comparative element. Such element was presented in the previous chapter, which concluded, *inter alia*, by noting that the United States' judicial protections of civil liberties seem higher than those of their European counterparts. Therefore, now the study will turn to recommendations. These recommendations will be directed primarily to *American* counter-intelligence, counter-terrorism and surveillance practices. This will be done not only because the study itself focuses heavily on American law. But also because these recommendations may well serve as guidelines for improvement to our European colleagues too, due to higher judicial protections of civil liberties American system affords. At least in this area.

When trying to put the ultimate sacrifice of people's right to privacy in balance against the value of prevention of terrorist attacks – the outcome will be different depending on who is putting these two on balance. Unfortunately, looking at the war on terror, or wars in general, in a more skeptical way, one would see that wars are profitable for many actors in the conflict. The terrorist attacks are profitable. They have many benefits including being a counter-balance to growing population, an additional mechanism of control over population and its attitudes, increase in investments in infrastructure of affected places, increase in profits from taxes from military industry, controlled and predicted leaps in market of natural resources. Furthermore, a constant state of danger allows governments to market their anti-democratic laws easier, such as the Investigatory Powers Act and FAA, and potentially giving the government institutions greater oversight of what people say, do or contemplate about. Therefore, in effect it seems hypocritical to say that these counter-terrorism laws have positive effect over prevention of terrorist attacks when it may be deducted that the very existence of such threat is in the interest of some governments.

The case to prove the point can be the journalistic study of *Taliban* by Ahmed Rasheed. There, the author of this book has met with the greatest warlords of the civil war in Afghanistan, including the leaders of Taliban and intelligence officers of Pakistan. The author of this book has vividly illustrated, arguably intentionally, indirect financing of Taliban by the United States and direct financing of Taliban by Pakistan. With Taliban, it has been shown, the supporting states had potential to control the gas transit from Turkmenistan to Pakistan, as well as total control over drug production and traffic from Afghanistan.[231]

[231] ***See*** Ahmed Rashid, *Taliban: Islam, oil and the new great game in Central Asia* (2001); ***also see*** *EU: Orwellian counter-terrorism laws stripping rights under guise of defending them, Amnesty International* (January 17, 2017), https://www.amnesty.org/en/latest/news/2017/01/eu-orwellian-counter-terrorism-laws-stripping-rights-under-guise-of-defending-them/

So, in effect, the study offers recommendations for improvement of the practices. The study argues that taking into account the grave danger that these practices might be detrimental to a democratic society – these practices need to be limited and always targeted, put into a bigger oversight by independent, and checked bodies, and the bulk collection of any personal data should be eliminated. These will be shorter than expected in the start for the length constraints.

a. Section 215

Congress' decision to end bulk metadata collection, under Freedom Act, is consistent with the PCLOB recommendations and Circuit Court's findings. Nonetheless, it is unclear why does PCLOB hail the said Act. Whilst claiming that Section 215 was of basically no use to the intelligence community, it is curious to know why would the American people continue to need it. Admittedly, the intelligence community may need call detail records of certain suspects. To that end and taking into account value of the program to counter-terrorism efforts, the author has several recommendations:

Recommendation 1: Obtain a probable cause warrant under the Fourth Amendment from a district court or the FISC. Upon receipt of the warrant, the executive would have permission to search up to two hops. Furthermore, the warrant should be effective long enough for the intelligence agency to search for any "identifiers" that are of interest to the investigation. Otherwise, if no identifiers have matched, the agency, after the warrant expires, would have to delete all the hops data. The fruits of the search of the identified target can remain at the disposal of the law enforcement agencies for longer. The length should be identified by experts in technology and criminal investigations.

Explanation: If the value of Section 215 is limited to mostly confirming what suspicions the law enforcement have, then added safeguards will not detrimentally slow down the operations. If adopted, this recommendation may increase number of requests for use of Section 215. This has a positive effect of having the judiciary fully informed of what the executive is doing. Nonetheless, the operations of the intelligence community will not be critically slowed down. Reason for that is expected heightened carefulness of the NSA on requesting the warrant. This, in turn, would still bring additional sought confirmations of ties to terrorism, increase legitimacy of the program and, most importantly, strengthen civil rights protections.

Recommendation 2: If violations of these procedures occur, retraining and substantial fines on analysts, and/or their superiors who gave the orders, could serve as effective punitive mechanism. The agency in which the violations occurred should file a report outlining punitive procedures and steps taken.

Explanation: People have proven to be money driven animals in their great majority. There are numerous works written on corruption, its causes, how to combat and prevent it. One of the first and fundamental steps in any combat against corruption would be the increase in pay

and possible punishments if caught. This would increase the price of corruption and make one less inclined to take a bribe. Now coming back to the recommendation, the reverse is viable too. Everyone needs to feed him/herself and the family (be that 10+ person family, or just a dog waiting home), if you put financial incentive on not breaking the rules (besides obvious termination) it makes anyone more careful and accountable.

Retraining would play psychological role too, because no one likes retraining. Some could even prefer money fine than retraining.

If any of the two recommendations is accepted, the threshold of numbers of violations could be defined by the FISC. Also, compliance mechanisms should be set up in intelligence community, similar to those in private sector. In particular, by implementing, among those, anonymous reporting mechanisms could substantially lower the risk of leaks committed by Snowden or Chelsea Manning. The reports could be then sent to a specially formed "intelligence watchdog agency", or be directly reported to Senate Intelligence Committee. An additional safeguard should be added too – threat that information will go public if Senate Intelligence Committee will be inactive. Another option could be a special website set up by the government where intelligence employees could anonymously raise concerns, with strict prohibition to reveal any specific intelligence information (such as names, locations, technology). These could facilitate open public discourse, leading to favorable (to the people) reaction by Congress and decrease of blind deference of judiciary to the executive in matters concerning national security and civil rights and liberties.

b. Section 702

In regards to Section 702 of FAA, the recommendations remain the same as in the analysis of this Section.

Recommendation 1: Bring back FISA to its original form and require individual determinations based on probable cause for FISA warrant on communication interception by the FISC.

Explanation: As the study discovered, Congress was incredibly careful to delineate the exercise of Section 702. In essence, Section 702 does not violate the Fourth Amendment for it is directed towards non-US persons located abroad. These people cannot and do not have protections of the United States Constitution even if it is the United States agency conducting a search. The Constitution reads, "We the People of the United States," and therefore any provision of the Constitution (be that explicitly written or implied) belongs to the People of the United States. The question arises on who are those people? And it seems that the Court has already answered this question – it is anyone who is a US Citizen, Permanent Resident or a person currently located in the United States.

Any US Person's intercepted communication is "incidental" to the search. However, the problems associated with this were discussed – numerous times the real target of the search

could have been a US person. This could have most likely occurred through reverse targeting, upstream collection and "about" communication. "About" communication interception is cancelled by the NSA so only two are left. Upstream collection is most controversial because of its, arguably, uncontrolled interception of communication. On April 28th, 2017, the NSA informed that it halted the "upstream" collection of data because of some non-compliance issues. Reverse targeting is intentional disobedience to the Constitution and statutory law of Section 702.

The FISC determination of giving the warrant and existence of probable cause is vital to bring the practice within the parameters of the Fourth Amendment. It will also increase legitimacy of the surveillance practices of the NSA if a US person would be connected to a terrorist plot.

Recommendation 2: Elimination of "upstream" collection.

Explanation: It is unlikely NSA would rule out upstream collection from their playbook, thus the Supreme Court is needed. Why Supreme Court? Because up to now only Supreme Court takes into account all aspects, can act independent (and even contrary) to precedents, and now begins to take into account the developing nature of technology and showing willingness (from both isles) to adapt Fourth Amendment to the 21st Century. Circuit Courts on the other side, as the study discovered, are willing to lean on the side of the executive and give deference to the executive in the matters of national security. As it was discovered, the American courts are not the only ones to do so. The executive is probably the best informed and skillful branch of all who can handle the national security. Nonetheless, if the judiciary sacrifices rights and liberties of American people and residents, then they do not faithfully execute the role bestowed upon them – to protect those very rights and liberties from governmental encroachment. Especially they will not execute their roles as checks and balances to each other. If government is competent as it always claims to be, there is no doubt they have manpower and material resources to conduct extensive surveillance that would be both – in conformity with the Fourth Amendment and legitimate. Legitimacy would stir down any possible uproar from leaks like those after Snowden or Manning. Supreme Court is people's best hope.

c. Overall

It has been argued that if Congress would have better oversight over the practices of the intelligence community, some problems would be solved.[232] However, as it is seen through experience of the UK and France, Congress might not be the protector and best representor of the people's interest in such matters. Therefore, the following recommendation is prudent.

[232] ***See*** Stephanie Pell and Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 Yale Journal of Law and Technology 134, at 138 (2013)

Recommendation 1: Create an independent oversight board consistent from representatives chosen by judiciary, legislature and executive. The legislature should be represented by representatives from the House of Representatives. The reports they produce should be made public.

Explanation: An oversight board is satisfaction of the mechanisms set down in the Constitution and explained by Framers in the Federalist Papers regarding checks and balances. An independent oversight board is an additional level of security and legitimacy for the programs. The importance of choosing a representative(s) from House of Representatives is in their short terms. As explained in the Federalist 52 and 53, the shortness will make sure they always and only represent the interests of their constituents. So, if anything goes wrong and this board did not report that – the wrath of the people would fall on Congress too (and not only the executive). The publicity of their reports would limit the ability of thorough reporting. However, an oversight of what takes place will nonetheless be useful to the people.

Recommendation 2: Guarantee that every current and future surveillance program's operations would be going through approval of judiciary. So, if FISC warrants are needed – the satisfaction of standards and creation of standards should be judiciary's prerogative.

Explanation: the judicial standards are always a prerogative of the judiciary itself, the intelligence matters should be of no exception. The satisfaction of the standards is also the prerogative of the judiciary and the national security shall be no different.

Recommendation 3: An independent office of civil rights and liberties defender should be created. This office would consist of a lawyer, with a great expertise in civil rights and liberties protections, and a technologist, who will be an expert in Information Technology, including surveillance technologies and techniques. This office will analyze each request of the executive for the FISC warrant or do that after the granting of the warrant to file complaints to the FISCR.

Explanation: Because the intelligence is secretive, there was no counter-balance to the government as it is in usual criminal law by the defendants' lawyers. This office would create such counter-balance.

CONCLUSION

Today, the study looked at an extensive overview of Section 215 of USA PATRIOT Act and Section 702 of FISA Amendments Act, while also giving an insight into practices of British and French governments. Taken together, these were then compared and recommendations were given.

Looking over the precedents allowed the reader to understand where the Court stands right now in regards to the Fourth Amendment. Taking that into account and tracing each, Section 215 and Section 702, study found fundamental constitutional problems they pose. However, each one poses a different problem. Section 215 presents little value to the cause of fight against terror, or finding new terrorists, or stopping coming attacks. After the analysis, it was reasoned that because of *Riley*, it is very possible that the Court could find that metadata that government could freely request should be protected under the Fourth Amendment. USA FREEDOM Act amended Section 215 and brought it in line with stricter constitutional interpretation, ending bulk collection of data and eliminating the record archives.

Nonetheless, USA FREEDOM Act did not do much for Section 702, which, despite ending the "about" communication collection and halting "upstream" collection, still has a great number of controversies that violate the Fourth Amendment. The most obvious is the warrant requirement. FAA changed traditional FISA warrant requirement and got rid of probable cause determination on each target. This is on top of the reverse targeting and more than clear probability that "upstream" collection will be renewed.

Looking at European law, the study did not find as many differences as intended. EU Member States are passing harsher counter-terrorism laws that violate citizens' right to privacy, which, in contrast to the US, is codified. In fact, it was shown that France and the UK have publicly known and recognized programs that are much worse (liberty-wise) than practices under Section 215 and 702.

In total there were seven recommendations, two per each Section analyzed and three additional ones on overall intelligence practices. Preservation of traditional warrant requirements in the counter-intelligence and national security practices were advised. With Section 215, because it did not show much value for counter-terrorism efforts, the inevitable slowdown of process should not be of great damage. With Section 702 it is obvious, especially after *Riley* court, that communications and data people have on their phones are protected under the Fourth Amendment. Furthermore, strict textual read of the Fourth Amendment dictates to obtain a warrant when search is conducted. Because NSA surveillance does not meet the exceptions, *Riley* commands that interception of communication between US person requires a warrant.

This issue was incredibly complex and intriguing. If more time, resources and space were available, practices of EU Member States would be studied more extensively and recommendations would be given in their regard. For now, general recommendations put in place for the US are as advisable for the EU Member States. Another interesting topic would be the right to privacy under the Fourteenth Amendment and how it applies to Section 702 or even

Big Data, by balancing business interests with reasonable expectations of privacy of the society in the internet.

Bibliography

Primary Sources:

US Supreme Court Cases

1. *Amos v. United States*, 255 U.S. 313 (1921)
2. *Barron v. Baltimore*, 32 U.S. 243 (1833)
3. *Bernal v. Fainter*, 467 U.S. 216, 219 (1984)
4. *Boyd v. United States*, 116 U.S. 616 (1886).
5. *Brown v. Board of Education*, 347 U.S. 483 (1954)
6. *Eisenstadt, Sheriff v. Baird*, 405 U.S. 438 (1972)
7. *Ex Parte Jackson*, 96 U.S. 727 (1878).
8. *Gouled v. United States*, 255 U.S. 298 (1921)
9. *Griswold v. Connecticut*, 381 U.S. 479 (1965)
10. *Johnson v. United States*, 333 U.S. 10 (1948)
11. *Katz v. United States*, 289. U.S. 347(1967).
12. *Korematsu v. United States*, 323 U.S. 214 (1944)
13. *Kyllo v. United States*, 533 U.S. 27 (2001)
14. *Lewis v. United States*, 385 U.S. 206 (1966)
15. *Lyng v. Int'l Union*, 485 U.S. 360, (1988)
16. *Mapp v. Ohio*, 387 U.S. 643 (1961).
17. *Olmstead v. United States*, 277 U.S. 438 (1928)
18. *Ontario v. Quon*, 560 U.S. 746 (2010).
19. *Riley v. California*, 134 S.Ct. 2473.
20. *Rios v. United States*, 364 U.S. 253 (1960).
21. *Roe v. Wade*, 410 U.S. 113 (1973)
22. *Silverman v. United States*, 365 U.S. 505 (1961)
23. *Smith v. Maryland*, 442 U.S. 735 (1979).
24. *United States v. Chadwick*, 433 U.S. 1 (1977)
25. *United States v. Jones*, 132 S.Ct. 945 (2012).
26. *United States v. New York Tel. Co*., 434 U.S. 159, 166 (1977)
27. *Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294 (1967)
28. *Weeks v. United States*, 232 U.S. 383 (1914)
29. *Wyoming v. Houghton*, 526 U.S. 295 (1999)

English Law

1. *Entick v. Carrington and Three Other King's Messengers*, [1765] EWHC KB J98, (1765) 19 Howell's State Trials 1029; 95 ER 807.

Appellate Court Cases

1. *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013)
2. *Al-Haramain Islamic Foundation v. Bush*, 451 F. Supp. 2d 1215 (D. Or. 2007).
3. *Hepting v. AT&T*, 508 F.3d 898 (9th Cir. 2006).
4. *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2015).
5. *Klayman v. Obama*, 142 F. Supp. 3d 172 (D.C. Cir. 2015)
6. *U.S. v. Mohamed Mohamud*, 666 Fed. Appx. 591 (9th Cir. 2016)

District Court Cases

1. 2011 U.S. Dist. LEXIS 157706, 2011 WL 10945618
2. *United States v. Jamshid Muhtorov et al.*, No. 12-cr-00033-JLK (2015)
3. *United States v. Mohamud*, 843 F. 3d 438 (2016)

European Court of Human Rights Cases

1. *James v. United Kingdom*, [1986] 8 Eur. H.R. Rep. 123.
2. *Silver v. United Kingdom*, [1981] 3 Eur. H.R. Rep. 475

FISC Court Orders

1. *In re Production of Tangible Things*, No. BR 08-13 (FISA Ct. Mar. 2, 2009)

Declassified Documents

1. Kevin J. O'Connor, *Letter to FISC Judge Walton*, U.S. Department of Justice National Security Division (March 18, 2014), https://www.dni.gov/files/documents/0928/Letter%20to%20Judge%20Walton%2018%20March%202014.pdf
2. Kevin J. O'Connor, *Letter to FISC Judge Hogan*, U.S. Department of Justice National Security Division (March 18, 2014), https://www.dni.gov/files/documents/0928/Letter%20to%20Judge%20Walton%2018%20March%202014.pdf

Secondary Sources:

Books

1. Clan Murphy, 31 EU Counter-Terrorism Law: Pre-Emption and the Rule of Law (2012)

2. Niccoló Machiavelli, The Prince (1532)
3. Thomas Hobbes, Leviathan (Penguin 1985) (1651)
4. Ahmed Rashid, Taliban: Islam, oil and the new great game in Central Asia (2001)
5. Jennifer H. Meadows & August E. Grant, Communication Technology Update (2012)
6. Herbert N. Casson, History of the Telephone (1910)
7. Claude S. Fisher, America Calling: Social History of the Telephone to 1940 (1992)

Other web-sources:

1. Charm Offensive — Switzerland's 'Polite War' of 1847, Military History Now (January 18, 2013), http://militaryhistorynow.com/2013/01/18/charm-offensive-switzerlands-polite-war-of-1847/
2. The History, Old Telephones, http://oldtelephones.com/the-history/ (last visited Apr 18, 2017);
3. Talking Wires: The Development of the Telephone, Talking Wires: The Development of the Telephone, http://www.moah.org/talkingwires/talkingwires.html?KeepThis=true (last visited Jul 18, 2017).

Reports

1. Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT ACT (Aug. 9, 2013), https://www.eff.org/document/administration-white-paper-section-215-patriot-act
2. David Medine et al., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy and Civil Liberties Oversight Board (2014).
3. David Medine et al., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, Privacy and Civil Liberties Oversight Board (2014).
4. *The FISA Amendments Act: Q&A*, Office of Director of National Intelligence (April 18, 2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf

Scholarly Articles

1. Akhil R. Amar, *Fourth Amendment First Principles*, 107 Harvard Law Review 757, 757-819 (1994).
2. Andrew Campbell, *'Taqiyya': How Islamic Extremist deceive the West,* National Observer 11 (Winter 2005).
3. Antkowiak Christian, *Parolee's Reduced Expectation of Privacy May Justify Suspicionless Search: Samson v. California*, 45 Duq. L. Rev. 311 (2007).
4. Chad Squitieri, *CONFRONTING BIG DATA: APPLYING THE CONFRONTATION CLAUSE TO GOVERNMENT DATA COLLECTION*, 101 Virginia Law Review 2011 (2015).

5. Charles J. Dunlap, Jr., *The Law and the Human Target in Information Warfare: Cautions and Opportunities,* Cyberwar 3.0: Human Factors in Information Operations and Future Conflict 137.
6. Coleen M. Ernst, *LOOKING BACK TO LOOK FORWARD: REEXAMINING THE APPLICATION OF THE THIRD-PARTY DOCTRINE TO CONVEYED PAPERS*, 37 Harv. J.L. & Pub. Pol'y 329 (2014)
7. David Gray, Danielle Keats Citron & Liz Clark Rinehart, *FIGHTING CYBERCRIME AFTER UNITED STATES V. JONES*, 103 Journal of Criminal Law and Criminology 745 (2013).
8. Devon Ombres, *NSA DOMESTIC SURVEILLANCE FROM THE PATRIOT ACT TO THE FREEDOM ACT: THE UNDERLYING HISTORY, CONSTITUTIONAL BASIS, AND THE EFFORTS AT REFORM*, 39 Seton Hall Legislative Journal 27 (2015).
9. Jeffrey L. Vagle, *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 Indiana Law Journal 101 (2015).
10. John Hedigan, *The European Convention on Human Rights and Counter-Terrorism*, 28 Fordham Int'l Law Journal 392 (2005).
11. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harvard Journal of Law and Public Policy 757 (2014).
12. Liz C. Rinehart, *CLAPPER V. AMNESTY INTERNATIONAL USA: ALLOWING THE FISA AMENDMENTS ACT OF 2008 TO TURN "INCIDENTALLY" INTO "CERTAINLY,* 73 Maryland Law Review 1018 (2014).
13. Monu Bedi, *THE CURIOUS CASE OF CELL PHONE LOCATION DATA: FOURTH AMENDMENT DOCTRINE MASH-UP*, 110 Northwestern University Law Review 507 (2016).
14. Orin S. Kerr, *THE MOSAIC THEORY OF THE FOURTH AMENDMENT*, 111 Michigan Law Review 311 (2012).
15. Patrick Walsh, *Stepping On (or Over) the Constitution's Line: Evaluating FISA Section 702 in a World of Hanging "Reasonableness" under the Fourth Amendment*, 18 NYU Journal of Legislation and Public Policy 741 (2015).
16. Richard H. Seamon, *Kyllo v. United States and the partial ascendance of Justice Scalia's Fourth Amendment*, 79 Wash. U. L. Q. 1013 (2001).
17. Richard K. Ashley, *Political Realism and Human Interests*, 25 International Studies Quarterly 204 (Jun. 1981).
18. Richard S. Frase, *Comparative Criminal Justice as a Guide to American Law Reform: How do the French do it, How can we Find out, and Why Should we Care*, 78 California Law Review 539 (1990).
19. Samuel D. Warren & Louis D. Brandeis, *THE RIGHT TO PRIVACY*, 4 Harvard Law Review 193 (1890).
20. Stephanie C. Blum, *"USE IT AND LOSE IT": AN EXPLORATION OF UNUSED COUNTERTERRORISM LAWS AND IMPLICATIONS FOR FUTURE COUNTERTERRORISM POLICIES*, 16 Lewis and Clark Law Review 677 (2012).
21. Stephanie Pell and Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 Yale Journal of Law and Technology 134 (2013).
22. Steven G. Stransky, *The Fourth Amendment and Bulk Telephone Metadata: An Overview of Recent Case Law*, 35 Saint Louis University Public Law Review 3 (2015).

News Articles

1. *10 spy programmes with silly codenames used by GCHQ and NSA Amnesty International* (March 18, 2015), https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa/.
2. *53 - Relations with the US on intelligence cooperation and counter-terrorism*, EUROPEAN COUNCIL ON FOREIGN RELATIONS, http://www.ecfr.eu/scorecard/2016/usa/53 (last visited June 3, 2017).
3. Adam Klein, *The End of "About" Collection under Section 702*, Lawfare (May 1, 2017, 10:07 AM), https://www.lawfareblog.com/end-about-collection-under-section-702.
4. Angelique Chrisafis, *France passes new surveillance law in wake of Charlie Hebdo attack*, The Guardian (May 5, 2015), https://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack.
5. Arik Hesseldahl, *France Has a Powerful and Controversial New Surveillance Law*, Recode (November 14, 2015), https://www.recode.net/2015/11/14/11620670/france-has-a-powerful-and-controversial-new-surveillance-law.;
6. Asaf Lubin, *A NEW ERA OF MASS SURVEILLANCE IS EMERGING ACROSS EUROPE*, JUST SECURITY (2017), https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/
7. Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, The Washington Post (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.
8. David Meyer, HUMAN RIGHTS GROUPS TAKE U.K. SURVEILLANCE CHALLENGE TO HIGHEST COURT HUMAN RIGHTS GROUPS TAKE U.K. SURVEILLANCE CHALLENGE TO TOP EURO COURT | FORTUNE.COM (September 30, 2016), http://fortune.com/2016/09/30/surveillance-human-rights-europe/
9. Dustin Volz, *Trumps Russian imbroglio prompts Republican rethink on surveillance law*, Reuters (March 21, 2017, 3:52 AM), http://www.reuters.com/article/us-usa-trump-russia-surveillance-idUSKBN16R2O1.
10. Ellen Nakashima, *NSA halts controversial email collection practice to preserve larger surveillance program*, The Washington Post (April 28, 2017), https://www.washingtonpost.com/world/national-security/nsa-halts-controversial-email-collection-practice-to-preserve-larger-surveillance-program/2017/04/28/e2ddf9a0-2c3f-11e7-be51-b3fc6ff7faee_story.html;
11. Emma Woollacott, *UK MASS SURVEILLANCE RULED ILLEGAL BY EU COURT*, FORBES (December 26, 2016), https://www.forbes.com/sites/emmawoollacott/2016/12/21/uk-mass-surveillance-ruled-illegal-by-eu-court/#17411aec4c42
12. *EU: Orwellian counter-terrorism laws stripping rights under guise of defending them, Amnesty International* (January 17, 2017), https://www.amnesty.org/en/latest/news/2017/01/eu-orwellian-counter-terrorism-laws-stripping-rights-under-guise-of-defending-them/

13. *France: New surveillance law a major blow to human rights* , AMNESTY INTERNATIONAL (JULY 24, 2015), https://www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights/;
14. *France: Parliament must reject law that gives carte blanche to mass surveillance globally*, Amnesty International (September 30, 2015), https://www.amnesty.org/en/press-releases/2015/09/france-must-reject-law-that-gives-carte-blanche-to-mass-surveillance-globally/.
15. *French parliament approves new surveillance rules*, BBC News (May 6, 2015), http://www.bbc.com/news/world-europe-32587377.;
16. *French parliament approves new surveillance rules*, BBC News (May 6, 2015), http://www.bbc.com/news/world-europe-32587377
17. *French surveillance bill draws criticism from web firms and civil liberty groups*, THE GUARDIAN (April 13, 2015), https://www.theguardian.com/world/2015/apr/13/french-surveillance-civil-liberty-criticisms
18. Guy Chazan, German court strikes down terrorism law expanding police powers Financial Times, https://www.ft.com/content/34b79052-06fc-11e6-96e5-f85cb08b0730 (last visited May 19, 2017).
19. Helen Jung, MOHAMED MOHAMUD SENTENCED TO 30 YEARS IN PRISON FOR TREE-LIGHTING BOMB PLOT OREGONLIVE.COM (2014), http://www.oregonlive.com/portland/index.ssf/2014/10/mohamed_mohamud_sentenced_for.html (last visited May 22, 2017).
20. Ian Burrell, *Nosey Smurf, Gumfish and Foggybottom: The snooping tools that may have got GCHQ in hot water*, The Independent (May 13, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/nosey-smurf-gumfish-and-foggybottom-the-snooping-tools-that-may-have-got-gchq-in-hot-water-9362642.html.
21. James Ball, EDWARD SNOWDEN NSA FILES: SECRET SURVEILLANCE AND OUR REVELATIONS SO FAR THE GUARDIAN (2013), https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations (last visited May 22, 2017).
22. Jason Murdock, *Edward Snowden: No smartphone is safe from GCHQ spying*, V3 (October 6, 2015), https://www.v3.co.uk/v3-uk/news/2429187/edward-snowden-no-smartphone-is-safe-from-gchq-spying.
23. Joseph Cox, *The UK Just Legalized Mass Surveillance*, Motherboard (November 29, 2016), https://motherboard.vice.com/en_us/article/nz7kvm/mass-surveillance-in-the-uk-is-now-legal.;
24. Josh Magness, FISA SECTION 702: IS WARRANTLESS SURVEILLANCE NATIONAL SECURITY OR A HIT TO PRIVACY? MCCLATCHYDC, http://www.mcclatchydc.com/news/politics-government/congress/article135841918.html (last visited May 22, 2017).
25. Julian Borger, *GCHQ and European spy agencies worked together on mass surveillance*, The Guardian (November 1, 2013), https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden
26. Kim Willsher, *France approves 'Big Brother' surveillance powers despite UN concern*, The Guardian (July 24, 2015), https://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers; Arik Hesseldahl, *France Has a Powerful and Controversial New Surveillance Law*, Recode (November 14, 2015),

https://www.recode.net/2015/11/14/11620670/france-has-a-powerful-and-controversial-new-surveillance-law.
27. Kim Zetter, *How to Keep the NSA From Spying Through Your Webcam*, Wired (March 13, 2014), https://www.wired.com/2014/03/webcams-mics/
28. Laura K. Donohue, *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law*, Council on Foreign Relations (June 26, 2017), https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law;
29. Lucian Constantin, *NSA reportedly compromised more than 50,000 networks worldwide*, Computerworld (November 25, 2013), http://www.computerworld.com/article/2486266/data-security/nsa-reportedly-compromised-more-than-50-000-networks-worldwide.html
30. Lucian Constantin, *NSAs plans reportedly involve infecting millions of computers with surveillance malware*, PCWorld (March 12, 2014), http://www.pcworld.com/article/2107680/nsas-plans-reportedly-involve-infecting-millions-of-computers-with-surveillance-malware.html
31. Luke Harding, *Mass surveillance is fundamental threat to human rights, says European report*, The Guardian (Monday 26, 2015), https://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe.
32. Myria Saarinen & Julie Ladousse, *Privacy in France: overview*, Practical Law UK (February 1, 2017), https://uk.practicallaw.thomsonreuters.com/7-573-6346?source=relatedcontent&__lrTS=20170510095814251&transitionType=Default&contextData=%28sc.Default%29&firstPage=true&bhcp=1.
33. Natasha Lomas, *UK parliament rubberstamps mass surveillance law*, Techcrunch (November 17, 2016), https://techcrunch.com/2016/11/17/uk-parliament-rubberstamps-mass-surveillance-law/.;
34. Nick Hopkins, From Turing to Snowden: how US-UK pact forged modern surveillance The Guardian (2013), https://www.theguardian.com/world/2013/dec/02/turing-snowden-transatlantic-pact-modern-surveillance (last visited May 22, 2017).
35. Nicolas Boring, *Foreign Intelligence Gathering Laws: France*, Library of Congress (2016), https://www.loc.gov/law/help/intelligence-activities/france.php (last visited Aug 2, 2017).
36. Orin Kerr, *The Problem With the Administration "White Paper" on the Telephony Metadata Program*, VOLOKH CONSPIRACY (Aug. 12, 2013, 2:34 PM), http://www.volokh.com/2013/08/12/problem-withthe-administration-white-paper-on-the-telephony-metadata-program
37. Owen Bowcott, *EU's highest court delivers blow to UK snooper's charter*, The Guardian (2016), https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter
38. Owen Bowcott, *European court to consider legality of UK surveillance laws*, The Guardian (2016), https://www.theguardian.com/world/2016/apr/11/european-court-to-consider-legality-of-uk-surveillance-laws
39. Owen Bowcott, Mass surveillance exposed by Snowden 'not justified by fight against terrorism' The Guardian (2014),

https://www.theguardian.com/world/2014/dec/08/mass-surveillance-exposed-edward-snowden-not-justified-by-fight-against-terrorism (last visited May 22, 2017).
40. *Parliament adopts the intelligence bill*, GOUVERNEMENT.FR (June 30, 2015), http://www.gouvernement.fr/en/parliament-adopts-the-intelligence-bill
41. Ray Sanchez, MAN SENTENCED 30 YEARS FOR OREGON CHRISTMAS BOMB PLOT - CNN.COM CNN (2014), http://edition.cnn.com/2014/10/01/justice/oregon-terror-sentencing/ (last visited May 22, 2017).
42. Sean D. Carberry, *NSA HALTS SECTION 702 'UPSTREAM' COLLECTION*, FCW (April 28, 2017), https://fcw.com/articles/2017/04/28/702-upstream-nsa-carberry.aspx
43. Spencer Ackerman & James Ball, NSA LOOPHOLE ALLOWS WARRANTLESS SEARCH FOR US CITIZENS EMAILS AND PHONE CALLS THE GUARDIAN (2013), https://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (last visited May 22, 2017).
44. Spied on for Being Muslim? NSA Targets Named in Snowden Leaks Respond to U.S. Gov't Surveillance, Democracy Now!, https://www.democracynow.org/2014/7/10/spied_on_for_being_muslim_nsa (last visited May 19, 2017).
45. Spied on for Being Muslim? NSA Targets Named in Snowden Leaks Respond to U.S. Gov't Surveillance, Democracy Now!, https://www.democracynow.org/2014/7/10/spied_on_for_being_muslim_nsa (last visited May 19, 2017).
46. *Statement - NSA Stops Certain Section 702 "Upstream" Activities*, National Security Agency (April 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml;
47. Steve Dent, France gets its own 'Patriot Act' in wake of 'Charlie Hebdo' attack Engadget (July 7, 2015), https://www.engadget.com/2015/07/24/france-surveillance-act/.;
48. Steve Dent, *FRANCE GETS ITS OWN 'PATRIOT ACT' IN WAKE OF 'CHARLIE HEBDO' ATTACK*, ENGADGET (July 24, 2015), https://www.engadget.com/2015/07/24/france-surveillance-act/
49. Uzbekistan: Jamshid Mukhtorov arrested in the USA and a former police officer from Uzbekistan used to be friends, Fergananews.Com, http://enews.fergananews.com/articles/2744 (last visited May 22, 2017).