UNIVERZITA KARLOVA V PRAZE

FAKULTA SOCIÁLNÍCH VĚD

Institut mezinárodních studií

Tereza Krauzová

Land of freedom or land of surveillance? Right to privacy in the U.S. after 9/11

Diplomová práce

Praha 2015

Autor práce: **Tereza Krauzová**

Vedoucí práce: **PhDr. et Mgr. Kryštof Kozák, Ph.D.**

Rok obhajoby: **2015**

Bibliografický záznam

KRAUZOVÁ, Tereza. *Land of freedom or land of surveillance? Right to privacy in the U.S. after 9/11*. Praha, 2015. 55 s. Diplomová práce (Mgr.) Univerzita Karlova, Fakulta sociálních věd, Institut mezinárodních studií. Vedoucí práce PhDr. et Mgr. Kryštof Kozák, Ph.D.

Abstrakt

Spojené státy americké byly vždy vnímány jako země svobody. Ústava Spojených států se těší ve své zemi velké úctě a stala se modelem pro další ústavy světa. Teroristické útoky 11. září 2001 přinesly nejen zvrat v americké zahraniční politice v rámci války proti terorismu, ale ovlivnily i domácí politický vývoj a zapříčinily vytvoření komplexní bezpečnostní legislativy. Tato protiteroristická opatření se ale stala terčem kritiky, protože mnohé programy vycházející zejména ze zákona Patriot Act se zdají být ústavně kontroverzní, ne-li přímo s rozporu občanskými právy, zejména právem na soukromí. V roce 2013 odhalil Edward Snowden tajné odposlouchávací programy Národní bezpečnostní agentury. Tato práce zkoumá zjevné rozpory mezi proklamovanou americkou svobodou a realitou, v níž se USA řadí mezi země s nejvyšší mírou sledování svých občanů.

Klíčová slova: USA, Patriot Act, Snowden, NSA, sledování, protiteroristická legislativa

Abstract

The United States of America has been always perceived as a land of freedom. The U.S. citizens are very proud of their Constitution that became model for other constitutions in the world. The terrorist attacks of September 11, 2001 not only brought a change in the U.S. foreign policy as the war on terror was launched, but also influenced the domestic political development and caused creation of a complex network of security legislative. These antiterrorism measures have been criticized, as the programs arising especially from the Patriot Act are controversial, challenging the civil rights and especially the right to privacy. In 2013, Edward Snowden revealed secret spying programs of the National Security Agency. This thesis examines the discrepancies between the

proclaimed freedom and the reality, in which the United States is ranked among endemic surveillance societies.
Keywords: USA, Patriot Act, Snowden, NSA, surveillance, antiterrorism legislative

Rozsah práce: 99 247 znaků

Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracovala samostatně a použila jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 3. ledna 2015 Tereza Krauzová

Poděkování

Na tomto místě bych ráda poděkovala vedoucímu své diplomové práce PhDr. et Mgr. Kryštofovi Kozákovi Ph.D. za věnovaný čas a cenné rady, které mi poskytl. Zároveň děkuji Normě Hervey Ph.D. za pečlivost a hodnotné připomínky k práci.

TEZE DIPLOMOVÉ PRÁCE

Jméno:
Tereza Krauzová

E-mail:
tereza.krauz@gmail.com

Semestr:
Zimní 2013

Akademický rok:
2013/2014

Název práce:
Země svobody nebo země pod dohledem? Právo na soukromí v USA po 11. září

Předpokládaný termín ukončení (semestr, školní rok):
Zimní 2014

Vedoucí diplomového semináře:
PhDr. Jan Bečka, Ph.D.

Vedoucí práce:
PhDr. et Mgr. Kryštof Kozák, Ph.D.

V čem se oproti původními zadání změnil cíl práce?
Cíl práce se konkretizoval na zmapování protiteroristických opatření, zejména zákonů a programů Národní bezpečnostní agentury. Práce se bude zaměřovat na debatu mezi odborníky, zda je přijatá bezpečnostní legislativa a usutečňované programy v souladu s Ústavou Spojených států, či zda již dochází k porušování základních principů ukotvených v Listině práv a v zájmu maximální národní bezpečnosti se potlačuje právo na soukromí.

Jaké změny nastaly v časovém, teritoriálním a věcném vymezení tématu?
Časové a teritoriální vymezení práce zůstává stejné. Výchozím datem je 11. září 2001, horní časová hranice není pevně stanovena, do diplomové práce budou zapracovány relevantní události na území Spojených států nastalé přibližně do poloviny roku 2014. Věcně se práce posunula více ke zkoumání kontroverzních programů odhalených Edwardem Snowdenem místo rozboru Patriot Actu jako celku.

Jak se proměnila struktura práce (vyjádřete stručným obsahem)?
Oproti projektu se změnilo rozvržení práce na kapitoly. První kapitola bude představovat právní pojem právo na soukromí, jeho vznik a význam v právním řádu USA. Zároveň bude dáno do kontextu legitimní právo státu na zajištění vlastního bezpečí. Tato kapitola rovněž stručně shrne vývoj sledovací legislativy před přijetím klíčového zákona FISA. Těžištěm práce bude druhá kapitola, představující zákon FISA, jenž se stal východiskem pro protiteroristickou legislativu po 11. září, zejména Patriot Act. Dále zde budou představena relevantní ustanovení Patriot Actu, a oba programy Národní bezpečností agentury, které byly odhaleny v roce 2013 Edwardem Snowdenem. Třetí kapitola bude zkoumat otázku, jak jsou získané informace využívány a zda se vychýlení rovnováhy od důrazu na občanské svobody směrem k národní bezpečnosti trvá, nebo zda se kurz obrací.

Jakým vývojem prošla metodologická koncepce práce?
Z metodologického hlediska se pro mou práci nejlépe hodí analýza právních názorů expertů a mediální debaty.

Které nové prameny a sekundární literatura byly zpracovány a jak tato skutečnost

ovlivnila celek práce?

Brandeis, Louis D. and Warren, Samuel D. "The Right to Privacy." Harward Law Review, Vol. IV, No. 5 (December 1890).

Bungard, Jessica M. "The Fine Line between Security and Liberty: The "Secret" Court Struggle to Determine the Path of Foreign Intelligence Surveillance in the Wake of September 11th." University of Pittsburgh School of Law Journal of Technology Law and Policy Volume IV, Article 6 (Spring 2004).

Copeland, Rebecca A. "War on terrorism or war on constitutional right? Blurring the lines of intelligence gathering in post-September 11 America." Texas Tech Law Review Vol. 35, No. 1 (2004).

Glick, Scott J. "FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security." Harvard National Security Journal, Volume 1, (May 30, 2010).

Greenwald, Glen. "NSA collecting phone record of milions of Verizon customers daily," The Guardian, June 6, 2013.

Liu, Edward C. "Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments." Congressional Research Service Report for Congress, Library of Congress, April 1, 2014.

"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," July 2, 2014. Privacy and Civil Liberties Oversight Board.

"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," January 23, 2014. Privacy and Civil Liberties Oversight Board.

Zprávy publikované Radou pro dohled nad soukromím a občanskými svobodami rozšířily prostor, který bude v práci věnovaný analýze programů Národní bezpečnostní agentury odhalených Snowdenem.

Charakterizujte základní proměny práce v době od zadání projektu do odevzdání tezí a pokuste se vyhodnotit, jaký pokrok na práci jste během semestru zaznamenali (v bodech):
Základní posun spočívá v prostudování části potřebných zdrojů, které změnily těžiště práce. Nejvýznamnější část je ta věnovaná zkoumání sledovacích programů NSA, které vyvolávají značné kontroverze.

Podpis studenta a datum:
27. ledna 2014

Schváleno:	**Datum**	**Podpis**
Vedoucí práce	**28. ledna 2014**	
Vedoucí diplomového semináře	**28. ledna 2014**	

Table of Contents

Introduction

The United States has always been perceived as a land of freedom. Millions of people left their home countries and headed to America in pursuit of a new life. The freedom rhetoric can be easily tracked in speeches delivered by the U.S. presidents. George W. Bush mentioned in his second inaugural address the words "free," "freedom" and "liberty" forty-nine times in total.[1] Similarly, the U.S. national anthem contains the "land of free" wording.

The U.S. Constitution, valid for more 200 years, has become model for other constitutions in the world, as it introduces a system of government built on recognition of personal rights, rule of law, system of checks and balances limiting the power of leaders and anchoring judicial review of their decisions. The belief that the government is created to protect these values and the inalienable human rights creates an ideal that can be called an American creed.[2] U.S. citizens are very proud of their long democratic tradition. "The Declaration, the Constitution and the Bill of Rights (...) represent what is best about America. They are symbols of the liberty that allows us to achieve success and of the equality that ensures that we are all equal in the eyes of law."[3]

On September 11, when the terrorist attacks shocked the United States and the whole world, President George W. Bush assured his people: "Terrorist acts can shake the foundation of our biggest buildings, but they cannot touch the foundation of America."[4] That foundation, as explained by President Obama, is three documents – the Declaration, the Constitution and the Bill of Rights – anchoring "the foundation of liberty and justice in this country, and a light that shines for all who seek freedom, fairness, equality and dignity around the world."[5]

---

[1] William Safire, "Bush's Freedom Speech," *The New York Times,* January 21, 2005 http://www.nytimes.com/2005/01/21/opinion/21safire.html?_r=0 [downloaded on December 13, 2014].
[2] Jeffrey Rosen and David Rubenstein, "Constituing Liberty: from the Declaration to the Bill of Rights," *National Constitution Center,* Exhibition Pamphlet, http://constitutioncenter.org/media/files/13_Exhibition_Pamphlet.pdf [downloaded on December 14, 2014].
[3] Ibidem.
[4] Citation from the George W. Bush's address on September 11, 2001, *CNN,* September 11, 2001 http://edition.cnn.com/2001/US/09/11/bush.speech.text/ [downloaded on December 13, 2014].
[5] „Remarks by the President on National Security," *The White House,* May 21, 2009 http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09 [downloaded on December 13, 2014].

The war on terror declared by President Bush after the 9/11 is waged not only outside the U.S. borders. In addition to shifts in foreign policy, many changes have occurred and new security provisions have been adopted to apply on American soil. Civil rights organizations, academic experts and recently also authors of some of the provisions have been voicing concerns that the new pieces of antiterrorism legislation and intelligence provisions ceased to observe constitutional protection. In addition, in June 2013, Edward Snowden, a former employee of the National Security Agency, revealed together with journalist Glenn Greenwald, secret files containing information about secret government surveillance programs affecting all U.S. citizens.

The federal government declares the United States to be the land of freedom stating: "We uphold our most cherished values not only because doing so is right, but because it strengthens our country and it keeps us safe. Time and again, our values have been our best national security asset – in war and peace; in times of ease and in eras of upheaval."[6] In contrast to this, Privacy International ranked the United States as one of the endemic surveillance societies, alongside Russia or China. According to this London-based international organization, the U.S. performed worst among democratic countries in terms of statutory protections and privacy enforcement. The bad rating is result of the extensive government surveillance programs and information gathering in the name of security.[7]

This thesis examines the contradiction between the proclaimed freedom and the factual complex surveillance mechanisms intruding privacy, whose legality and constitutionality is being questioned. Has the United States shifted from the land of freedom into the land of surveillance?

After 9/11, a vast number of antiterrorism acts, executive orders, presidential directives and intelligence programs in the name of national security have been introduced. This paper focuses on the two major National Security Agency eavesdropping programs, revealed by Edward Snowden. The first of them is the bulk collection of telephony metadata conducted under Section 215 of the USA Patriot Act and the other is PRISM and upstream acquisition of Internet communications pursuant

---

[6] Ibidem.
[7] David Ward, "Britain rated worst in Europe for protecting privacy," *The Guardian,* December 31, 2007 http://www.theguardian.com/politics/2007/dec/31/uk.eu [downloaded on December 14, 2014].

to Section 702 of the Foreign Intelligence Surveillance Act of 1978 modified by the Amendments Act of 2008.

Chapter one of this thesis introduces the theoretical framework of the right to privacy and the state surveillance issue. The right to privacy as a personal right of citizens limits to a certain extent the right of government to have control over society. The right to privacy, its anchor and evolution in the U.S. legal system and an introduction of the surveillance legislation prior to 9/11 open the thesis.

Chapter two elaborates on the legal context of the current surveillance issues with focus on the possible statutory and Constitutional deficits of the NSA data collecting programs revealed by Edward Snowden. To provide a sufficient explanation of both programs, it is essential to introduce the Foreign Intelligence Surveillance Act (FISA) as well. Even though the act does not belong among the legislation passed after 9/11, it is the crucial basis for the antiterrorism legislation, especially for USA Patriot Act, which builds significantly on FISA provisions, as it deepens, modifies and amends them. For purposes of this thesis, only the Sections 215 and 218 of the Title II of the USA Patriot Act will be analyzed. The law itself is 365 pages long and consists of ten Titles, encompassing a wide variety of issues. However, only Title II, "Enhanced surveillance procedures," is thematically connected with this thesis, as it brought new rules for surveillance procedures. Sections 215 and 218 raise high concerns regarding privacy rights.

Chapter three examines the mechanism of proper exploitation of the collected data. In addition, it assesses the question whether the U.S. will remain a country of increased level of surveillance or whether the pendulum will swing back to the land of freedom.

This paper focuses primarily on the disputed surveillance provisions violating the right to privacy. It does not include the Guantánamo prison issue, indefinite detention and imprisonment, although these are important and controversial issues arising directly from the 9/11 legislative measures as well, but they are beyond the scope of this thesis. Similarly, this paper is not involved with any deeper examination of the commercial tracking of one's online activities by private companies for purposes of marketing and targeted advertising.

The first source is the landmark legal article *The Right to Privacy*[8] by Louis Brandeis and Samuel Warren, the earliest crucial text dealing with the topic. Even though the article focuses more on violations of privacy from other individuals than from the government, it captures the legal evolution of the right.

The Privacy and Civil Liberties Oversight Board is an independent, bipartisan agency within the executive branch, established by implementing the 9/11 Commission recommendations. The 9/11 Commission – officially named National Commission on Terrorist Attacks Upon the United States – was created in 2002 to examine circumstances od the 9/11 attacks and draft adequate suggestions how to improve the U.S. political system and avoid repeating similar events. The five member Privacy and Civil Liberties Oversight Board is appointed by the President and confirmed by the Senate. The Board's mission is to balance federal government's efforts to prevent terrorism with the need to protect privacy and civil liberties. For this purpose, the PCLOB analyzes actions of the executive branch and ensures that the liberty concerns are appropriately considered in the development and implementation of antiterrorism law and policies.[9]

The PCLOB work began approximately since the early summer of 2013, which corresponds with the months of Snowden's first revelation. In this respect, the Board issued two comprehensive reports about National Security Agency's programs. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*[10] and *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.*[11] Both reports were issued in the year 2014 and play important role in this thesis, as they introduce not only the government position but thoroughly examine privacy and civil rights concerns. The PCLOB

[8] Louis D. Brandeis, Samuel D. Warren, „The Right to Privacy," *Harvard Law Review* Vol. IV, No. 5 (December 1890): 193-220 http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf [downloaded on December 14, 2014].

[9] Official webpage of the Privacy and Civil Liberties Oversight Board. http://www.pclob.gov/meetings-and-events/2014meetingsevents/23-january-2014-public-meeting.html [downloaded on December 13, 2014].

[10] „Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," *Privacy and Civil Liberties Oversight Board,* July 2, 2014 http://www.pclob.gov/Library/702-Report-2.pdf [downloaded on November 26, 2014].

[11] "Report on the Surveillance 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,* January 23, 2014 http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf [downloaded on November 22, 2014].

recommended shutting down the NSA phone program and retaining the PRISM and upstream collection program. Of special value to this thesis are the separate statements of two Board members – Rachel Brand and Elisabeth Collins Cook – who did not agree with the majority conclusions of the Board. Their opinions are part of the final Report.

The Congressional Research Service (CRS) of the Library of Congress is a nonpartisan think tank working exclusively for the United States Congress providing valuable policy and legal analysis for Congressmen, who use the reports as information source for their policymaking.[12] The reports present facts and introduce the reader to various aspects of the issue. The author and co-author of the CRS reports are Edward C. Liu, legislative attorney and researcher with focus on national security, and Elisabeth B. Bazan, expert on FISA.

Very important for this thesis are books and articles published by Glenn Greenwald, a journalist, constitutional lawyer and columnist on civil liberties and national security issues for the *Guardian*. He focuses in his career on civil and constitutional rights. Edward Snowden selected Greenwald for publishing the reports about NSA surveillance programs. His book called *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*[13] introduces how the cooperation with Snowden emerged, why did they decide to reveal the programs and contains also inspiring thoughts on the privacy and surveillance issues. However, Greenwald's texts are one-sided, condemning the current government policies but not suggesting any alternative.

Daniel J. Solove is a law professor at the George Washington University Law School. He is an internationally known expert in privacy law and author of number of books and textbooks about this topic. Solove's books offer deeper legal and historical understanding of the privacy issue, introducing it in more detailed context. Especially the book *Nothing to Hide. The False Tradeoff between Privacy and Security*[14] is an important source for understanding of the Constitutional background and recent perception of the right to privacy.

---

[12] Official webpage of the Congressional Research Center, *the Library of Congress* http://www.loc.gov/crsinfo/ [downloaded on December 13, 2014].

[13] Glenn Greenwald, *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books. Henry Holt and Company, LLC, 2014).

[14] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, Yale University Press, 2011).

This thesis works also with number of records and analysis published by various activist organizations, for example the American Civil Liberties Union and the Electronic Frontier Foundation. According to some authors, in times of national crises, the three branches of state power tend to support each other. Therefore, not even the Supreme Court works reliably in revising the new laws, and, in most cases, decides in favor of the disputed federal policies.[15] Organizations and think tanks opposing the government policies have been playing the role of substitutive checks and balances, focusing on problems. They can be considered the real living constitution, keeping the proclaimed foundation of America even in an era of upheaval still alive.[16]

[15] David Cole, "Where Liberty Lies: Civil Society and Individual Rights After 9/11," *Georgetown Public Law and Legal Theory Research Paper* No. 12-164, 2012, page 1212 http://scholarship.law.georgetown.edu/facpub/1119/ [downloaded on November 26, 2014].
[16] Ibidem.

Chapter 1: Privacy and surveillance

1.1 What is the right to privacy

The right to privacy developed both in the European and American legal framework as an essential element in the palette of indispensable individual rights related to human dignity. The right to privacy creates a protected legal space for individuals, excluding intrusive acts of government and others.

Rights of privacy developed gradually over centuries as a legal response to growing expectations of people, whose lives were changing and evolving. At the present time, there are three legal foundations of the right to privacy in the United States: common law, constitutional law and federal statues.[17] An important milestone in this process was achieved in the article "The Right to Privacy" by two lawyers, Louis D. Brandeis and Samuel D. Warren, in the *Harvard Law Review* in December 1890. The authors were among the first to use the term "right to privacy" in U.S. legal history. In the text, they are advocating for this right, which was at their time becoming essential, defining it as "a right to be left alone".

Brandeis and Warren declared that the dynamics of social and technological progress required an adequate legal response. Earlier, British common law declared only physical interference with one's life and property to be legally significant – people were protected from battery. Later, as the law evolved, protection from verbal assault as well as concepts of nuisance and defamation became part of the law. Brandeis and Warren argue that while liberty was originally meant freedom from actual restraint, personal immunity was extended beyond the body of the individual.[18] "Gradually the scope of these legal right broadened; and now the right to life has come to mean the right to enjoy life, - the right to be left alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession – intangible, as well as tangible."[19]

The authors experienced the very dynamic era of rapid development of new technologies and increasing influence of media, when privacy began to be threatened

[17] Robert Sprague, "Orwell was an optimist. The evolution of privacy in the United States and its de-evolution for American employees," *The John Marshall Law Review* 83 (2008-2009): p. 93.
[18] Louis D. Brandeis, Samuel D. Warren. "The Right to Privacy." *Harvard Law Review,* Vol. IV, No. 5 (December 1890): pp. 193–194.
[19] Ibidem, 193.

and defamation became a serious issue.[20] The right to privacy, as a new legal term, evolved and gained specific features in the decades after this groundbreaking article.

In the United States, the right to privacy is explicitly mentioned neither in the Constitution, nor in the Bill of Rights. However, according to consistent rulings of the Supreme Court, it is based on these documents and arises especially from the First and Fourth Amendment. Mainly during the 20th century, the constitutional conception of privacy rights in various aspects of people's lives gradually developed. According to the Supreme Court, privacy as constitutional right is stemming from concepts of individualism, limited government, and private property. [21] Consistent legal interpretations state that privacy is implied also in number of the Amendments to the Constitution, besides the First and Fourth from the Third, Fifth and Fourteenth. Several Supreme Court decisions focusing on privacy in various contexts of human life are also significant.

General public connects the right to privacy mostly with cases in the sphere of personal, especially sexual, intimacy. The effort to "keep government out of bedrooms" – a slogan used by activists – became more and more insistent in recent decades. *Griswold v. Connecticut* (1965), *Roe v. Wade* (1973) and, quite recently, *Lawrence v. Texas* (2003) define legal boundaries, which the government is not allowed to cross with respect to interference with sexual behavior. Nevertheless, enlarging the untouchable autonomous sphere of people at the same time limits government powers. This chapter focuses on the clash between privacy of people and the need of government to have some kind of control over society.

1.2 Rights of the government vs. rights of the governed

Political philosophers have always studied the concept of the state, providing explanations as to the purpose of the state, the origins of government authority and justification of those powers. In modern times – leaving aside various anarchistic and radical ideologies – the theory of state generally explains the purpose of existence of states as a social contract of people living in a defined area, who give some of their rights to a government in order to ensure protection of life and property and achieve a

[20] Sprague, "Orwell was an optimist," 98.
[21] Ibidem, 102.

value often called "common good", "good life" or "general interest".[22] These terms include numerous values and qualities people seek for satisfactory living.

To make a step back from the level of values such as privacy, the elemental human need for a good life, essential to this thesis, is physical safety. People naturally look for peaceful environments in which they can live, raise children, go to work and enjoy their free time undisturbed by fear of threats to their lives, health and property. Famous political philosopher Thomas Hobbes explained in his milestone book *Leviathan* that protection of the life of citizens is the vital and essential duty of every government, as the natural environment is very dangerous and would lead to anarchy – a war of all against all. Therefore people, who cannot fully protect themselves, give up some of their freedoms in exchange for services the government should provide. To make this concept functional, every individual committed to a social contract must obey the laws of the state.

In addition to Hobbes, John Locke, another influential political philosopher, further elaborated the theory of the state but coming from different assumptions about human nature. Locke, a representative of the Enlightenment, included in purposes of existence of states apart from obvious protection of lives of citizens also the responsibility to safeguard unalienable human rights – property and liberty. In the state of nature, people are maybe equally free and independent, but some of them endanger peace and safety. For this reason, people created states and authorities to ensure security. However, to make this social contract work, government should also protect people's rights and freedoms.[23] This liberal perception influenced strongly the Founding Fathers of the United States, as Thomas Jefferson expressed in the Declaration of independence – life, liberty and pursuit of happiness are there described as unalienable. These concepts still resonate in the American society.

According to prevalent liberal theory, a government that is expected to be able to provide for common good and security of its inhabitants needs to dispose of necessary power and authority to impose rules and make all subjects of law obey these regulations. Those coercive powers as well as other authority of government are derived from rights of the governed, who chose their leaders in order to lead the society and

[22] Henk E.S. Woldring, „On the purpose of state: Continuity and Change in Political Theories." 1. http://maritain.nd.edu/ama/Sweetman/Sweetman12.pdf [downloaded on November 2, 2014].
[23] Ibidem, 158.

protect it from external as well as domestic threats. Accordingly, the level and extent of rights the citizens are still able to exercise, are thus inevitably being limited. For this reason, there arises the question of where should a balanced line be drawn between the inviolable rights of individuals on the one hand, and powers of governments ensuring security and enforcing adherence to laws on the other. As a consequence, in reality there occurs an inverse relationship between freedom and security: the more freedom individual citizens in their country possess in their hands, the fewer tools remain available for effective actions of the government. There is no simple and evident answer to this question that could be applicable and appropriate everywhere and under all conditions, as it depends – among others – on the culturally political customs of each particular society and the level of threat the society is facing. Thorough human history, people have experienced different approaches to this issue in different places of the world. In addition, it is a political problem, as there are groups within each country which push the state to adapt their version of the border.

Perception where this boundary dividing authorities of the government and the rights of the governed should be placed has differed distinctively under various political ideologies. To illustrate, imagine a comparison where totalitarianism at one end constitutes one extreme, and libertarianism at the other represents the opposite approach.[24] The Encyclopaedia Britannica defines libertarianism as a political philosophy that puts emphasis on individual liberty and personal freedom; those objectives are of the primary political value for the supporters of this view.[25] Libertarianism builds on the heritage of John Locke, Adam Smith and Thomas Jefferson and in the light of natural rights to life, liberty, private property, freedom of speech and association, freedom of worship, equality under law and moral autonomy, thereby favors very limited government by consent, whose activities would be restricted to protection of lives, properties and freedoms of people.[26] The Libertarian Party of the United States proposes to cut taxes to a minimum and thus limit the government agenda

[24] Kenneth Janda, *Výzva demokracie. Sytém vlády v USA* (Praha: Slon, 1998): p. 29.
[25] Encyclopaedia Britannica: Libertarianism. http://www.britannica.com/EBchecked/topic/339321/libertarianism [downloaded on October 27, 2014].
[26] Janda, *Výzva demokracie,* 29.

significantly.[27] Nevertheless, the Libertarian Party plays a marginal role in the political process dominated by the two major parties, Democratic and Republican.

Totalitarian government, on the other hand, subscribes to an opposite approach theoretically permitting even no individual freedom and seeking to subordinate all aspects of the individual's life to the authority of government through coercion and repression.[28] Totalitarian regimes usually develop very complex systems of controlling society and psychology and advanced technical measures of surveillance. Those governments justify their mass repression of society and even control of private lives as necessary if they are to take care of the state.

In reality it is hardly possible to achieve a pure form of either libertarianism or totalitarianism, as these are abstract ideals of extreme forms of political ways of thinking and governing. Even though in history several totalitarian regimes came very close to the absolute Orwellian form of controlling society, most of the undemocratic states in today's world are authoritarian instead. Authoritarian regimes do not use a complex state ideology explaining and justifying every aspect of life. Authoritarian governments target repression only at opposing movements and individuals. Nazi Germany or the Soviet Union under Joseph Stalin are among totalitarian regimes, as the level of control over the society was extremely high; however some of the socialist regimes in the former Soviet block, especially in the last decade or their existence, could be classified rather as authoritarian regimes, since inhabitants who did not challenge the regime were able to achieve quite undisturbed lives.[29]

1.3 Surveillance

As explained above, the vital purpose of national security measures is to create a state, which is undisturbed by potential domestic or external threats, even though these threats can be easily socially constructed, especially if they are potential. In order to provide for these conditions, governments are endowed with various tools and powers. Governments use their military forces to confront open hot conflicts. At the same time,

[27] Official webpage of the Libertarian Party of the United States. *How do Libertarians, Republicans, and Democrats differ?* http://www.lp.org/how-do-libertarians-republicans-and-democrats-differ [downloaded on October 27, 2014].
[28] Encyclopaedia Britannica: Totalitarianism. http://www.britannica.com/EBchecked/topic/600435/totalitarianism [downloaded on October 27, 2014].
[29] Ladislav Cabada and Michal Kubát. *Úvod do studia politické vědy* (Praha: Vydavatelství a nakladatelství Aleš Čeněk, 2007), pp. 369-372.

to support prevention, states use diplomacy and economic influence to create favorable international environments of stability where deployment of military troops will not be necessary. Among external threats belong also non-states actors – various hostile movements and often even terrorist organizations that are difficult to combat.

However, destructive effects also arise from within the state itself. Maintaining domestic social order might be an even trickier challenge requiring more delicate approaches. For this purpose, governments use various forms of monitoring people's behavior – so-called surveillance measures – even though these can be used to counter some forms external threats as well, e.g. foreign spies. In this sense, surveillance is a form of social control, whose task is to recognize and prevent possible threats and then investigate criminal activities. There are many options that can be used at different levels of intruding into personal spheres of people, ranging from violating confidentiality of correspondence to complex networks of secret police and random house searches. In our technically advanced society, means of surveillance are mostly electronic, such as the highly discussed and widely used surveillance cameras at public places, high speed computers able to search through all forms of electronic communication or sophisticated biometrics software which analyzes physical features of a human in a second and connects it with a database of suspect individuals.

It depends on the character of a state and the level of threats it faces when a state decides what means and to what extent to use against domestic dangers. Some countries reject extensive intrusions and decide to fight only against imminent threats such as political extremists who manifest their destructive views openly, and respect private sphere of those citizens, who do not show hints of dangerous attitudes. This approach, however respectful to rights of individuals, cannot reveal all threats in a timely way. Therefore, some countries facing higher levels of danger might decide to favor crime prevention over freedom and liberty. Adopted measures can thus slowly move the balance between freedom and security more towards the totalitarian end of the scale, as people under surveillance would suppress their activities in order to avoid problems.

In times of national crisis, the balance between national security measures and civil liberties of people is disrupted in favor of national security. We can observe this trend throughout the history of the United States, when various more or less serious security threats provoked waves of public hysteria and higher level of government intrusions. Even though Americans believe in the reliability of their system built on

checks and balances, history shows that judiciary in times of crises does not always stop excesses of the executive and legislative infringing on civil liberties.[30]

During World War II, targeted enemies were the Japanese-Americans, who were deprived of their rights and imprisoned in camps. An era of fear of increased communist influence on the American society – the so-called Red Scare – came in two waves: the first after the Russian revolution 1917 and then especially during McCarthyism in the post-World War II era. In these times, people whose loyalty was believed to be questionable or who criticized government actions faced higher level of surveillance, intimidation and detention.[31]

Spreading of communist ideas and potential enlargement of the Soviet block was understood as an existential danger to the United States. In the following decades, United States got involved in the Vietnam War, because it was scared of the domino effect in Southeast Asia. The geopolitics of the Cold War was considered as a zero-sum game. Today, there is still a threat, but it is now in the form of radical Islamist terrorism instead of communism. And similarly to Cold War, the fight is being led in the world as well as on the domestic front. In the war on terror, as in the previous war on communism, much is allowed and acceptable for the government.

The terrorist attacks of 9/11 influenced the security issues in numerous national states, not only the United States. In addition to the U.S., Great Britain, France, Australia and Canada also significantly expanded the scale of antiterrorist surveillance. In all of these countries, new patterns of tracking money transactions have been introduced; retention time of records of telephone and electronic communication has been extended; restrictions on monitoring suspicious individuals have been eased, and multiple new ways of checking a person's identity have been introduced.[32]

Proponents of the surveillance measures often use the nothing to hide argument, an assumption that people who did not anything do wrong do not need to be afraid of the fact that government possesses their personal information. This argument might be viable only under ideal conditions, when the democratic government strictly obeys all rules and acts constitutionally limited by the system of checks and balances. Problems

[30] Nancy Murray and Sarah Wunsch. "Civil Liberties in Times of Crisis: Lessons from History." *Massachusetts Law Review*. http://www.massbar.org/publications/massachusetts-law-review/2002/v87-n2/civil-liberties-in-times-of/ [downloaded on December 15, 2014].
[31] Ibidem.
[32] James B. Rule, *Privacy in peril: How are we sacrificing a Fundamental Right in Exchange for Security and Convenience* (New York: Oxford University Press, 2009), pp 82–83.

arise, however, when this legitimate and favorable system is eroded – either by domestic or foreign factors. In such cases, new rulers how do not bother with obeying laws would have direct access to sensitive information that can and most probably will be misused. This can be illustrated with an example, which happed during German occupation of the Netherlands during the Second World War. At that time, the Nazis discovered census registries of the Dutch government, which included data on people's religious preferences. These could have served for a beneficial purpose; however, the Nazis used them to identify Jews and sent them to concentration camps.[33] It is impossible to anticipate today what kind of threat the future will bring; all the government can do is to approach this issue wisely. Because storage of the information as a result of technological development is easy and cheap, the less data that can be potentially misused, the better.

1.4 Historical development of surveillance legislation

The First and Fourth Amendment included in the Bill of Rights are crucial for the right to privacy as they work together as keystones in the protection against government power, which cannot gather information without proper oversight and limitation. The First Amendment states:

> "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise of thereof; or abiding the freedom of speech, or of the free press; or he right of the people to peaceably assemble, and to petition the Government for a redress of grievances."[34]

The purpose of this sentence is to restrict the government from creating a chilling effect on freedom of speech, association, and receipt of ideas, as people would naturally suppress these knowing that government can draw consequences.[35] In addition to this, the Fourth Amendment is worded as follows:

---

[33] Rule, *Privacy in peril*, 42.
[34] „Bill of Rights of the United States of America," Bill of Rights Institute, http://billofrightsinstitute.org/founding-documents/bill-of-rights/ [downloaded on December 26, 2014].
[35] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven: Yale University Press, 2011), pp. 147-148.

> "The right of people to be secure in their persons, houses, papers and effects, against a unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon a probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[36]

As is clear from the wording, the Fourth Amendment protects against those searches and seizures that are unreasonable under the law, and requires authorities to obtain a court warrant upon a probable cause before acquiring information. The probably cause is understood as a reasonably trustworthy information that the search will turn up needed evidence of a conducted wrongdoing.[37]

The Fourth Amendment does not apply always, just in cases when an individual can reasonably expect privacy. Therefore a vast number of situations is not covered, for example police can collect evidence on suspect's plots, where only the immediate surroundings of a house is considered protected under Fourth Amendment. Similarly, trash – abandoned things – cannot be reasonably expected private. These examples are only a fraction of situations where the application of the Fourth Amendment is questionable or excluded.[38]

When the Fourth Amendment was created, there was not the number of decentralized government agencies such as the FBI and the NSA, but the government was rather a narrow group that did not dispose of sophisticated means of intruding people's private sphere. Over time, as the law enforcement body was developing, the Supreme Court had to fill in this emerging gap between the original focus of the Fourth Amendment on the government and the new decentralized agencies.[39] Briefly, the Supreme Court has to determine how the Fourth Amendment applies in cases that were not expected by the Founding Fathers. This development is still ongoing and depends on the available surveillance technology.[40]

During the first decades of the twentieth century, a legal question arose as to whether the Fourth Amendment protection of people's privacy applies only to tangible things, or if also intangible things, as for example conversations, are equally protected.

---

[36] "Bill of Rights of the United States of America."
[37] Solove, *Nothing to Hide*, 95.
[38] Ibidem, 99-100.
[39] Ibidem, 95.
[40] Solove, *Nothing to Hide*, 95.

Several Supreme Court decisions at the turn of nineteenth and twentieth centuries favored only tangible things, since at that level of technological development not so many types of violation were possible.[41]

Subsequently in 1928, a milestone Supreme Court decision *Olmstead v. United* States was reached. In this case, the Supreme Court considered the question, whether it is in accordance with Fourth Amendment to wiretap telephone conversation and use information thus obtained as evidence in criminal procedure, since the Fourth Amendment plays a crucial role in guaranteeing the privacy rights of people. In *Olmstead v. United States* the justices ruled, that this does not constitute any constitutional violation, as "the well-known historical purpose of the Fourth Amendment, directed against general warrant and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will."[42]

The majority ruling established the so-called trespass doctrine, which lasted for of decades. Essence of this doctrine rests in the fact, that there occurred no real physical trespass and thus no truly illegal search under the Fourth Amendment. In another words, a physical entry to defendant's premises is necessary before he would be entitled to complain that his rights were violated.[43] In the year 1928 Louis D. Brandeis, author of the above-mentioned Right to privacy article, was a Supreme Court Justice and he did not agree with the majority ruling in the Olmstead case. He was convicted, that technological progress provided Government with means of espionage on its own people. Brandeis expressed his dissenting opinion:

> "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They sought to protect Americans in their beliefs, 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. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the

[41] Sprague, "Orwell was an optimist," 104.
[42] Ibidem, 103.
[43] William S. Doenges. "Search and Seizure: The Physical Trespass Doctrine and the Adaption of the Fourth Amendment to Modern Technology." *Tulsa Law Review* Vol. 2, Issue 2 (1965): p. 2.

> individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[44]

Similarly, Brandeis warned: "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to jury the most intimate occurrences of the home."[45] In this ruling in which the issue of eavesdropping was negotiated for the first time, the justices of the Supreme Court favored literal interpretation of the Constitution and did not apply it in the new context.

Decades later, in 1967, the Supreme Court overruled the Olmstead decision in *Katz v. United States*, stating that the Fourth Amendment protects people, not places and therefore it covers also electronic communications. In this case, FBI obtained information through recording device attached to the outside of a public telephone booth used by the defendant.[46] The trespass doctrine was overruled: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." [47] The constitutional scope of privacy protection was thus redefined. Justice Harlan defined two key privacy conditions: "First, a person must have an actual, subjective expectation of privacy; and second, that expectation must be one that society is prepared to accept as reasonable." [48] For this reason, surveillance communications, even though done without physical intrusion, such as wiretapping, became a violation of the right to privacy, because what a person seeks to keep private was to be protected by the Constitution. What seems to be more problematic in practice, however, is evaluation of what privacy expectation society is prepared to accept as reasonable.

Considering the year when *Olmstead v. United States* was decided – 1928, the Supreme Court was not facing that high level of technology, which could effectively intrude into everyday lives of all people. We can assume, that in the *Katz* ruling the

---

[44] US Supreme Court. *Olmstead v. United States 277 U.S. 438 (1928)*. Judge Brandeis, dissenting. https://supreme.justia.com/cases/federal/us/277/438/case.html [downloaded on October 31, 2014].
[45] Ibidem.
[46] US Supreme Court. *Katz v. United States 389 U.S. 347 (1967)*. https://supreme.justia.com/cases/federal/us/389/347/case.html [downloaded on October 31, 2014].
[47] Sprague, "Orwell was an optimist", 106.
[48] Ibidem.

Supreme Court judges realized the dangers hidden in the quickly developing technology and reflected this in the perception of the Fourth Amendment privacy protection. All government wiretappings, of both state and federal authorities, became subject to the Fourth Amendment warrant requirements.

The *Katz* decision also incidentally laid foundations for a crucial issue – foreign intelligence surveillance and its compliance with the Fourth Amendment warrant requirements. Justice White pushed through in the final wording of the *Katz* ruling footnote number 23, which states: "Whether safeguard other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security is a question not presented by this case."[49] According to many authors, footnote twenty-three proved to have lasting historical significance, since even though *Katz* case was not dealing with the foreign surveillance issue, the executive branch used the footnote twenty-three for its purposes which was accepted by the lower courts.[50]

Several years later, in 1972, the *United States v. U.S. District Court*, also known as the *Keith Case*, reviewed the Katz's reference to the national security exception. In this case, three members of the White Panther Party were sued for bombing of CIA office. The investigation discovered that agents used warrantless wiretapping of defendant's conversation. Government argued that national security exception is sufficient excuse for this search in order to protect the nation from attempts to subvert the existing structure of the government.[51] The Supreme Court, however, upheld unanimously that the Fourth Amendment warrant requirement applies when domestic security issues are involved.[52]

Nevertheless, further judicial decisions following *Keith* and immediately preceding the Foreign Intelligence Surveillance Act of 1978, to be the focus of the next chapter, decided in favor of the legality of warrantless surveillance in cases when foreign intelligence purposes were involved in order to protect national security.[53] The national security justification of warrantless surveillance proved to be problematic, as

[49] *Katz v. United States*, footnote 23.
[50] Rush Atkinson, "The Fourth Amendment's National Security Exception: Its History and Limits." *Vanderbilt Law Review* Vol. 66, No. 5 (October 2013): p. 1380.
[51] Atkinson, "The Fourth Amendment's National Security Exception," 1381–2; Rebecca A. Copeland, "War on terrorism or war on constitutional right? Blurring the lines of intelligence gathering in post-September 11 America." *Texas Tech Law Review* Vol. 35, No. 1 (2004): 10.
[52] Elizabeth B. Bazan, "The Foreign Intelligence Surveillance Act: An Overview of Selected Issues." Congressional Research Service Report for Congress, Library of Congress, July 7, 2008, p. 1 https://www.fas.org/sgp/crs/intel/RL34279.pdf [downloaded on January 2, 2015].
[53] *United States v. Brown* in 1973 and *United States v. Butenko* in 1974

cases of governmental spying on American citizens were also revealed. Subsequently, in *Zweibon v. Mitchell* (1975), the court held that a court order is necessary for surveillance of domestic organizations even though the surveillance was installed under Presidential order for purposes of national security protection.[54]

The *Zweibon v. Mitchell* decision can be understood as a judicial step back from the extensive national security concept and as a return to giving more weight to First and Fourth Amendment protections. As a consequence, the Foreign Intelligence Surveillance Act was adopted as a legislative act responding to the events of the time reacting to the courts' decisions by providing clear legal boundaries of surveillance under clearly specified conditions.

[54] Elizabeth B. Bazan, "The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions." Congressional Research Service Report for Congress, Library of Congress, February 15, 2007, p. 5 http://www.fas.org/sgp/crs/intel/RL30465.pdf [downloaded on January 2, 2015].

Chapter 2: Legal context of the current surveillance issues

2.1 Foreign Intelligence Surveillance Act

In June 2013, Edward Snowden, an employee of the National Security Agency, revealed the bulk collection of telephony metadata collected by the NSA, prompting public discussions about privacy issues in relation to national security. At the same time, revelation of the PRISM and upstream acquisition of Internet communications added fuel to the fire of general anger. Even though both programs declare to arise from the valid law, their existence and control by the National Security Agency was secret. The NSA is a secret agency created by President Truman in 1952 to decode encrypted foreign communications. It is probably the largest, most costly and most technologically sophisticated spy agency in the world.[55] This chapter introduces both programs analyzing major statutory and constitutional concerns. In order to explain the context, it is necessary to introduce also the Foreign Intelligence Surveillance Act (FISA), which was not originally a part of antiterrorism legislation, but approved earlier in different historical circumstances. It has served, however, as the cornerstone for legislative development after 9/11 – the Patriot Act and both programs revealed by Snowden.

FISA was approved in the year 1978. Its purpose was to create a legal framework solely for the collection of foreign intelligence information through electronic surveillance, to get access to communications of foreign powers and foreign agents. However, the scope of FISA today is much greater because, since 1978, numerous bills amending the original act and changing its content have been approved.

FISA, as it was designed, entitled the President through the Attorney General to authorize electronic surveillance[56] without court order to obtain foreign intelligence information,[57] in maximum period of one year, or alternatively, seek an order from the

[55] Solove, *Nothing to Hide,* 81.
[56] The term of electronic surveillance in this context equals using electronic devices to keep surveillance over a person.
[57] "Foreign Intelligence Information means– (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against– (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning the United States person is necessary to– (A) national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States."

FISA Court (FISC), which remains a special court set up to oversee surveillance activities under FISA. Congress was responsible for the supervision of the process.[58]

When considering the roots of FISA adoption, it is crucial to take into consideration the context of the Cold War and the political affairs of Nixon's presidency. The struggle with the Soviet Union was perceived to be essential for the survival of the United States and the checks and balances of the American political system, to a certain extent, limited the effectiveness of adequate political responses to current events. In order to make the U.S. system more operational, a slow shift in the factual balance of power away from Congress towards the executive branch occurred.[59] Intelligence agencies became more powerful and were able to eavesdrop on people who were not agents of foreign powers and, as individuals, posed no serious threat to national security, i.e., Vietnam War protesters or army personnel who refused to fight in the conflict.[60] In addition, in 1973 the Watergate affair revealed the extensive spying of the Nixon administration on the Democratic Party headquarters. As a response, the Church Committee[61] was established in 1975 to examine the warrantless intelligence gathering by CIA, FBI and NSA. This committee published 14 reports reviewing the warrantless intelligence activities of previous years.[62] Consequently, the Foreign Intelligence Surveillance Act was a legal response to these revelations, banning any further warrantless eavesdropping on people, but allowing some legal space for authorities to adequately respond to the needs of national security by enabling surveillance of potentially dangerous foreign individuals and organizations, suspected of acting on behalf of foreign powers, under specific statutory conditions.

President Carter's signature of FISA took the authorization of secret surveillance out of the exclusive hands of the President's office. All three branches of government were to work strictly in the system of checks and balances again. It is important to stress, that FISA was not drafted as a criminal law statue, but a measure regulating

---

Foreign Intelligence Surveillance Act, 50 U.S. Code, §1801. http://www.law.cornell.edu/uscode/text/50/1801 [downloaded on November 28, 2014].

[58] Francoise Gilbert, "Demystifying the United States Patriot Act." *Journal of Internet Law* 16, no. 8 (February 2013), p. 5.

[59] Foreign Intelligence Surveillance Court. *AllGov. Everything Our Government Really Does.* http://www.allgov.com/departments/department-of-justice/foreign-intelligence-surveillance-court?agencyid=7206 [downloaded on November 28, 2014].

[60] Ibidem.

[61] United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church.

[62] Foreign Intelligence Surveillance Court. *AllGov.*

secret eavesdropping on people suspected of cooperation with foreign powers.[63] Briefly, FISA was adopted to ensure separation of intelligence gathering important for national security from that of criminal investigation by law enforcement.[64] FISA worked under these conditions for more than two decades, until the terrorist attacks of 9/11 changed the rules. The Patriot Act, together with further FISA and Patriot Act amendments, breached the legal safeguard separating these two processes.

2.2 United States Patriot Act

The United States Patriot Act of 2001 is the crucial piece of the U.S. antiterrorism legislation. The act was adopted very quickly and also under questionable, as well as highly problematic circumstances. The usual components of a legislative procedure in the U.S. Congress were ignored, as the negotiations took place behind closed-door, there was no conference committee, no committee report and no final hearing at which opponents could testify.[65] Records from the negotiations are poor, which complicates any effort to get an idea of the legislative intent of the Congressmen.[66] It was signed into law by President George W. Bush only six weeks after the terrorist attacks, on October 26, 2001.

It is difficult to read the Patriot Act, as there is not a consistent text regulating concrete topics, but rather a set of amendments to statues already in place for many years before the Patriot Act was approved, which covered a great range of issues. Given the fact that law, in general, should serve the public in familiarizing people with what they are or are not allowed to do, this act does not serve that purpose. For a casual reader the Patriot Act does not make any sense. Instead of complete formulations of new provisions, the Patriot Act includes only sentences and formulations, cancelled by this statute, added or modified. Consequently, for the reader who is not familiar with exact formulations in the older amended acts, the Patriot Act cannot have any informative value and is very confusing. Just for an illustration, Section 206 states:

---

[63] Bryan Denson. "FISA: Understanding the Foreign Intelligence Surveillance Act (FAQ)." *The Oregonian,* November 26, 2013 http://www.oregonlive.com/news/index.ssf/2013/11/faq_what_is_fisa.html [downloaded on November 28, 2014].
[64] Murray, Wunsch, „Civil Liberties in Times of Crisis."
[65] Robert E. Levy, „The USA Patriot Act: We Deserve Better." Cato Institute. http://www.cato.org/publications/commentary/usa-patriot-act-we-deserve-better [downloaded on November 17, 2014].
[66] Ibidem.

> "Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting ", or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such as other persons," after "specified person".[67]

Ideally there should be available a full wording of the affected laws, such as FISA. It is obvious, that those provisions can cause levels of confusion and legal uncertainty, which is generally understood to be undesirable as democratic states should try to make their legal system as transparent as possible in order to clearly inform the public and prevent the emergence of legal loopholes.

The Patriot Act is also poorly organized and its sentences vaguely formulated. Expressions such as "or in similar cases" or "in general" are common. Taking into consideration those problems together with the length and complexity of the act, as well as the short negotiation process, it is not surprising that there have been concerns about how the bill was prepared at the time of its adoption, and whether Congressmen had enough time to become familiar with what they voted for, especially given the bill's importance to fundamental constitutional questions. The Patriot Act generates concerns as to whether the government still obeys the Constitution, particularly privacy rights of American people as guaranteed by the Fourth Amendment.[68]

2.2.1 Section 218

Criminal investigation requires a higher standard of Constitutional guarantees than foreign intelligence information gathering. Section 218 illustrates very well how the Patriot Act uses slight wording changes to shift balance between government authorities with regard to national security and privacy rights of U.S. citizens. Even though the Section 218 has only one sentence, its impact is far-reaching, as it states:

> "Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are

[67] Section 206, „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001.
[68] American Civil Liberties Union, "Surveillance Under the USA Patriot Act." https://www.aclu.org/national-security/surveillance-under-usa-patriot-act [downloaded on November 20, 2014].

each amended by striking `the purpose' and inserting `a significant purpose"'.[69]

The right to privacy is implied also in the Fourth Amendment which requires a warrant for all searches and seizures in order to prevent unreasonable intrusion in an individual's life, property, papers, and effects.[70] As was mentioned in the previous chapter, since 1967 the *Katz v. United States* Supreme Court decision, this warrant requirement was extended to all areas, where a person can reasonably expect privacy, which now include also emails, phone calls and other private records, where people do not expose the content of communications publicly. The Fourth Amendment requires authorities to present a probable cause, after which a court warrant can be provided.[71] Under FISA it was not necessary for the authorities to provide a probable cause that a crime had been committed, but only a probable cause that the target is a foreign power or an agent of foreign power.[72] This lower standard of warrant requirement was possible just because FISA was not intended to regulate criminal prosecution, but only the collection of foreign intelligence information. Therefore, under FISA, an official applying for electronic surveillance only had to certify that the primary purpose of the intended surveillance was to obtain foreign intelligence information.

In order to avoid violation of this lower Fourth Amendment warrant requirement, there was a legal barrier, "a wall", which prevented law enforcement from exploitation of this intelligence advantage, because circumvention of the warrant requirement in criminal investigation would be a gross violation of the Constitution. A wall was referred to the procedural barriers limiting information sharing between the intelligence division of the FBI and the Criminal Division.[73]

After the terrorist attacks, the wall between intelligence agencies and law enforcement started to be considered undesirable.[74] The 9/11 Commission – designed after the attacks to examine the circumstances and provide recommendations against repeating similar events in future – noted in its final report that the removal of the pre-

[69] Section 218, USA Patriot Act.
[70] Fourth Amendment, Bill of Rights of the United States (1791). Bill of Rights Institute. http://billofrightsinstitute.org/founding-documents/bill-of-rights/.
[71] Fourth Amendment, Bill of Rights of the United States.
[72] Scott J. Glick, "FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security," *Harvard National Security Journal*, Vol. 1 (May 30, 2010) p. 101.
[73] "The 9/11 Commission Report," National Commission on Terrorist Attacks upon the United States, July 22, 2004, pp. 78-79. http://www.9-11commission.gov/report/911Report.pdf [downloaded on November 25, 2014].
[74] Ibidem, 78-80.

9/11 wall between intelligence and law enforcement would open up new opportunities for cooperative action within the sections of FBI.[75] Consequently, the Commission recommended removal of this barrier and strengthening cooperation and information sharing among the government agencies.

The Patriot Act enacted these recommendations into law. Section 218 now requires government only to certify that acquisition of foreign intelligence information is a significant purpose of the proposed surveillance. However much this looks like a simple stylistic change, the shift in the language brings very important consequences. The fact that collection of foreign intelligence information can be instead of "the purpose" – which was the original FISA formulation – only "a significant purpose" of the electronic surveillance, means that amended FISA can now be used also for cases of criminal prosecution, which is a violation of the Fourth Amendment privacy right. In fact, law enforcement is required to obtain a warrant to acquire information for criminal investigation.[76]

FISA was passed solely for the purpose of national security surveillance which differs in certain extent from ordinary domestic criminal surveillance – both have different goals and, therefore, also require slightly different procedures and policy. [77] In cases of national security surveillance, different standards may be compatible with the Fourth Amendment if they are proved to be reasonable, both in relation to the legitimate government need of intelligence information, and the protected privacy rights of citizens. However, reality is not always that easy and the division between intelligence and law enforcement is not crystal clear. This is what the 9/11 Commission referred to when they recommended the removal of the procedural wall: allowing relevant intelligence information needs link to criminal investigators.[78] Proponents of privacy rights and restrictive interpretation of the Fourth Amendment warrant requirement suggested limiting the warrantless intelligence activities under FISA with changing the provision to "sole purpose", so that the sole purpose of surveillance must be to obtain foreign intelligence. The U.S. Supreme Court evaluated this suggestion in the *Truong Dinh Hung v. United States* case, but rejected it, stating that all intelligence

[75] Ibidem.
[76] Glick, "FISA's Significant Purpose Requirement," p. 109.
[77] Elisabeth B. Bazan, "The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions." Congressional Research Service Report for Congress, Library of Congress, September 22, 2004, p. 5 http://www.fas.org/irp/crs/RL30465.pdf [downloaded on January 2, 2015].
[78] "The 9/11 Commission Report," 79.

investigations are at least in part also criminal investigations and therefore these two processes cannot be effectively completely separated from each other.[79]

When speaking of FISA purposes, it is essential to mention that the text of the act has never included the word "primary" – officials had only to confirm, that "the purpose" of the surveillance is acquiring foreign intelligence information. However, it became a legal habit to use the term "primary purpose" in describing the actions of the government.[80]

Nevertheless, the special sensitive circumstances of warrantless surveillance anchored in the act have become applicable to a wider scope of targets since the Patriot Act. Even though the Foreign Intelligence Surveillance Court of Review later limited the government – declaring that if the government's primary purpose was criminal prosecution, then it could only use FISA if it intended to prosecute the alleged terrorist or spy for a foreign intelligence crime – such legal changes raise concerns.[81]

2.3 PRISM and upstream acquisition of Internet communications

In the last two years, discussion about the acts of government authorities in respect to privacy rights of individuals has been escalated. The legal development of antiterrorism and surveillance legislation did not stop with the Patriot Act. Edward Snowden brought to light two National Security Agency surveillance programs whose statutory and constitutional challenges are elaborated in this chapter.

PRISM and upstream acquisition of Internet communications is legally anchored in Section 702 of the FISA Amendments Act of 2008. In contrast to the bulk collection of telephony metadata, this program collects content of the communications and is focused on a narrower group of persons.[82] In general, Section 702 program faces lower levels of criticism because it is a valuable and important national security tool and is not

---

[79] Jessica M. Bungard, "The Fine Line between Security and Liberty: The "Secret" Court Struggle to Determine the Path of Foreign Intelligence Surveillance in the Wake of September 11th." *University of Pittsburgh School of Law Journal of Technology Law and Policy* Vol. IV, Article 6 (Spring 2004) p. 15.
[80] Scott. "FISA's Significant Purpose Requirement," 111.
[81] Ibidem, 111-112.
[82] John W. Rollins and Edward C. Liu. "NSA Surveillance Leaks: Background and Issues for Congress." Congressional Research Service Report for Congress, Library of Congress, September 4, 2013, p. 3 http://www.fas.org/sgp/crs/intel/R43134.pdf [downloaded on January 1, 2015].

primarily focused on U.S. citizens.[83] The collected information must fit the definition of foreign intelligence information according to FISA.[84] This program cannot run when a target – any person whose communications are being collected – is a U.S. citizen or a foreigner currently located on U.S. soil. The reason for this is Fourth Amendment protection, which relates to U.S. citizens and everybody located in the United States. The program also cannot be applied in cases, when targeting of two non-U.S. persons[85] located abroad should indirectly lead to collection of information about somebody protected by the Fourth Amendment.

The program consists of two means of collecting communications of foreign targets through American networks, both under Section 702 – PRISM and the so-called upstream collection of communications. The difference between them is in what phase of sending is the communication, for example an email, collected. Under the PRISM system, the communication is taken directly from the Internet service providers. On the other hand, during the upstream collection, the communications are collected while messages are in transit. Targeted persons can be senders, receivers or even the subjects of the communication; an example is a targeted person mentioned in an email conversation of two untargeted persons.[86] The upstream acquisition can also be focused on phone calls, which is not possible under PRISM. PRISM serves as a mean of access to the Internet service providers and covers approximately 91% of all communications targeted under Section 702.[87]

The NSA is required to have FISC approval plus a written directive from both the Attorney General and the Director of National Intelligence for collection of contents of the communications.[88] The FISC evaluates whether there is a probable cause that the targeted person is a foreign power or its agent, and that the communications are owned, possessed or will be used by the target. The approval is valid as long as one year. [89]

---

[83] Ibidem, 3.
[84] "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," July 2, 2014. Privacy and Civil Liberties Oversight Board, p. 6. http://www.pclob.gov/Library/702-Report-2.pdf [downloaded on November 26, 2014].
[85] Non-U.S. person means in this context neither citizen, nor permanent resident.
[86] Rollins, Liu, "NSA Surveillance Leaks," 4.
[87] Edward C. Liu, "Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments. Congressional Research Service Report for Congress, Library of Congress, April 1, 2014, p. 10 https://www.fas.org/sgp/crs/intel/R43459.pdf [downloaded on January 1, 2015].
[88] Rollins, Liu. "NSA Surveillance Leaks," 11.
[89] Ibidem, 7.

Subject of criticism in this context is the fact that in a number of cases it is impossible to determine with certainty, whether the targeted person is located in the United States or not and, therefore, should be protected by the Fourth Amendment warrant requirement. Similarly, due to technical imperfections some data is collected of unrelated communications of U.S. citizens.[90] This happens either incidentally, for example, when two targeted foreigners share an email conversation about a U.S. citizen, or when a U.S. citizen emails to a targeted foreigner, or inadvertently, due to technical errors.[91] This information cannot be used and must be destroyed.[92]

Even though civil rights organization criticize Section 702 collection programs as the imperfections lead to accidental collection of communication of U.S. citizens, experts mostly agree on the necessity of having such national security tools and consider the oversight mechanism to be sufficient. There is also an interesting debate about protection of privacy of non-U.S. persons and is mentioned in the Chapter 3.

2.4 Bulk collection of telephony metadata program

In June 2013, the British *Guardian* published a story about the collection of phone records of millions Verizon customers on a daily basis. Glenn Greenwald, author of the article, revealed the content of the FISC order granting the FBI unlimited authority to obtain data on all phone calls made within the United States and between the U.S. and other countries for a three months period starting in April 2013. According to the author, the court order also expressly prohibited Verizon from disclosing this information to the public.[93] It revealed for the first time that President Obama continued the large-scale collection of call records data, which was known to be happening during the Bush Administration.[94]

What the *Guardian* publicly disclosed was in reality a three-month extension of a program that was at that had been ongoing for seven years.[95] This program, the bulk collection of telephony metadata, is legally anchored in Section 215 of the USA Patriot Act, titled *Access to records and other items under the Foreign Intelligence*

[90] Ibidem, 13.
[91] Report on the Surveillance Program Pursuant to Section 702, p. 86.
[92] Report on the Surveillance Program Pursuant to Section 702, p. 91.
[93] Glen Greenwald, "NSA collecting phone record of milions of Verizon customers daily," *The Guardian,* June 6, 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [downloaded on November 23, 2014].
[94] Ibidem.
[95] Rollins, Liu. "NSA Surveillance Leaks,"1.

Surveillance Act, which was an amendment also changing the original version of FISA. Even though Edward Snowden made this Section publicly known, the bulk collection call information is not the only mean of implementing the. It also permits access of governmental agencies, such as the FBI, to personal records of people held by physicians, bookstores, universities, Internet service providers, and libraries. Legal authority of Section 215 enlarged the scope of materials that may be sought by the government and lowered the legal standard required to be met.[96]

Even though information about this program is still classified, many facts have been released by the Administration itself in order to assure the public of the program's compliance with the Constitution. It is known that not only Verizon, but also other major American telecommunications providers have been required to provide information. The description of this program, collecting metadata "in bulk", aims to distinguish it from the narrower collection of metadata of an identified individual or group of individuals. As a result, the National Security Agency has an access to all phone calls made in the United States or to calls made by individuals since 2006, when one person is located in the U.S. and the other in a foreign country.[97]

What does the term metadata actually mean? It refers to data about a phone call, but not the content of the conversation. Intelligence has thus access to the number that was dialed from, the number that was dialed to, and the date and duration of the call. Information about the location of those calling is not included, except the area code identified in the phone number.[98] Here arises the first objection from the perspective of privacy advocates: can we consider such collection of data anonymous in a situation, when phone numbers are another identifier of people? From this perspective, pointing to distinction between a telephone number and subscriber identity seems to be insignificant.[99]

The bulk collection metadata program raises concerns of privacy advocates on two basic levels where the legality of the program can be challenged. The first level is whether the program is in compliance with the statutory law in the first place, which means whether it can be really subsumed under the Section 215 of the Patriot Act. The second level, more publicly known, is the constitutionality of the program. Privacy

[96] Ibidem, 4.
[97] Liu. "Overview of Constitutional Challenges," 2.
[98] Rollins, Liu. "NSA Surveillance Leaks," 2.
[99] Ibidem.

advocates challenge the telephony metadata program regarding potential Fourth Amendment as well as First Amendment violations. There were two crucial lawsuits filled in federal district courts that are relevant to these constitutionality concerns: *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*. In both decisions, the courts drew different conclusions that are interesting to consider, but before the constitutional level is the statutory issue.

The independent bipartisan Privacy and Civil Liberties Oversight Board which works within the executive branch, published in August 2012 a report on the bulk metadata collection program, in which it paid significant attention to the questions of legality. According to the Report, Section 215 does not constitute a sufficient legal basis for the bulk collection program for several reasons.[100] First, the data obtained through the bulk collection program are not at the moment of their collection connected with a specific FBI investigation, but are stored simply just in case they will be needed in the future. Similarly, a collection in bulk cannot be regarded relevant to any FBI investigation, because relevant are only particular pieces of information, not all of them. Third, the program makes the telephony companies collect complex sets of data on a daily basis even though there is no legal foundation which would require them to do so. In addition, according to Section 215, it is the FBI that is entitled to collect items and information needed for investigation, not the National Security Agency.[101] In reality, however, the FBI only applies for the collection order, but the NSA, an organization not statutory entitled to carry out the collection, collects and stores all the data. The NSA is also prohibited by the FISC to share the data with FBI except in situations explicitly mentioned in the FISC orders.[102]

On the other hand, some experts deny any discrepancy between the wording of Section 215 and the bulk collection program. For example Rachel Brand or Elisabeth Collins Cook, prominent lawyers, are persuaded that the reading of Section 215 stating the bulk collection is unstatutory is only one of possible interpretations.[103] It is crucial to take into account that two Administrations and a number of experts and officials

[100] "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," January 23, 2014. Privacy and Civil Liberties Oversight Board, p. 10. http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf [downloaded on November 22, 2014].
[101] "Report on the Telephone Records Program," 10.
[102] Ibidem, 88-89.
[103] Ms. Brand and Ms. Collins are lawyers, members of the Privacy and Civil Liberties Oversight Board who also served in various top governmental positions.

considered the program in good faith to be in compliance with Section 215. Similarly, the program itself also works in good faith.[104] There is an extensive system of safeguards and oversight, therefore the bulk collection program needs to be considered as statutory, even though supporters admit that this question is difficult.[105]

From the perspective of the U.S. Constitution, there the two cases, the *American Civil Liberties Union v. Clapper* and *Klayman v. Obama*. The principal legal question in these lawsuits was whether the government has engaged in searchech, which occurs when a subjective expectation of privacy recognized by the society as reasonable is violated by the government.[106] The Foreign Intelligence Surveillance Court issuing the order for metadata collection, similarly as the two courts deciding the lawsuits, took into consideration an older Supreme Court decision *Smith v. Maryland* (1979). In *Smith*, a telephone company installed upon police requests a pen register – a device recording the dialed outgoing numbers – in order to find out whether Mr. Smith had called a victim of a robbery. There were concerns that installation of the pen register violates the Fourth Amendment. However, the Supreme Court concluded that the Constitution was not violated, because Mr. Smith had no legitimate expectation of privacy in the telephone numbers he dialed.[107] The decision was built on a third party doctrine – a theory about the loss of privacy protection when somebody voluntarily shares information with a third party, even if the third party is a private company or government.[108] If Mr. Smith, according to the ruling, could not expect privacy in dialing the numbers, the police did not need to conduct a search and therefore the Fourth Amendment was not violated.

FISC builds its argumentation analogically on the logic introduced by the Supreme Court in *Smith*: "Where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence ex nihilo."[109] FISC argued that issuing the order for collection of telephony metadata under Section 215 is constitutional, as the Fourth Amendment "imposed any impediment to the government's

[104] Good faith is a legal term referring to a situation in which a person is persuaded about rightfulness of his or her actions. Good faith brings a certain legal protection and mitigates negative consequences.
[105] "Report on the Telephone Records Program," 210, 215.
[106] Liu. "Overview of Constitutional Challenges," 6.
[107] Liu. "Overview of Constitutional Challenges," 6.
[108] US Supreme Court, *United States v. Jones 565 U.S. (2012)* https://supreme.justia.com/cases/federal/us/565/10-1259/ [downloaded on November 23, 2014].
[109] Liu. "Overview of Constitutional Challenges," 7.

proposed collection. Having found none in accord with U.S. Supreme Court precedent"[110] – here is the FISC referring to the *Smith* decision – the FISC issued the requested orders. Accordingly, in *ACLU v. Clapper*, the District Court for the Southern District of New York concluded that lower courts are bound to apply *Smith* unless the Supreme Court itself has explicitly overruled it.[111]

Despite these decisions, in *Klayman v. Obama*, the District Court for the District of Columbia presents a totally different perspective on the same issue. The Court took into consideration the scope of the information collection, which differed greatly from the simple pen register in *Smith* that this decision is for the purpose of evaluating NSA metadata collection of little value. The aggregation of telephone records can therefore result in Fourth Amendment search.[112] The D.C. District Court introduced a more suitable "mosaic theory" arguing, that even though short them collection of information does not necessarily violate expectation of privacy of individuals, in a long term perspective such search creates a wealth of detail – a mosaic about person's familial, political, professional, religious, and sexual associations.[113]

Validity of the mosaic theory was examined in a short-term experiment at Stanford University, where computer science students evaluated how sensitive metadata are. They used phone metadata of 546 volunteers and revealed detailed information, for example a person having an abortion or an owner of a specific brand of firearm, as the structured nature of the data reveals a lot, for example calling to a suicide hotline for three hours during night.[114]

Concluding that the collection of metadata was a search, the D.C. District Court also focused on the question whether the search was reasonable under the Fourth Amendment. The core of the issue lies actually in the fact that warrants allowing searches have to be based upon probable cause. There exists, however, a "special

---

[110] Ibidem.
[111] United States District Court Southern District of New York. *American Civil Liberties Union v. Clapper No. 13 Civ. 3994 (WHP) (S.D.N.Y. Dec 27, 2013)* https://casetext.com/case/aclu-v-clapper [downloaded on November 23, 2014].
[112] United States District Court for the District of Columbia, *Klayman v. Obama*, December 16, 2013. http://online.wsj.com/public/resources/documents/JudgeLeonNSAopinion12162013.pdf [downloaded on November 23, 2014].
[113] *Klayman v. Obama*.
[114] Clifton B. Parker. "Stanford students show that phone record surveillance can yield vast amounts of information." *Stanford News*, March 12, 2014. http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html [downloaded on November 24.2013].

needs" exception applicable in extraordinary cases making the normal warrant procedure impracticable, such as drug testing of high school students, automobile checkpoints for illegal immigrants, drunk drivers or searching planes, the subway or passengers' carry-on bags.[115] D.C. District Court evaluated the NSA program as neither stopping an imminent attack nor otherwise aiding the Government in achieving any objective that was time sensitive in nature. For this reason and for the serious violations of privacy of people, the metadata collection program was considered to be unreasonable under the Fourth Amendment.[116]

The bulk collection program is constitutionally controversial also from the perspective of the First Amendment, particularly the freedom to peacefully assemble. The program collects huge amount of data where certain patterns of connections and frequency of associations among individuals and organizations can be easily found. People who are engaged in legal, but controversial activity may feel vulnerable and therefore limit those activities, even though the Constitution guarantees them this right. Among the potentially threatened groups belong investigative journalists and political activists as well as whistleblowers.[117]

It is expected that the *Smith v. Maryland* decision as an appropriate legal basis for evaluating the bulk metadata program will be challenged. In many ways, the circumstances of the year 1979 when the *Smith* was decided do not correspond with the level of surveillance at present. According the records, Mr. Smith's phone calls were examined for three days. Technology that was used collected only information about phone numbers dialed, not about the length and time of the calls. Mr. Smith was also a suspect in a criminal investigation. The differences from current issues are obvious. Not phone calls of one person are being examined, but all phone calls made by all U.S. citizens, adding the links between the length and time when the call occurred. Moreover, there is the fact that almost everybody has a private phone number today, compared to 1979 when phones were shared by groups of people – families or companies.[118] The third party doctrine is another aspect, whose suitability for the purposes of bulk metadata collection seems questionable. The argument, that people

[115] Liu. "Overview of Constitutional Challenges," 8.
[116] *Klayman v. Obama*.
[117] Report on the Telephone Records Program, 132-135.
[118] Nadia Kayyali. "In Klayman v. Obama, EFF Explains Why Metadata Matters and the Third-Party Doctrine Doesn't." *Electronic Frontier Foundation*, November 3, 2013. https://www.eff.org/deeplinks/2014/11/klayman-v-obama-eff-explains-why-metadata-matters-and-third-party-doctrine-doesnt [downloaded on November 26, 2014].

when dialing a phone number are submitting this information to a third party and cannot expect privacy is problematic, because this is how making a phone call works and it has nothing in common with a conscious and voluntary choice.[119]

However, what must not be forgotten in these debates is the fact, that even though the suitability of the *Smith v. Maryland* decision for the present issues may be questionable, it is a valid Supreme Court ruling and as such it is part of law of the United States until it is overruled.[120] On the other hand, *Klayman* case shows that it is possible to make a distinction stating that the Supreme Court decision does not apply. In January 2014 the government filled notice of appeal against the decision in *Klayman v. Obama*. The hearing in this case was held on November 2014. During December 2014, another case challenging legality of the metadata program, *Smith v. Obama*. Final rulings have not been published yet therefore the question of constitutionality of the bulk metadata collection remains in progress.

[119] Ibidem.
[120] Report on the Telephone Records Program, 215.

Chapter 3: Challenges of Pandora's Box

3.1 Pendulum effect: back to land of freedom

Thirteen years have passed since the 9/11 terrorist attacks and the subsequent legal provisions reshaped the balance between national security and personal liberties, especially the right to privacy. The previous chapter introduced the current legal mechanisms behind the major privacy debates in the United States. However, society and its priorities change. Over the years, a certain shift has occurred in the perception of the optimal line between the two legitimate interests.

It is not sufficient to examine the development only on statements of Democratic and Republican politicians as their opinions on this issue naturally depend to a great extent on when they were the governing or opposing party. For illustration, in 2005 during George W. Bush's presidency, Democrats criticized the NSA warrantless domestic eavesdropping controversy that was at that time revealed by the New York Times, while Republicans defended the NSA's authority emphasizing security interests. Today, Republicans condemn every new eavesdropping disclosure and Democrats advocate for the Obama administration's policies.[121]

It is far more informative to examine the perception of security measures and civil rights evolution in the eyes of U.S. citizens. The Pew Research Center, a non-partisan think tank based in Washington D.C., conducted a survey documenting this public development. In 2004, 29% of respondents stated that government's anti-terrorism policies had gone too far in restricting civil liberties, whereas 49% of respondents replied that these policies have not gone far enough to protect the country. Nine years later, in 2013, this ratio reversed and 47% of respondents were persuaded that the policies have gone too far and 35% spoke in favor of them. Generally speaking, government surveillance powers today pose a bigger threat than terrorism for a higher number of U.S. citizens than post 9/11.[122]

This development appears to support the validity of the so-called pendulum argument. The pendulum theory argues that in times of national crisis – in a war, after an attack or generally when people feel their safety is threatened – personal liberties are

---

[121] Gleen Greenwald, *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books. Henry Holt and Company, LLC, 2014), pp. 197-198.
[122] Pew Research Center, "But More Approve than Disapprove. Few See Adequate Limits on NSA Surveillance Program." July 26, 2013, page 5, http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf [downloaded on December 12, 2014].

naturally curtailed and civil rights protection weakened. As soon as the danger passes, the scope of freedoms and liberties naturally recovers. Restriction of freedom under immediate threat is a natural human reaction; according to the former Supreme Court Justice William Rehnquist, it is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as in peacetime.[123] Laws in such situation are not silent, but "speak with somewhat different voice."[124] This opinion shared another Supreme Court Justice, Robert H. Jackson, who expressed this in 1949: "The Constitution is not a suicidal pact."[125] The belief that protection of civil liberties and Constitutional rights cannot at the same time threaten the safety of the state and its people denies Daniel Solove: "The protection of liberty is most important in times of crisis, when it is under the greatest threat. During times of peace, because we are less likely to make unnecessary sacrifices of liberty, the need to protect it is not as dire."[126]

Since 9/11 as no other comparable attacks occurred, people started to approach the security issue more soberly. David Cole argues, that the swing of the pendulum back to civil rights does not however happen automatically by some kind of gravity, but relies on various external forces, which must come into play. Among those belong the Supreme Court overruling older decisions, reports of investigative journalists, whistleblowers revealing secrets, Congressmen paying higher attention to what they oversee, and, especially, strong civil rights groups. According to Cole, civil rights survived in the United States, despite the measures adopted after 9/11, in which he includes extensive surveillance threatening right to privacy, torture, and indefinite detention.[127]

In times of crisis, the system of checks and balances can fail as the judicial branch does not reliably reverse excesses made of the executive. After 9/11, a number of new civil liberties groups emerged to play the role of living Constitution, pointing out problems and thereby contributing to solutions.[128] For example, the American Civil Liberties Union, in the ACLU v. Clapper case, focused on the issue of the bulk collection program violating the Fourth Amendment.

---

[123] Solove, *Nothing to Hide*, 55.
[124] Ibidem.
[125] Ibidem.
[126] Ibidem, 61.
[127] David Cole, "Where Liberty Lies: Civil Society and Individual Rights After 9/11." *Georgetown Public Law and Legal Theory Research Paper* No. 12-164, 2012. Page 1254. http://scholarship.law.georgetown.edu/facpub/1119/ [downloaded on November 26, 2014].
[128] Ibidem, 1205-1206, 1250.

Civil liberties groups and privacy advocates, the Obama administration, and representatives of the telecommunications providers drafted the USA Freedom Act in 2013. This bill aimed to address the major privacy concerns, to end the bulk collection of telephony metadata by the NSA, as was recommended in the final report of the Privacy and Civil Liberties Oversight Board, and also modify Section 702 of FISA – while still preserving Intelligence Community capabilities.[129] In contrast, thirteen years earlier the Attorney General openly labeled critics of the Patriot Act and government policies unpatriotic.[130] The fact that Jim Sensenbrenner, author of the Patriot Act, and a later strong opponent of the NSA bulk data collection, introduced the USA Freedom Act in the House of Representatives, testifies to the opinion shift even among legislators who originally proposed the antiterrorist surveillance measures.[131]

Negotiations on the bill ended unsuccessfully in Senate in November 2014 for various reasons. For some privacy advocates, the negotiations shifted the bill too far from the original intent. Senator Patrick Leahy, a lead sponsor of the bill, said that opponents of the bill contributed to the failure by using scare tactics about terrorist threats. His words were in reaction to Mitch McConnell's statement about hampering of the USA Freedom Act to protect Americans against the Islamic State.[132] The Obama Administration, advocated for months to address the issue of privacy violations, strongly supported the bill as a "reasonable compromise that enhances privacy and civil liberties and increases transparency."[133] The director of the ACLU's Washington legislative office expressed her disappointment after the failure of negotiations: "This was the last best chance to get something down before Snowden fades from public consciousness."[134]

---

[129] Letter from Attorney General Eric Holder and Director of National Intelligence James Clapper to Chairman Patrick Leahy, concerning the USA Freedom Act. September 2, 2014. https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/2014-9-2-FISA-letter-from-AG-and-Clapper-to-Leahy-on-S.-2685-USA-Freedom....pdf [downloaded on November 30, 2014].
[130] Jeffrey Tobin, "Ashcroft's Ascent. How far will the Attorney General go?" *The New Yorker,* April 15, 2002. http://www.newyorker.com/magazine/2002/04/15/ashcrofts-ascent [downloaded on December 3, 2014].
[131] Cyrus Farivar, "Patriot Act author says NSA's bulk data collection is unbounded in its scope," *Ars technica,* September 5, 2013. http://arstechnica.com/tech-policy/2013/09/patriot-act-author-says-nsas-bulk-data-collection-is-unbounded-in-its-scope/ [downloaded on December 3, 2014].
[132] Erin Kelly, "NSA spying bill stalls in Senate vote," *USA Today*, November 18, 2014. http://www.usatoday.com/story/news/politics/2014/11/18/leahy-usa-freedom-act-nsa-spying/19222895/ [downloaded on December 3, 2014].
[133] Letter from Holder to Clapper concerning the USA Freedom Act, https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/2014-9-2-FISA-letter-from-AG-and-Clapper-to-Leahy-on-S.-2685-USA-Freedom....pdf.
[134] Kelly, "NSA spying stalls in Senate vote."

Now the new Congress will control this issue in the next year. The problems remains open and civil rights organizations will probably push for another satisfying proposal – the Electronic Frontier Foundation considers the Freedom Act to be a floor for further negotiations, not its ceiling.[135]

3.2 Exploitation of the collected data

People under the influence of threats and willing to surrender part of their rights, for example privacy, probably expect that the new security measures will not affect them. It is true that surveillance and extensive security measures do not affect the whole society equally as minorities or politically controversial people are more likely to be targeted in the first place.[136] Snowden's revelations, showing that NSA programs collecting massive amounts of personal data can affect everyone's lives, raise questions of how the data is stored, examined and overseen.[137]

The vast majority of the material has no relevance to national security but it reveals private lives of people. Moreover, experts argue that the information leads to a certain level of distortion, as data show a lot but fail to reflect the whole personality. When the government possesses the material, it can harm individuals, intentionally, or, more likely, inadvertently. Daniel Solove provides an example of a person who writes a crime book and for the storyline needs to know different ways how to produce methamphetamine. He buys for this purpose two specialized books. If the government reveals the purchase, the author might be groundlessly considered dangerous.[138]

Both the NSA telephone data collection and the acquisition of Internet communication under Section 702 rely on orders of the Foreign Intelligence Surveillance Court, which is crucial for proper implementation of the programs and for prevention of misuse of acquired information. Unfortunately for civil rights, transparency and impartiality of the FISC decision-making can be problematized.

The Foreign Intelligence Surveillance Court (FISC) is a special body established for purposes of controlling the surveillance activities of FISA. The Patriot Act expanded the number of FISC judges from the original number of seven to eleven in total. The

---

[135] Kurt Opsahl and Rainey Reitman, "A Floor, Not a Ceiling: Supporting he USA FREEDOM Act as a Step Towards Less Surveillance," *Electronic Frontier Foundation*, November 14, 2013. https://www.eff.org/deeplinks/2013/11/floor-not-ceiling-supporting-usa-freedom-act-step-towards-less-surveillance [downloaded on December 4, 2014].
[136] Greenwald, *No Place to Hide*, 200.
[137] Solove, *Nothing to Hide*, 28.
[138] Ibidem, 31.

judges are appointed solely by the Chief Justice of the United States for seven years, work in FISC only part-time and do not even receive an extra salary for this work. [139] The fact that the judges do not work full-time is one subject of criticism: they cannot entirely focus on their work which makes of FISC more or less a "rubber stamp"[140] court as applications are not adequately examined and are just approved in most cases. According to Reuters, between 2001 and 2012, the FISC judges approved 20,909 surveillance and property search warrants and during that period denied or withdrew only 36 applications.[141] Whether the Reuters' sources are reliable or not, it is important to take into consideration, that the court is secret, there are only the judges and the applicant present and therefore an adversarial argument is not possible. Moreover, most of the cases are still classified.[142] Even supporters of both surveillance programs admit that FISC needs significant reform. It would enhance the quality of its work if opposing views could be heard when ruling on surveillance requests.[143] The failed USA Freedom Act addressed the transparency issue and proposed creating an Office of a Special Advocate tasked with promoting privacy interests before the FISC closed proceedings. The bill also aimed to improve the reporting requirements, because the Congress is the body entitled to oversee both programs.[144]

Since the USA Freedom Act was not adopted, the FISC continues to work under the old rules and exploitation of the collected data relies on mechanisms anchored within both programs. Intentional misconduct or bad faith of any government officials or agents involved in the bulk collection program under Section 215 has not been proven.[145] However, benefits of this program for national security and anti-terrorism operations are, according to many experts and even the Obama administration itself, questionable, if indeed there are any. President Obama announced in March 2014 the

---

[139] David Gewirtz, "For spy court judges, overseeing America's surveillance efforts is a part-time job," *ZD Net,* February 10, 2014 http://www.zdnet.com/article/for-spy-court-judges-overseeing-americas-surveillance-efforts-is-a-part-time-job/ [downloaded on December 5, 2014].
[140] Russel Tice, a former NSA agent, said that the FISC is a „kangaroo court with a rubber stamp". Spencer Ackerman, "FISA chief judge defends integrity of court over Verizon records collection," *The Guardian,* June 6, 2013 http://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance [downloaded on December 4, 2014].
[141] John Shiffman and Kristina Cooke, "The judges who preside over America's secret court," *Reuters*, June 21, 2013 http://www.reuters.com/article/2013/06/21/us-usa-security-fisa-judges-idUSBRE95K06H20130621 [downloaded on December 4, 2014].
[142] Ackerman, "FISA chief judge defends integrity of court over Verizon records collection."
[143] "Report on the Telephone Records Program," 13.
[144] Congressman Jim Sensenbrenner, The USA Freedom Act http://sensenbrenner.house.gov/legislation/theusafreedomact.htm [downloaded on December 5, 2014].
[145] "Report on the Telephone Records Program," 9.

intent to shut down the NSA phone program, which recommended also the Privacy and Civil Liberties Oversight Board.[146] The Congress, however, has not adopted new legislation and the government has therefore sought another order to reauthorize the program for 90 days expiring on February 27, 2015.[147]

The government enacted certain changes of the rules under which can be the collected metadata examined in February 2014. All the collected metadata is placed in a huge database where it remains five years when it must be deleted. The metadata can be searched by a narrow group of trained expert analysts only when there is a reasonable articulable suspicion that the telephone number is associated with one the foreign intelligence targets approved in a FISC order.[148] A reasonable, articulable suspicion is required to protect against the indiscriminate querying of the collected data.[149] In such an authorized query, telephone numbers that have been in contract with this terrorist-associated identifier can also be examined and then further associated with contacts in a chain.[150] President Obama limited the contact chaining in February 2014.[151]

According to the wording of Section 215, the acquired data needs to be relevant to an authorized investigation. Section 215 does not redefine the term "relevant" therefore it needs to be interpreted in its ordinary meaning. Since the metadata are collected in bulk, and at the time of their gathering, are not connected with a particular FBI investigation, many experts consider the bulk collection inconsistent with the relevance requirement.[152]

The PRISM and upstream acquisition of Internet communications under Section 702 targets people protected by the Fourth Amendment – either U.S. persons or foreigners located on U.S. soil, as explained above in chapter 2. The question of national security exceptions for warrantless foreign intelligence surveillance, elaborated in chapter 1, is interesting also from the perspective of pendulum effect. In 2008, the

---

[146] Ibidem, 168.
[147] "Joint Statement from the Office of the Director of National Intelligence and the Office of the Attorney General on the Declassification of Renewal of Collection Under Section 501 of the Foreign Intelligence Surveillance Act," *Office of the Director of National Intelligence. IC on record,* December 4, 2014. http://icontherecord.tumblr.com [downloaded on December 4, 2014].
[148] "Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act," Administration White Paper, August 9, 2013, page 3 http://www.documentcloud.org/documents/750210-administration-white-paper-section-215.html [downloaded on December 4, 2014].
[149] Ibidem.
[150] Ibidem.
[151] Joint Statement on the Declassification of Renewal of Collection Under Section 501.
[152] "Report on the Telephone Records Program," 58.

Foreign Intelligence Surveillance Court of Review considered the purposes of foreign intelligence investigations sufficiently important and different from traditional law enforcement to justify an exception to the warrant requirement. In other words, the procedures used were assumed to be reasonable when balanced against the government interest in protecting national security, which was of the "highest order of magnitude."[153] Three years later, in 2011, the same court considered the same question again but this time came to an opposite conclusion. According to the new opinion, some elements of the collection program were statutory deficient and, therefore, inconsistent with the Fourth Amendment. Government's interests were not of the highest magnitude anymore.[154] The FISCR ruled, that the minimization procedures – mechanisms to exclude information about U.S. persons under the Fourth Amendment – were insufficient especially in cases when a U.S. person is mentioned in a communication of two legitimate targets.[155]

It is interesting how the FISCR's prioritization of national security and civil rights changed. In addition, Obama Administration declassified records about these two Court analyses in 2013. This can be understood as a swing of a pendulum back to civil rights due to public pressure after Snowden's revelations. Another reason can also be the decreasing willingness of other nations and foreign companies to participate in data sharing with U.S. firms or loss of credibility of the U.S. commitment to an open and secure global Internet.[156]

The classified character of the NSA files makes it difficult to determine with certainty what happens to the U.S. data collected inadvertently. Generally, when a collected communication is wholly domestic – involves only U.S. persons – it must be destroyed upon recognition.[157] However, if the communication is not wholly domestic – involves also non-U.S. persons – it does not need to be destroyed if the information contained is encrypted, believed to be relevant to cyber security or usable for intelligence purposes or suggests criminal activity or threat of harm to people or

[153] Rollins and Liu, "NSA Surveillance Leaks," 9.
[154] Ibidem.
[155] Ibidem, 13.
[156] "Presidential Policy Directive PPD-28. Signals Intelligence Activities," *The White House,* January 17, 2014. http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [downloaded on December 8, 2014].
[157] "Report on the Surveillance Program Pursuant to Section 702," 54.

property. In those cases, the NSA in fact gains information whose acquisition otherwise requires a warrant.[158]

Recently, the U.S. government also considers the question whether and to what extent the United States should guarantee the same level of privacy protection of non-U.S. persons with respect to foreign surveillance.[159] President Obama issued a directive stating that: "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in handling of their personal information."[160] However the Section 702 programs remains in force because it is a valuable national security tool and there is not an adequate program to replace it yet.

Snowden's whistleblowing opened the issues between privacy rights and justifiable authorities of government and its agencies. He approached his revelations differently from the previous whistleblowers, Daniel Ellsberg and Bradley Manning, who published the documents in bulk. Snowden, on the other hand, decided to hand the files over to a carefully chosen journalist who was able to present the information in context. Regardless of how the statutory and Constitutional concerns will be resolved, the American people took an important step towards more transparent and considered balance between national security interests and right to privacy in the recent past.

---

[158] Glen Greenwald, "The top secret rules that allow NSA to use US data without a warrant," *The Guardian*, June 20, 2013. http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant [downloaded on December 8, 2014].
[159] "Report on the Surveillance Program Pursuant to Section 702," 100.
[160] "Presidential Policy Directive PPD-28."

Conclusion

It remains to summarize the findings from the previous chapters about the contradiction between the proclaimed freedom and the factual extensive surveillance, and answer the question whether the United States shifted from the land of freedom to the land of surveillance? There is no clear answer to this question and every attempt to answer it decidedly would inevitably lead to a certain level of simplification and distortion as there is no evident and universally applicable rule for where the balancing line between freedom of individuals and national security measures should be drawn.

Perception of the boundary between individual rights of the governed and the authorities of government depends largely on the cultural and political customs of each particular country, on the level of threat the society is facing and it derives also from the state's political ideology. The United States is somewhere in the middle between the extreme ideology of totalitarianism at the one end and libertarianism at the other, where libertarian political theory denies intrusions of the government into the individual freedoms arising from the natural law. Totalitarian governments, on the other hand, seek to eliminate the private sphere of people through coercion, repression and complex and sophisticated surveillance measures that are justified as necessary for security of the state.

The United States defines itself as a land of freedom. The freedom rhetoric is easily traceable in speeches of the U.S. Presidents. The Declaration, the Constitution and the Bill of Rights are understood as symbols of what is best about the country. However, the terrorist attacks of 9/11 caused complex legislative changes in the name of security and the surveillance apparatus flourished. In 2007, the United States was even ranked as an endemic surveillance society.

The right to privacy belongs to the elemental personal freedoms of individuals and closely relates to the value of human dignity, as it creates a protected space from where intrusive acts of both other individuals and the government are excluded. Even though the right to privacy is not explicitly defined in the Constitution, legal tradition, based to a great extent also on the Supreme Court rulings, ranks it among the Constitutionally protected personal liberties, arising especially from the First and Fourth Amendment. Legal development of the right to privacy started in the 19th century, when

Louis D. Brandeis, later Justice on the Supreme Court, and Samuel D. Warren published a milestone article, defining the right to privacy as "a right to be left alone."

In the 20th century, the right to privacy developed and its boundaries in respect to the surveillance authority of the government were gradually shaping. In a number of rulings, the Supreme Court defined what is the protected private sphere of an individual and what is already a search under the Fourth Amendment warrant requirement. In the first relevant ruling, the *Olmstead v. United States* of 1928, the Supreme Court concluded that wiretapping a telephone conversation was not violating the Fourth Amendment and the right to privacy, as it did not intrude into one's premises. In this case the justices favored a literal interpretation of the Constitution, since the Founding Fathers could imagine only physical intrusions into one's correspondence or places. As the technology was evolving and new eavesdropping possibilities were emerging, the Supreme Court had to reflect these also in the interpretation of the Fourth Amendment searches and seizures. The *Olmstead* was overruled in *Katz v. United States* in 1967. The justices concluded that the Fourth Amendment protects people, not places, and therefore it covers also electronic communications. In addition, the constitutional scope of privacy protection was redefined. A person must have an expectation of privacy, and that expectation must the society accept as reasonable. Warrantless eavesdropping of electronic communications thus became violation of the right to privacy.

During *Katz* negotiations a question emerged, whether the search warrant requirement applies also to foreign intelligence surveillance. Subsequent legal tradition decided in favor of security exception, however, in the 1970s, the issue developed deeper. The so-called *Keith Case* and then also the *Zweibon v. Mitchell* decision stressed, that warrantless surveillance must not ever be used for domestic surveillance. In addition to the rulings, the Foreign Intelligence Surveillance Act was approved in 1978 as a reaction to the Cold War warrantless intelligence activities and political affairs of Nixon's presidency. FISA was therefore understood as a legislative response to the events, providing clear legal boundaries for surveillance of potentially dangerous foreign individuals and organizations suspected of acting on behalf of foreign powers. Moreover, FISA supported the system of checks and balances through the oversight of the surveillance programs and ensured separation of tools necessary for intelligence gathering from the ones of criminal investigation by law enforcement. More than two decades later, the terrorist attacks of 9/11 and the subsequent FISA amendments and the

USA Patriot Act breached the legal wall between warrantless authorities of the foreign intelligence surveillance apparatus and the domestic law enforcement.

The USA Patriot Act raises questions already from the moment of its approval within weeks after 9/11. The length, complexity, and confusing structure of amendments to previously enacted statutes raise legal uncertainty. The act also creates concerns whether the government still respects the right to privacy of U.S. citizens.

Section 218 of the Patriot Act illustrates very well, how the Act uses slight wording changes to circumvent the above-mentioned separation of intelligence gathering from criminal investigation and thus achieves far-reaching legal consequences for the right to privacy of people. A simple wording change of striking words “the purpose” and inserting “a significant purpose” from the original FISA results in violation of the Fourth Amendment warrant requirement. In practice, in cases when acquisition of the foreign intelligence information is not “the purpose” but only “a significant purpose” of a investigation, the domestic law enforcement personnel is able to obtain information without a warrant required by the Constitution and the original version of FISA.

The clash between privacy rights and the surveillance measures to protect the country from threats has been a hot topic in the U.S. society especially since the Snowden’s revelations in 2013. In June 2013, Edward Snowden together with journalist Glenn Greenwald reveled two secret eavesdropping programs conducted by the powerful National Security Agency pursuant to Section 216 of the USA Patriot Act and Section 702 of the FISA Amendments Act of 2008. Revelation of these secret programs provoked outrage in the U.S. public and also concerns about their constitutionality. As this thesis shows, not only constitutionality, but also compliance with the statues the programs arise from is questionable.

PRISM and upstream acquisition of Internet communications is not that highly criticized, as it is a valuable national security tool affecting the U.S. citizens in a lesser extent. The program collects contents of phone and electronic communications but is not allowed to target a U.S. person or a foreigner, who is located on the U.S. soil. The program cannot be applied even in cases when targeting of two non-U.S. persons located abroad would lead to collection of information about somebody protected by the Fourth Amendment. However, in this case most of the unintentional and inadvertent

collections happen, as due to errors and technological imperfections it is not possible to determine with certainty who is on the U.S. soil and who is not.

The bulk collection of telephony metadata program is more publicly known, as it targets all American citizens, whose metadata from phone calls are being stored. The term metadata refers not to the actual content of the conversation, but to the phone numbers and the date and duration of the call. However, the metadata proved to be revealing privacy of people, especially today, when everybody has a phone and the number works as an identifier. The bulk collection program is questionable on both the statutory and the constitutional level. It is questionable whether Section 215 constitutes a legal basis, as the data obtained in the bulk collection are not connected with a specific FBI investigation and all of them cannot be considered legally relevant. There is no statue that would require telecoms providers to collect complex sets of data on a daily basis. According to Section 215, the FBI entitled to collect information, not the NSA.

Constitutionally, there is the question whether the government has engaged in Fourth Amendment searches. This issue has been dealt in court cases that build on different assumptions. The *American Civil Liberties Union v. Clapper* is based on the *Smith v. Maryland* Supreme Court ruling of 1979, according to which dialing a phone number does not constitute an expectation of privacy and therefore is not protected by the Constitution. On the other hand, *Klayman v. Obama* concluded that the *Smith* case could not be applied, as it does not fit today's reality. Long-term collections create a wealth of detail, revealing one's privacy. The court ruled, that the bulk collection of metadata was an unreasonable search under Fourth Amendment. Proponents of the bulk collection program argue, that considering the program unstatutory is only one of possible interpretations of Section 215, given the fact that two Administrations and a number of experts considered it in good faith in compliance with Section 215.

Both NSA programs are supervised by the Foreign Intelligence Surveillance Court, which also oversees proper exploitation of the collected data. However, when it comes to the data exploitation, information mostly remains classified. It is known, that the collected metadata pursuant to Section 215 is stored for five years and can be examined only upon FISC order. The FISC is also subject of criticism as it approves vast majority of the surveillance requests and the opposing party is not present at the hearing. If the contents of communications acquired under Section 705 include information only about persons protected by the Fourth Amendment, the files must be

deleted. Nevertheless, if the communication involves also non-U.S. persons, it does not need to be destroyed.

It is obvious, that legality and constitutionality of the NSA surveillance programs, especially the bulk collection, is controversial. Does it mean that the United States really forgot how freedom is important for it? In times of crisis, the balance between personal liberties of people and national security is disrupted in favor of increased number of surveillance measures. This is not a new feature, there were eras in history – for example the so-called Red Scare or later the McCarthyism – when people whose loyalty was questioned faced higher level of surveillance, intimidation and detention. In this sense, the 9/11 attacks started a new wave of fear and the security surveillance apparatus flourished. What was in the first years after the attacks considered appropriate is now being more questioned if not denied as intrusive. This social phenomenon is called pendulum effect and states that the sense of threat naturally curtails personal liberties and weakens the civil rights protection. However, as soon as the danger passes, the scope of freedoms and liberties naturally recovers. The United States has not experienced any further terrorist attack comparable with the 9/11, therefore the pendulum swung back.

We can conclude – even though the process has not ended – that the United States is returning to freedom again. In a reaction to the post 9/11 legislative changes a number of civil rights organizations emerged which contributed significantly to general awareness of the problems and initiated lawsuits challenging the provisions, e.g. the *American Civil Liberties Union v. Clapper.* Also events from the recent months seem to support the optimistic view. The Obama Administration revealed some of the secret information about the eavesdropping programs and prompted negotiations of a new bill that would address the security needs without intruding privacy. This USA Freedom Act failed recently for number of reasons, but it managed to bring to the negotiation table both the surveillance apparatus and the civil rights and privacy advocates who will hopefully continue in their effort to find ways how to restore the balance between security and right to privacy.

Souhrn

Spojené státy americké jsou tradičně vnímány jako země svobody a jejich ústava garantující občanská práva se těší velké úctě obyvatel. V letech po 11. září 2001 však byly zařazeny mezi země s nejvyšší mírou sledování svých občanů.

Přestože americká Ústava právo na soukromí výslovně nezmiňuje, řadí se mezi ústavně garantovaná práva jak na základě ústavních dodatků – zejména prvního a čtvrtého – tak rozhodnutími Nejvyššího soudu USA. Americké právo pracuje s pojmem právo na soukromí od roku 1890. V průběhu 20. století vydal Nejvyšší soud USA řadu rozhodnutí, kde postupně definoval přesnější hranice mezi právem na soukromí a právem vlády na zajištění bezpečnosti země, které vyžaduje jistou míru zásahu do soukromí občanů. Rozbujelé výjimky z požadavku soudního povolení zásahu do soukromí ve jménu národní bezpečnosti v době studené války a politické aféry Nixonovy administrativy vyústily v roce 1978 k přijetí zákona o dohledu nad tajnými službami, který pro následující desetiletí stanovil jasná pravidla hry.

Teroristické útoky 11. září 2001 však šokovaly svět a vzbudily v USA pocit ohrožení, který vyústil k přijetí komplexního systému ústavně kontroverzní bezpečnostní legislativy. Jejím základem se stal Patriot Act, který funguje na systému dodatků k již platným zákonům, zejména stěžejního zákona o dohledu nad tajnými službami. V návaznosti na tyto právní události vznikla řada lidskoprávních organizací kritizujících pravděpodobné porušování Ústavy a práva na soukromí, které rovněž v tomto směru zahájily důležité právní spory.

Edward Snowden zveřejnil v roce 2013 dva tajné programy Národní bezpečnostní agentury sbírající data o všech telefonních hovorech a řadě elektronických komunikací na území USA. Otázka zákonnosti a ústavnosti žalovaných programů Národní bezpečnostní agentury ještě není rozhodnuta, protože rozsudky v posledních soudních sporech ještě nebyly vydány. Přestože poslední zákon navrhující zásadní revizi ve způsobu sběru potřebných dat byl odmítnut, lze pozorovat jednoznačný odklon od prosazování národní bezpečnosti na úkor občanských práv jak v dílčích soudních rozhodnutích, tak na úrovni Obamovy administrativy a i v Kongresu. Lze tedy dovozovat, že Spojené státy se opět vrací k důrazu na svobodu a právo na soukromí.

Bibliography

Primary Sources

- Bazan, Elisabeth B. "The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions." Congressional Research Service Report for Congress, Library of Congress, September 22, 2004 http://www.fas.org/irp/crs/RL30465.pdf [downloaded on January 2, 2015].
- Bazan, Elizabeth B. "The Foreign Intelligence Surveillance Act: An Overview of Selected Issues." Congressional Research Service Report for Congress, Library of Congress, July 7, 2008 https://www.fas.org/sgp/crs/intel/RL34279.pdf [downloaded on January 2, 2015].
- Bazan, Elizabeth B. "The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions." Congressional Research Service Report for Congress, Library of Congress, February 15, 2007 http://www.fas.org/sgp/crs/intel/RL30465.pdf [downloaded on January 2, 2015].
- "Bill of Rights of the United States of America," Bill of Rights Institute, http://billofrightsinstitute.org/founding-documents/bill-of-rights/ [downloaded on December 26, 2014].
- "Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act," Administration White Paper, August 9, 2013, page 3 http://www.documentcloud.org/documents/750210-administration-white-paper-section-215.html [downloaded on December 4, 2014].
- Foreign Intelligence Surveillance Act of 1978. http://www.law.cornell.edu/topn/foreign_intelligence_surveillance_act_of_1978 [downloaded on November 28, 2014].
- "Joint Statement from the Office of the Director of National Intelligence and the Office of the Attorney General on the Declassification of Renewal of Collection Under Section 501 of the Foreign Intelligence Surveillance Act," *Office of the Director of National Intelligence. IC on record,* December 4, 2014. http://icontherecord.tumblr.com [downloaded on December 4, 2014].

- Letter from Attorney General Eric Holder and Director of National Intelligence James Clapper to Chairman Patrick Leahy, concerning the USA Freedom Act. September 2, 2014. https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/2014-9-2-FISA-letter-from-AG-and-Clapper-to-Leahy-on-S.-2685-USA-Freedom....pdf [downloaded on November 30, 2014].
- Liu, Edward C. "Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments," Congressional Research Service Report for Congress, Library of Congress, April 1, 2014 https://www.fas.org/sgp/crs/intel/R43459.pdf [downloaded on January 1, 2015].
- Pew Research Center, "But More Approve than Disapprove. Few See Adequate Limits on NSA Surveillance Program." July 26, 2013, http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf [downloaded on December 12, 2014].
- "Presidential Policy Directive PPD-28. Signals Intelligence Activities," *The White House,* January 17, 2014. http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [downloaded on December 8, 2014].
- "Remarks by the President on National Security," *The White House,* May 21, 2009 http://www.whitehouse.gov/the-press-office/remarks-president-national-security-5-21-09 [downloaded on December 13, 2014].
- "Report on the Surveillance 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,* January 23, 2014 http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf [downloaded on November 22, 2014].
- "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," *Privacy and Civil Liberties Oversight Board,* July 2, 2014 http://www.pclob.gov/Library/702-Report-2.pdf [downloaded on November 26, 2014].
- Rollins, John W. and Liu, Edward C. "NSA Surveillance Leaks: Background and Issues for Congress," Congressional Research Service Report for Congress,

Library of Congress, September 4, 2013 http://www.fas.org/sgp/crs/intel/R43134.pdf [downloaded on January 1, 2015].

- "The 9/11 Commission Report," National Commission on Terrorist Attacks upon the United States, July 22, 2004 http://www.9-11commission.gov/report/911Report.pdf [downloaded on November 25, 2014].
- United States District Court for the District of Columbia, *Klayman v. Obama*, December 16, 2013. http://online.wsj.com/public/resources/documents/JudgeLeonNSAopinion12162013.pdf [downloaded on November 23, 2014].
- United States District Court Southern District of New York. *American Civil Liberties Union v. Clapper No. 13 Civ. 3994 (WHP) (S.D.N.Y. Dec 27, 2013)* https://casetext.com/case/aclu-v-clapper [downloaded on November 23, 2014].
- "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001." http://epic.org/privacy/terrorism/hr3162.html [downloaded on November 20, 2014].
- US Supreme Court. *Katz v. United States 389 U.S. 347 (1967).* https://supreme.justia.com/cases/federal/us/389/347/case.html [downloaded on October 31, 2014].
- US Supreme Court. *Olmstead v. United States 277 U.S. 438 (1928)* https://supreme.justia.com/cases/federal/us/277/438/case.html [downloaded on October 31, 2014].
- US Supreme Court. *United States v. Jones 565 U.S. (2012)* https://supreme.justia.com/cases/federal/us/565/10-1259/ [downloaded on November 23, 2014].

Secondary Sources

Books

- Cabada, Ladislav a Kubách, Michal. *Úvod do studia politické vědy* Praha: Vydavatelství a nakladatelství Aleš Čeněk, 2007.

- Greenwald, Gleen. *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Metropolitan Books. Henry Holt and Company, LLC, 2014.
- Janda, Kenneth. *Výzva demokracie. Sytém vlády v USA*. Praha: Slon, 1998.
- Rule, James B. *Privacy in peril: How are we sacrificing a Fundamental Right in Exchange for Security and Convenience*. New York: Oxford University Press, 2009.
- Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security.* New Haven: Yale University Press, 2011.

Journal Articles

- Atkinson, Rush. "The Fourth Amendment's National Security Exception: Its History and Limits," *Vanderbilt Law Review* Vol. 66, No. 5 (October 2013) http://www.heinonline.org.
- Brandeis, Louis D. and Warren, Samuel D. "The Right to Privacy," *Harvard Law Review* Vol. IV, No. 5 (December 1890): 193-220 http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf [downloaded on December 14, 2014].
- Bungard, Jessica M. "The Fine Line between Security and Liberty: The "Secret" Court Struggle to Determine the Path of Foreign Intelligence Surveillance in the Wake of September 11th," *University of Pittsburgh School of Law Journal of Technology Law and Policy* Vol. IV, Article 6 (Spring 2004) http://www.heinonline.org.
- Cole, David. "Where Liberty Lies: Civil Society and Individual Rights After 9/11," *Georgetown Public Law and Legal Theory Research Paper* No. 12-164, 2012 http://scholarship.law.georgetown.edu/facpub/1119/ [downloaded on November 26, 2014].
- Copeland, Rebecca A. "War on terrorism or war on constitutional right? Blurring the lines of intelligence gathering in post-September 11 America," *Texas Tech Law Review* Vol. 35, No. 1 (2004) http://www.heinonline.org.

- Doenges, William S. “Search and Seizure: The Physical Trespass Doctrine and the Adaption of the Fourth Amendment to Modern Technology,” *Tulsa Law Review* Vol. 2, Issue 2 (1965) http://www.heinonline.org.
- Gilbert, Francoise. “Demystifying the United States Patriot Act,” *Journal of Internet Law* 16, no. 8 (February 2013) http://www.ebsco.com.
- Glick, Scott J. “FISA’s Significant Purpose Requirement and the Government’s Ability to Protect National Security,” *Harvard National Security Journal*, Vol. 1 (May 30, 2010) http://www.jstor.org.
- Levy, Robert E. “The USA Patriot Act: We Deserve Better,“ Cato Institute. http://www.cato.org/publications/commentary/usa-patriot-act-we-deserve-better [downloaded on November 17, 2014].
- Murray, Nancy and Wunsch, Sarah. “Civil Liberties in Times of Crisis: Lessons from History,“ *Massachusetts Law Review* http://www.massbar.org/publications/massachusetts-law-review/2002/v87-n2/civil-liberties-in-times-of/ [downloaded on December 15, 2014].
- Sprague, Robert. “Orwell was an optimist. The evolution of privacy in the United States and its de-evolution for American employees,“ *The John Marshall Law Review* 83 (2008-2009) http://www.heinonline.org.
- Woldring, Henk E.S. “On the purpose of state: Continuity and Change in Political Theories,“ http://maritain.nd.edu/ama/Sweetman/Sweetman12.pdf [downloaded on November 2, 2014].

Newspaper Articles and Others

- Ackerman, Spencer. “FISA chief judge defends integrity of court over Verizon records collection,” *The Guardian,* June 6, 2013 http://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance [downloaded on December 4, 2014].
- American Civil Liberties Union, “Surveillance Under the USA Patriot Act.” https://www.aclu.org/national-security/surveillance-under-usa-patriot-act [downloaded on November 20, 2014].
- Congressman Jim Sensenbrenner, The USA Freedom Act http://sensenbrenner.house.gov/legislation/theusafreedomact.htm [downloaded on December 5, 2014].

- Denson, Bryan. “FISA: Understanding the Foreign Intelligence Surveillance Act (FAQ),” *The Oregonian,* November 26, 2013 http://www.oregonlive.com/news/index.ssf/2013/11/faq_what_is_fisa.html [downloaded on November 28, 2014].
- Farivar, Cyrus. “Patriot Act author says NSA’s bulk data collection is unbounded in its scope,” *Ars technica,* September 5, 2013. http://arstechnica.com/tech-policy/2013/09/patriot-act-author-says-nsas-bulk-data-collection-is-unbounded-in-its-scope/ [downloaded on December 3, 2014].
- Foreign Intelligence Surveillance Court. *AllGov. Everything Our Government Really Does.* http://www.allgov.com/departments/department-of-justice/foreign-intelligence-surveillance-court?agencyid=7206 [downloaded on November 28, 2014].
- George W. Bush’s address on September 11, 2001, *CNN,* September 11, 2001 http://edition.cnn.com/2001/US/09/11/bush.speech.text/ [downloaded on December 13, 2014].
- Gewitz, David. “For spy court judges, overseeing America’s surveillance efforts is a part-time job,” *ZD Net,* February 10, 2014 http://www.zdnet.com/article/for-spy-court-judges-overseeing-americas-surveillance-efforts-is-a-part-time-job/ [downloaded on December 5, 2014].
- Glen Greenwald, “The top secret rules that allow NSA to use US data without a warrant,” *The Guardian*, June 20, 2013. http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant [downloaded on December 8, 2014].
- Greenwald, Glen. “NSA collecting phone record of milions of Verizon customers daily,” *The Guardian,* June 6, 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [downloaded on November 23, 2014].
- Kayyali, Nadia. “In Klayman v. Obama, EFF Explains Why Metadata Matters and the Third-Party Doctrine Doesn’t,” *Electronic Frontier Foundation*, November 3, 2013. https://www.eff.org/deeplinks/2014/11/klayman-v-obama-eff-explains-why-metadata-matters-and-third-party-doctrine-doesnt [downloaded on November 26, 2014].

- Kelly, Erin. “NSA spying bill stalls in Senate vote,” *USA Today*, November 18, 2014. http://www.usatoday.com/story/news/politics/2014/11/18/leahy-usa-freedom-act-nsa-spying/19222895/ [downloaded on December 3, 2014].
- Libertarian Party of the United States. *How do Libertarians, Republicans, and Democrats differ?* http://www.lp.org/how-do-libertarians-republicans-and-democrats-differ [downloaded on October 27, 2014].
- Opsahl, Kurt and Reitman, Rainey. “A Floor, Not a Ceiling: Supporting he USA FREEDOM Act as a Step Towards Less Surveillance,” *Electronic Frontier Foundation*, November 14, 2013. https://www.eff.org/deeplinks/2013/11/floor-not-ceiling-supporting-usa-freedom-act-step-towards-less-surveillance [downloaded on December 4, 2014].
- Parker, Clifton B. “Stanford students show that phone record surveillance can yield vast amounts of information,” *Stanford News*, March 12, 2014. http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html [downloaded on November 24.2013].
- Rosen, Jeffrey and Rubenstein, David. “Constituing Liberty: from the Declaration to the Bill of Rights,” *National Constitution Center,* Exhibition Pamphlet, http://constitutioncenter.org/media/files/13_Exhibition_Pamphlet.pdf [downloaded on December 14, 2014].
- Safire, William. “Bush’s Freedom Speech,” *The New York Times,* January 21, 2005 http://www.nytimes.com/2005/01/21/opinion/21safire.html?_r=0 [downloaded on December 13, 2014].
- Shiffman, John and Cooke, Kristina. “The judges who preside over America’s secret court,” *Reuters*, June 21, 2013 http://www.reuters.com/article/2013/06/21/us-usa-security-fisa-judges-idUSBRE95K06H20130621 [downloaded on December 4, 2014].
- Tobin, Jeffrey. “Ashcroft’s Ascent. How far will the Attorney General go?“ *The New Yorker,* April 15, 2002. http://www.newyorker.com/magazine/2002/04/15/ashcrofts-ascent [downloaded on December 3, 2014].
- Ward, David. “Britain rated worst in Europe for protecting privacy,” *The Guardian,* December 31, 2007

http://www.theguardian.com/politics/2007/dec/31/uk.eu [downloaded on December 14, 2014].