IUS ET SOCIETAS 2014/2015

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

„Prohlašuji, že jsem esej na téma: Land of freedom or land of surveillance? Right to privacy in the U.S. after 9/11 zpracoval/a sama a uvedl/a jsem všechny použité prameny. Dávám souhlas s prvním zveřejněním své eseje vyhlašovateli soutěže nebo spolupracujícími institucemi v papírové či elektronické podobě.“

Praha 2015

1. 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 in three documents – the Declaration, the Constitution and the Bill of Rights – anchoring "the foundation

[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].

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]

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 clandestine 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]

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 bulk collection of telephony metadata conducted under Section 215 of the USA Patriot Act as revealed by Edward Snowden, stressing the contradiction between the proclaimed freedom and the factual complex surveillance mechanisms intruding privacy, whose legality and

[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].
[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].

constitutionality is being questioned. Has the United States shifted from the land of freedom into the land of surveillance?

2. What is the right to privacy

The right to privacy established 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.[8] 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.[9] "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."[10]

[8] 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.
[9] Louis D. Brandeis, Samuel D. Warren. "The Right to Privacy." *Harvard Law Review,* Vol. IV, No. 5 (December 1890): pp. 193–194.
[10] Ibidem, 193.

The authors experienced the very dynamic era of rapid development of new technologies and increasing influence of media, when privacy began to be threatened and defamation became a serious issue.[11] 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.[12] 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.

3. 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 value often called "common good", "good life" or "general interest".[13] These terms include numerous values and qualities people seek for satisfactory living.

The Founding Fathers of the United States were strongly influenced by John Locke's political theory, as Thomas Jefferson expressed in the Declaration of independence – life, liberty and pursuit of happiness are there described as unalienable. According to the liberal theory still resonating in the American society, a

[11] Sprague, "Orwell was an optimist," 98.
[12] Ibidem, 102.
[13] 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].

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 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 a 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 pushing the state to adapt their version of the border.

4. 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, 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-state 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 analyzing physical features of a human in a second and connecting 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 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 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.[14]

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.[15]

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.[16]

Proponents of the surveillance measures often use the nothing to hide argument, an assumption that people who did not anything wrong do not need to be afraid of the fact that government possesses their personal information. This argument

[14] 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].
[15] Ibidem.
[16] 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.

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 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 including 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.[17] 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 information as a result of technological development is easy and cheap, the less data that can be potentially misused the better.

5. Constitutional background

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."[18]

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

[17] Rule, *Privacy in peril*, 42.
[18] „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].

naturally suppress these knowing that government can draw consequences.[19] In addition to this, the Fourth Amendment is worded as follows:

> "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."[20]

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 probable cause is understood as reasonably trustworthy information that the search will turn up needed evidence of a conducted wrongdoing.[21]

The Fourth Amendment does not apply always, just in cases when an individual can reasonably expect privacy. Therefore a vast number of situations are not covered, for example police can collect evidence on suspect's plots, where only the immediate surroundings of a house are 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.[22]

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.[23] Briefly, the Supreme Court has to determine how the Fourth Amendment applies in cases that

[19] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven: Yale University Press, 2011), pp. 147-148.
[20] "Bill of Rights of the United States of America."
[21] Solove, *Nothing to Hide*, 95.
[22] Ibidem, 99-100.
[23] Ibidem, 95.

were not expected by the Founding Fathers. This development is still ongoing and depends on the available surveillance technology.[24]

6. Foreign Intelligence Surveillance Act and the USA Patriot Act

In June 2013, Edward Snowden, an employee of the National Security Agency, revealed the bulk collection of telephony metadata stored by the NSA, prompting public discussions about privacy issues in relation to national security. Even though the program declares to arise from the valid law, its existence and control by the National Security Agency was unknown. 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.[25] In order to explain the context and major statutory and constitutional concerns arising from the revelation, 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 programs revealed by Snowden.

FISA was approved in 1978 in the context of the Cold War and political affairs of Nixon's presidency, especially Watergate. 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.[26] Intelligence agencies became more powerful and were able to eavesdrop even on people who were not agents of foreign powers.[27].

Consequently, FISA was a legal response to these events, banning any further warrantless eavesdropping on people, but allowing some legal space for authorities to

[24] Solove, *Nothing to Hide*, 95.
[25] Solove, *Nothing to Hide,* 81.
[26] 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].
[27] Ibidem.

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. The law was adopted to ensure separation of intelligence gathering important for national security from that of criminal investigation by law enforcement.[28] 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 and especially terrorist attacks of 9/11 changed rules. The Patriot Act, together with further FISA and Patriot Act amendments, breached the legal safeguards separating these two processes.

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.[29] Records from the negotiations are poor, which complicates any effort to get an idea of the legislative intent of the Congressmen.[30] 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

[28] Murray, Wunsch, „Civil Liberties in Times of Crisis."
[29] 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].
[30] Ibidem.

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.

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.[31]

7. 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 that FBI was granted 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, Verizon was also expressly forbidden to disclose information to the public.[32] This 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.[33]

What the *Guardian* publicly disclosed was in reality a three-month extension of a program that had been ongoing for seven years.[34] 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 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 of call information is not the only mean of implementing the Section. It

[31] 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].
[32] 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].
[33] Ibidem.
[34] Rollins, Liu. "NSA Surveillance Leaks,"1.

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.[35]

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.[36]

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 this calling is not included, except the area code identified in the phone number.[37] 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.[38]

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 advocates challenge the telephony metadata program regarding potential Fourth Amendment as well as First Amendment violations. There were two crucial

[35] Ibidem, 4.
[36] Liu. "Overview of Constitutional Challenges," 2.
[37] Rollins, Liu. "NSA Surveillance Leaks," 2.
[38] Ibidem.

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.[39] 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 requiring 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.[40] 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 Foreign Intelligence Surveillance Court (FISC) to share the data with FBI except in situations explicitly mentioned in the FISC orders.[41]

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 unstatutory is only one of possible interpretations.[42] It is crucial to take into account that two Administrations and a number of experts and

[39] "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].
[40] "Report on the Telephone Records Program," 10.
[41] Ibidem, 88-89.
[42] Ms. Brand and Ms. Collins are lawyers, members of the Privacy and Civil Liberties Oversight Board who also served in various top governmental positions.

officials considered the program in good faith to be in compliance with Section 215. Similarly, the program itself also works in good faith.[43] 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.[44]

From the perspective of the U.S. Constitution, there are 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 search, which occurs when a subjective expectation of privacy recognized by the society as reasonable is violated by the government.[45] 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.[46] 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.[47] 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."[48] FISC argued that issuing the order for collection of telephony metadata under Section 215 is

[43] 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.
[44] "Report on the Telephone Records Program," 210, 215.
[45] Liu. "Overview of Constitutional Challenges," 6.
[46] Liu. "Overview of Constitutional Challenges," 6.
[47] 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].
[48] Liu. "Overview of Constitutional Challenges," 7.

constitutional, as the Fourth Amendment "imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent"[49] – 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.[50]

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.[51] 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.[52]

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.[53]

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

---

[49] Ibidem.
[50] 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].
[51] 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].
[52] *Klayman v. Obama*.
[53] 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].

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 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.[54] 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.[55]

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.[56]

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 –

[54] Liu. "Overview of Constitutional Challenges," 8.
[55] *Klayman v. Obama*.
[56] Report on the Telephone Records Program, 132-135.

families or companies.[57] The third party doctrine is another aspect, whose suitability for the purposes of bulk metadata collection seems questionable. The argument, that people 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.[58]

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.[59] 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.

8. 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 debate 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

[57] 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].
[58] Ibidem.
[59] Report on the Telephone Records Program, 215.

security interests. Today, Republicans condemn every new eavesdropping disclosure and Democrats advocate for the Obama administration's policies.[60]

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.[61]

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 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.[62] Laws in such situation are not silent, but "speak with somewhat different voice."[63] This opinion shared another Supreme Court Justice, Robert H. Jackson, who expressed this in 1949: "The Constitution is not a suicidal pact."[64] 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."[65]

---

[60] 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.
[61] 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].
[62] Solove, *Nothing to Hide*, 55.
[63] Ibidem.
[64] Ibidem.
[65] Ibidem, 61.

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.[66]

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.[67] 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.

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.[68] In contrast, thirteen years earlier the Attorney General openly labeled critics of the Patriot Act and government policies unpatriotic.[69] 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

[66] 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].
[67] Ibidem, 1205-1206, 1250.
[68] 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].
[69] 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].

the House of Representatives, testifies to the opinion shift even among legislators who originally proposed the antiterrorist surveillance measures.[70]

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.[71] 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."[72] 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."[73]

After the last year's election, the new Congress took control over this issue. The problems remain 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.[74]

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.[75] President Obama issued a directive stating that: "All persons should be treated with dignity and respect,

[70] 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].
[71] 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].
[72] 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.
[73] Kelly, "NSA spying stalls in Senate vote."
[74] 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].
[75] "Report on the Surveillance Program Pursuant to Section 702," 100.

regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in handling of their personal information."[76]

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.

9. 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.

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

[76] "Presidential Policy Directive PPD-28."

constitutionally protected personal liberties, arising especially from the First and Fourth Amendment.

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 published a secret eavesdropping program conducted by the powerful National Security Agency pursuant to Section 215 of the USA Patriot Act. Revelation of this secret program provoked outrage in the U.S. public and also concerns about its constitutionality. As this thesis shows, not only constitutionality, but also compliance with the statues the program arises from is questionable.

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.

It is obvious, that legality and constitutionality of the NSA 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.