Odsjek za anglistiku

Filozofski fakultet

Sveučilište u Zagrebu

DIPLOMSKI RAD

State of emergency: privacy, security and surveillance in modern-day U.S.A.

Kandidat: Arsen Brizić

Mentor: Izv. prof. dr. sc. Jelena Šesnić

Ak. godina: 2016./2017.

Contents:

1. Introduction

My thesis deals with a topic that is a subject of numerous debates and discussions in the American political and social discourse: the surveillance of U.S. security agencies and its effect on privacy. In recent years, this topic has been at the center of the world's attention after the shocking revelations made by the whistleblower Edward Snowden in 2013, when the world realized that the U.S. national security agencies had indiscriminately been gathering enormous amounts of data. Judging by the amount of data gathered in these surveillance programs, this represents the peak of U.S. surveillance, while Snowden himself described the situation as "a system of secret, pervasive surveillance from which there is no escape" (Greenwald 23). This master's thesis will explore the development of surveillance throughout U.S. history in order to explain how we as a society came to the point where people around the globe have to accept the fact that surveillance is omnipresent and that almost anyone can be traced at any time, while the agencies and government officials who authorize this unconstitutionally are not held accountable for these violations. This thesis will also argue that every time the scope of surveillance was increased, which happened several times in U.S. history, it represented an intrusion on privacy and often unjustifiably targeted specific ethnic or political groups. As this thesis will further argue, all of this was done in the name of protection of U.S. citizens and represented as right and reasonable to maintain national security at high levels, when in fact the threat of danger was greatly exaggerated and used as an excuse for deploying the surveillance system for economic or political purposes.

In this thesis I track the development of U.S. surveillance from the period of WWI and the surveillance of African Americans. The main argument here is that U.S. security agencies targeted African Americans because they represented a voice of dissent and opposed the participation of the United States in the war. This case proves to be very important

because it is one of the first surveillance operations with a recognizable pattern: the unconstitutional targeting of a political or ethnic group that is not a real threat to the country.

The next period considered here, the Cold War era, proved to be significant because it represents a time when the government spied on political enemies and a huge number of civil rights groups. As will be shown, this was again done for no justifiable reason because the targeted groups were neither a threat nor danger to the national security of the U.S.A. After showing that FBI surveillance in the Cold War period could even be considered illegal, the thesis briefly focuses on Nixon's Watergate scandal and the reasons of public outrage that it caused.

The consequences of the Watergate scandal and the FBI surveillance during that period led to the need for more control and transparency of surveillance programs, which resulted in the creation of FISA (Foreign Intelligence Surveillance Act), which is discussed in the next chapter. The main focus here will be on the changes that this act brought regarding transparency and control of surveillance, as well as its efficiency and high approval rate.

The discussion next turns to the post 9/11 period, as it is argued that this event created a shift, a new era in the surveillance of U.S. security agencies. This chapter is centered on the idea that FISA courts, which were supposed to limit the scope of surveillance, proved to be inefficient in the post-9/11 period after the introduction of the USA PATRIOT Act. The use of NSLs and FISA Amendments Act and their impact on civil rights will be discussed here as another form of broadening the scope of surveillance and defying the Constitution and laws. Related to these developments in the legal domain, public video surveillance in the U.S. is also discussed here to show that it is a largely unregulated area with possibilities of eroding privacy rights and gathering large amounts of sensitive information.

The last period discussed in this work is the most recent one: surveillance programs revealed by the whistleblower Edward Snowden in 2013. What every chapter of this thesis

shows is that the surveillance increased in the course of the twentieth century, finally resulting in a massive global web of surveillance in the twenty-first century. As this chapter will show, surveillance programs such as PRISM and Boundless Informant were designed to gather enormous amounts of data on U.S. and foreign citizens, and this was done quite indiscriminately and unconstitutionally. At this stage the surveillance is no longer domestic (i.e. no longer confined to the U.S.A.), but as the documents revealed by Snowden show, everyone in the world could be targeted at any time. The aftermath of these revelations and the consequences for the Obama administration will also be a subject of presentation in this chapter.

The next chapter explores the reasons that were used to justify the surveillance strategies and programs discussed in this thesis. In this section I argue that using the fear of terrorism or foreign enemy is a method that was always used to justify the broadening of surveillance while neglecting the citizens' rights, when in fact the real purpose of the latest surveillance programs turned out to be diplomatic and economic espionage, rather than terrorism.

After going through all the major surveillance programs carried out by U.S. security agencies and the reasons behind them, in conclusion the focus will be on "the way forward." Here ideas and opinions will be presented on ways to achieve balance between surveillance and security and steps to minimize abuses of government surveillance in the future. First a critique of three views that support greater surveillance will be given, after which I will focus on concrete proposals for achieving balance.

2. The beginnings of surveillance: WWI and the surveillance of African Americans

"The struggle between the needs of national security and political or civil liberties has been a continual one" ("Developments in the Law" 1133). This introductory remark from the Harvard Law Review Association's review of the history of conflict between national security and civil liberties is a good starting point for the argument and could even serve as a general idea of my thesis. Indeed, it seems that the need of the United States government to monitor specific groups of people within the country appears as early as 1798 with the Alien and Sedition Laws, which were designed to silence critics of the Adams administration ("Developments in the Law" 1133). However, the first instance of a surveillance program on a larger scale appeared with the Espionage Act of 1917. This was the time of World War I and what caused the enactment of the law was the fear of German subversion, even though the ethnic groups that were targeted in the end were not only Germans. As Henderson writes, the surveillance was not aimed at German spies, but rather political protesters, "while legions of informers, private investigators and federal agents combined to root out subversive elements" (186).

Mark Ellis's study shows that African Americans were the group that was specifically targeted. In his book entitled *Race, War and Surveillance: African Americans and the United States Government during World War I*, he did a thorough examination of this case and found numerous reports of surveillance of African Americans who fought for civil rights and represented a voice of dissent. Ellis writes that the surveillance took off after the national press started creating panic by claiming that "German agents were spreading anti-war propaganda among blacks, especially in the South" (xvi). These allegations were taken seriously so that the Wilson administration "closely monitored" the activities of the black activists and civil rights supporters during WWI (Johnson 28). The important fact regarding this case is that there were no signs of criminal activity, before or during the surveillance,

meaning there was no valid reason to conduct surveillance on this specific ethnic group. As several examples in this thesis will later show, the surveillance of specific groups within the American society that represented no real threat to the national security was a repeated practice of U.S. security agencies.

Ellis writes that in 1917 allegations of German subversion increased fourfold, which prompted the Attorney General to allow BI (Bureau of Investigation – predecessor to the FBI) agents a completely free hand in the investigation without congressional authorization (xvii). Conolly-Smith claims that during World War I the BI conducted "U.S. history's largest ever effort to clamp down on dissent, silence protest, and incarcerate radicals", with methods that included "wire-tapping, the use of informants, and the monitoring of mail" (7). Although it is debatable if this was “the largest ever” effort to silence dissent, the fact remains this was a massive scheme with several agencies involved and mostly illegal methods of surveillance.

As stated earlier, Congress did not have real oversight of the methods and actions that were taken in order to evaluate if they were justifiable, which led to the shameful case of the APL. The American Protective League (APL) was an organization consisting mostly of volunteers that assisted the BI in the investigation, but by the end of the war the APL turned out to be an embarrassment to the Department of Justice (Ellis xvii). They were prone to "overzealous 100% Americanism" and did not respect civil liberties of aliens or union members (Ellis xvii), while Henderson writes that "After each volunteer was given a badge similar to a police shield, the APL conducted a zealous campaign against numerous forms of perceived disloyalty" (186).

The Military Intelligence Branch (MIB) was another government agency responsible for the surveillance of African Americans. Johnson states that "racial and ethnic minorities were suspected of particular susceptibility to German and later Bolshevik agents of influence", with African Americans under special scrutiny in this regard (28). Van Deman,

the man in charge of the MIB, was convinced that United States was facing threats from the inside, while ethnic groups that opposed U.S. involvement in the war were deemed dangerous (Ellis xix).

Believing that black disloyalty presented a threat to the United States, he conducted a vigorous surveillance campaign of prominent African American civil-rights activists. What started as an investigation of German subversion among the black community quickly turned into a huge surveillance system aimed at a specific ethnic group, completely diverting from the original intention. To begin with, the surveillance of African American leadership in 1918 included tracking and excluding from circulation printed African American journals and publications, as well as any publications that criticized the American involvement in the war or the government's decisions (Conolly-Smith 10). For no justifiable reason, the letters of black Americans which contained comments on race relations were also frequently intercepted (Ellis 104), and this collaboration between the BI and the Post Office Department represents the first domestic surveillance program in the United States (Conolly-Smith 7). Several individuals fighting for the rights of the African American community were kept under constant surveillance, such as Chandler Owen, editor of the magazine *Messenger* (Ellis 111), and the African American sociologist Kelly Miller (Ellis 126). In 1918, the MIB even monitored the National Liberty Congress, whose focus was civil rights issues, acquiring the list of names of all the delegates and then labelling them "Loyal" or "Questionable" (Ellis 122).

All these actions were part of one of the first major surveillance programs conducted in the United States, involving tracking and censoring publications and letters, and keeping constant watch on certain prominent individuals in the black community. One thing stands out: this surveillance system was aimed at a specific ethnic community that was believed to represent an internal threat to the United States simply by criticizing the decisions of the

administration. More importantly, the accusations that black activists were influenced by German agents were completely false, since there are many reports that prove there was no evidence of German propaganda in the African American community (Ellis 122, 123, 135). At the end of his article on the domestic surveillance during WWI, Conolly-Smith states that those tracing the origins of the FBI will find that violation of civil rights and constitutional freedom is one of the agency's most enduring historical legacies (21). As further examples will show, this statement is not only true for the period of WWI but appears as a recurring practice throughout the agency's history.

3. FBI surveillance during the Cold War

As this chapter will show, after the end of World War II the U.S. security agencies again used the tactic of stoking fear of an outside enemy to conduct surveillance of internal political opponents and those that represented a voice of dissent. In this case, the FBI under Director J. Edgar Hoover during the Cold War had a massive web of surveillance, keeping constant watch over civil rights movements, political activists, anti-war protesters, socialist organizations… It seems that almost any sign of opposing or criticizing the current political status was seen as potentially dangerous.

Athan G. Theoharis did a thorough research of federal surveillance during the Cold War, focusing on the FBI in his work *FBI Surveillance during the Cold War Years: A Constitutional Crisis*. His opening claim warns that "the FBI investigated the dissident political activities of American citizens during the Cold War years, and in the process violated federal laws and constitutional guarantees" (Theoharis 4). Disrespect for human rights and the Constitution in these investigations became a practice very early on, after Hoover announced in the mid-1950s that the FBI does not need authorization to install surveillance devices on private property (Henderson 187), despite the fact that such practice is unconstitutional. Theoharis goes even further by claiming that the FBI deliberately misinformed presidents and attorney generals to get authorization on investigative techniques that were clearly illegal, even introducing separate filing and record destruction procedures in order to avoid discovery of these investigations (5). This level of dedication to avoid supervision and public awareness of these programs is a clear indicator that these programs were not legal and would cause public outrage. However, the fact remains that the FBI managed to avoid oversight for a long time, which allowed Hoover to introduce one of the most embarrassing cases in the FBI history: COINTELPRO.

COINTELPRO is a common name for several surveillance programs focusing on civil rights movements that started in 1956 and ended in 1971 after a public disclosure of the documents regarding the program. It was not only the illegal procedures, but also the choice of targets that contributed to the bad name of the program. The choice of targets for surveillance that Greenwald lists is a curious mix: "National Association for the Advancement of Colored People, black nationalist movements, socialist and Communist organizations, antiwar protestors, and various right-wing groups" (184). Greenwald explains that to the FBI “doing something wrong” extended to "meaningful dissent and any genuine challenge" to the government (183), while the Church Committee report, which is discussed later, showed that the groups that were under surveillance represented no threat to the country. Theoharis deals with this topic even further, claiming that the behavior of the FBI during this period represents "a breakdown of the American constitutional system of checks and balances and lawfully defined authority" (12). The factor that brought about what Theoharis claims was a constitutional problem was ineffectual oversight. Presidents and attorney generals were never asked to authorize COINTELPRO programs nor informed about them (Theoharis 12), while the previously mentioned record destruction procedures that were used to avoid detection and destroy evidence on these programs only support Theoharis’s claim.

The Watergate scandal in the 1970s showed that the surveillance programs were even larger and used more extensively, which deepened the constitutional crisis and created more problems for the executive office. The journalists that reported on the Watergate scandal discovered that the Nixon administration was directly responsible for wiretapping telephones of government officials and reporters to investigate news leaks and listen in on the conversations of political opponents (Henderson 188). Theoharis also claims that the FBI used wiretaps to gather "derogatory personal and political intelligence information" (6), while

it was proven that some members of Congress were also under surveillance (Shamsi and Abdo 7). All these revelations naturally caused public outrage, and Henderson even claims that the Watergate scandal "caused many people to question the authority claimed by the executive branch" (189).

The abuse of power that was discovered in COINTELPRO programs and the Watergate scandal simply couldn't go unnoticed, so in 1975 the Senate Church Committee was founded to investigate the disclosures about the programs. In 1976, five years after the evidence about the COINTELPRO program came out, the Church Committee concluded that the program was "aimed squarely at preventing the exercise of First Amendment rights of speech and association", adding that "Many of the techniques used would be intolerable in a democratic society even if all the targets had been involved in violent activity, but COINTELPRO was far beyond that" (qtd. in Greenwald 184). Cinquegrana's summary of the report also mentions constitutional abuse and illegal procedures:

> The inquiries of the "Church Committee" into the activities of the intelligence agencies of the United States had uncovered far-ranging infringements upon individual privacy interests through the unfettered use of electronic surveillance and other intelligence collection techniques. Of particular concern were instances where warrantless electronic surveillance had been used against United States citizens who were not readily identifiable as reasonable sources of foreign intelligence information, who appeared to pose little threat to the national security, and who were not alleged to be involved in any criminal activity. (806)

Basically, the Church Committee recognized all that was wrong with COINTELPRO: using illegal surveillance procedures with complete disregard to constitutional rights and targeting groups that did not represent any real threat to the national security of the United States. The Church Committee's conclusion indicates that the main reason those groups were under

surveillance was that they did not share the same political view as the established authority (Donohue 1092), and the fact that almost all the groups were non-violent only proves that there was no justifiable cause to put them under surveillance. For both COINTELPRO and Watergate the executive office used the ability of gaining information through surveillance to gain control over civil rights groups and to maintain political power, completely disregarding people's rights to privacy, free speech and free association.

4. Foreign Intelligence Surveillance Act (FISA)

The Church Committee report did not only include results of the investigation, but also recommendations on how to change the current situation in which the abuse of surveillance by the executive branch became a major problem. The report persuaded many there was need for regulation, and one specific recommendation in the report even urged Congress to adopt a framework that would disable the executive office to be the only one responsible for decisions regarding national surveillance (Cinquegrana 808). Congress responded by adopting the Foreign Intelligence Surveillance Act (FISA) in 1978, which although amended several times, is still in effect today. Henderson writes that with FISA Congress wanted to react to the abuses of surveillance, but at the same time keep national security at high levels: "For these reasons, Congress chose to limit, as opposed to completely eliminate, the ability of the executive branch to conduct electronic surveillance for national security purposes" (190).

FISA was a compromise that was supposed to provide more supervision and limit the President's power: it requires federal officers to submit applications for domestic electronic surveillance to the newly founded FISA courts for reviewing, which are then approved by the Attorney General. As Eggert puts it, "Indeed, the FISA imposes an *obligation* on the executive *to obtain a warrant* before conducting electronic surveillance to acquire foreign intelligence" (617), so in theory FISA should provide more oversight, because by requiring a warrant it limits the absolute power over surveillance that the president had before.

It comes as no surprise that such an important act provoked many contrary views, mostly regarding the high approval rate of submitted applications. Donohue, for example, questions if the FISA court serves merely as a rubber stamp by providing automatic approvals and failing to carefully review applications, stating that "Between 1979 and 2003, FISC only denied three out of 16,450 applications submitted by the executive branch" (1097).

Cinquegrana provides two counter-arguments to such high approval rates: proponents of FISA claim that such high acceptance happens because all applications are carefully prepared and reviewed, while its opponents argue the figures indicate that the FISA court encourages executive officials to conduct activities that would have never been proposed earlier (815). The fact still remains that almost all applications for surveillance are accepted, which could indicate that FISA only appears to provide oversight while it actually approves more applications than before. The question then is, what is actually the point of FISA if almost all applications are approved? Kenney argues that, since most wiretap applications are approved anyway, FISA is a bureaucratic obstacle, adding that "large numbers of requests have created logjams in the approval process that can potentially hinder counterterrorism investigations" (qtd. in Reedy and Miller 128). Kenney however ignores the fact that although it is a complicated process, it was designed to prevent the serious problem of surveillance abuse, so a problem in bureaucracy seems like a small downside for a much higher cause. Greenwald also points out the ineffectiveness of the FISA court, arguing it is a "cosmetic measure, providing just the appearance of reform", calling it "part of the executive branch rather an independent judiciary exercising real oversight" (128).

All of these arguments show that there are many aspects to FISA, a complex but important act. In theory, FISA serves to prevent the abuse of surveillance by the executive branch, but the large approval rate indicates that the FISA court is not a body that would prevent surveillance from becoming widespread, but rather only looks at the applications and approves almost all of them. At the time FISA was created, it was a reaction to public outrage and a message that a change was occurring. It was supposed to provide assurance that illegal and unwarranted surveillance would not be tolerated, but as will be shown in the next chapter, the scope of such surveillance only increased.

5. Legislative changes after 9/11

When it comes to surveillance, 9/11 is definitely an event that had a high impact on privacy and national security, changing the way both are regarded. In other words, the terrorist attacks that happened on September 11, 2001 created a shift which started a new era in surveillance: former laws were changed, new legislation was introduced and legal boundaries were stretched; and all of this as a result of 9/11.

Reedy and Miller make an interesting claim in their essay: "Similar to the post-9/11 reaction, most security strategies were shaped by events such as the movement for American Independence and the Second World War" (119). The first sentence of President Bush's letter introducing the 2006 National Security Strategy confirms their theory: "'America is at war. This is a wartime security strategy'" (qtd. in Doyle 627). Former President Bush, Doyle, Reedy and Miller, all see 9/11 as an important event similar to war emergency, a turning point that marked "the beginning of the modern era of homeland security" (Reedy and Miller 119), setting in motion changes that are still in effect today.

First of all, the change in homeland security structure after 9/11 can be seen in two things: the reorganization and collaboration of security agencies. Before 9/11 President Clinton preferred using domestic law enforcement agencies to fight terrorism instead of international security agencies such as CIA, while President Bush "failed to act aggressively against terrorism" (Reedy and Miller 124) when he took office. After 9/11 a swift reaction was needed, so security agencies started to cooperate on a much higher level, "while avoiding the establishment of a centralized body" (Reedy and Miller 125). However, the collaboration between the agencies after 9/11 also marked the start of massive surveillance programs in the United States.

Kent writes that "a military or other catastrophe, such as 9/11, can temporarily lead political actors, including the courts, to adopt and countenance fewer individual rights

protections than they ordinarily would" (1081). When talking about the executive branch after 9/11, Sunstein makes a similar claim: "In ‘perilous times,’ it might be thought, those branches are especially prone to a serious form of lawlessness, perhaps because of a kind of public panic, and it becomes all the more important for courts to insist on compliance with the rule of law" (270). This theory about 9/11 as a national crisis or a war emergency turned out to be true in the years after the terrorist attack, as there are many cases that prove surveillance started to increase rapidly in this period, along with legal questions regarding it. Sunstein did a thorough research of this topic and lists a series of post-9/11 legal questions and cases in which individual rights were jeopardized, including unwarranted searches to obtain private information or the executive branch engaging in illegal wiretapping (269). As both Kent and Sunstein notice, 9/11 marked the beginning of a new era similar to war periods, as it turned out that privacy and civil rights were jeopardized and laws were amended or bypassed in order to conduct various forms of surveillance. In their text "Privacy and Surveillance Post-9/11", Shamsi and Abdo show that United States government after 9/11 created "a society in which the long-standing ‘wall’ between surveillance for law enforcement purposes and for intelligence gathering has been dismantled," while laws did not keep up with the developments to provide oversight (5). These turned out to be perfect conditions for surveillance programs:

> As a result, the most sweeping and technologically advanced surveillance programs ever instituted in this country have operated not within the rule of law, subject to judicial review and political accountability, but outside of it, subject only to voluntary limitations and political expedience. (Shamsi and Abdo 5)

One of the first steps to start conducting wider surveillance was the introduction of the U.S.A. PATRIOT Act in October 2001. This act broadened the power of the executive and removed some of the limitations in the previously discussed FISA Act, whose purpose was to prevent

the abuse of surveillance. Under FISA, the government could conduct surveillance of agents of foreign power if the primary purpose was intelligence gathering (Shamsi and Abdo 7). This changed with the introduction of the USA PATRIOT Act, which significantly weakened this limitation of FISA. Now the government could conduct surveillance domestically if it is shown that its “significant purpose” is gathering foreign intelligence, meaning that laws regarding foreign intelligence, with reduced constitutional protection applied to them, could now be used on U.S. citizens (Shamsi and Abdo 7). Henderson concludes that when it comes to privacy concerns, "the modifications in their entirety do pose a threat" (180). One of the main problems with the new act was that the lowering of the standard to obtain a FISA order represents a huge expansion of the executive authority, and the public concern at the time of the enactment was that it would be used with insufficient discretion (Henderson 195).

Another development that caused concern was that the USA PATRIOT Act allowed a broader reach of roving surveillance. Roving surveillance is a type of wiretap that follows all of the surveillance target’s devices without the need for warrants for every single device. Under the new provision, the government could engage in this type of surveillance without proving that the target uses the targeted device, which caused criticism because of the invasion of privacy and fear that innocent conversations of U.S. citizens could be intercepted (Henderson 197). Donohue shares Henderson’s opinion that the USA PATRIOT Act "*did* have an immediate and far-reaching impact on civil liberties" (1102), adding that Congress added sunset provisions (meaning they last to a particular date) on the most intrusive powers to make the act more acceptable (1102), but these provisions were renewed after expiration in 2005, with some provisions even becoming permanent.

The USA PATRIOT Act was not the only change in the U.S. law after 9/11 regarding surveillance. Another example is the FISA Amendments Act that was enacted to legalize the warrantless domestic wiretapping program introduced shortly after 9/11 by President Bush. In

this program, President Bush authorized the National Security Agency (NSA) "to eavesdrop on telephone calls and emails made by U.S. citizens and others inside the United States without seeking warrants from the courts" (Lyons et al 812), which was later found in breach of U.S. laws and the Constitution (Lyons et al 813). Greenwald writes that *The New York Times* had information about that program in 2004, but waited for more than a year to publish it, thus allowing George W. Bush to be re-elected (55). If this indeed had led to President Bush's being re-elected, then Snowden might be right in claiming that *The New York Times'* procrastination "changed history" (Greenwald 56). This case shows that surveillance was and still is a huge topic of debate that could easily affect the executive branch, as in the Watergate case.

The FISA Amendments Act represents "the most sweeping surveillance authority" (Shamsi and Abdo 8) and a major threat to the privacy of U.S. citizens. This act expands the scope of government surveillance because it allows gathering of information on non-U.S. citizens without individual warrants, even if they are communicating with a U.S. citizen (Greenwald 74). To put it differently, under that provision the government can gather information on U.S. citizens without individual warrants. Shamsi and Abdo point out that judicial oversight of surveillance done under this act is minimal (8). In short, civil liberties of U.S. citizens are hereby infringed upon because all of their communication with foreign citizens can be accessed without any limitations, if considered vital information for national security.

Significant changes on FISA were also made in the implementation of national security letters (NSLs), which Shamsi and Abdo describe as "perhaps the most permissive of the government's domestic national-security surveillance tools" (8). NSLs are written orders by the FBI that require electronic communication providers to provide to the Bureau confidential customer information, such as subscriber information and an e-mail address.

Donohue writes that the introduction of the USA PATRIOT Act expanded the type of information that could be obtained in this way to include credit card records and information on internet use, as well as increasing the number of officials that could request the information (1108). A company served with an NSL also gets a gag order, meaning it cannot reveal to anyone that it has received the order. There is also no judicial review nor government oversight of the collection of information via NSLs (Donohue 1112). Donohue is right when showing concern about the lack of control over who has access to the information, how long it is kept, and the way it is used (1111), because when all is considered, NSLs seem like a dangerous broadening of surveillance power. Shamsi and Abdo write that reports from the Department of Justice show rapid increase in the use of NSLs and "disturbingly frequent violation of even the minimal limits" (8). These violations include under-reported use of NSLs, repeatedly ignoring NSL statutes, unlawful requests that relied on false claims, and finally, the fact that 22 % of audited files contained legal violations (Shamsi and Abdo 8). This summary of the reports shows that NSLs were often misused, especially after major changes were made to increase their use in government surveillance.

One domain of government surveillance that remains highly unregulated and needs to be examined closely is video surveillance of public places. Brown writes that the development of video cameras, such as tracking systems and facial recognition, "could erode privacy rights and substantially change the character of public places" and argues that the police use of public video systems demands more regulation (755). The main problem of public video systems is that regulation did not keep pace with technology: while the number and quality of public video cameras across the United States increased rapidly (Brown 759), there is no legislation governing the use of this system (Brown 760). An individual can expect to be monitored at any time in public spaces like sidewalks or parks; or as the Chicago mayor said about his city’s video surveillance: "The city owns the sidewalks. We own the

streets and we own the alleys"[1]. The police claims that public video surveillance is an effective tool to fight both crime and terrorism (Brown 761), but the fact remains there are many privacy issues that need to be considered. The ACLU, for example, argues that freedom of speech and association, anonymity and privacy are all infringed upon by video systems (Brown 762).

Most concerns about public video surveillance are based on the fact that a lot of sensitive information becomes available to the police and thus the government: attendance at political rallies, visits to abortion or HIV clinics and tracking what people read or buy (Brown 763) are only some of the potential threats for the individual. Mulligan claims that collecting this kind of sensitive information "could change the public character of our society" (qtd. in Brown 763), and that is why regulation of this domain is very much needed. The most important benefits that would result from the regulation of this system are shaping the conduct of officers using the video systems and defining their scope of permissible activities (Brown 764). The regulation would define the rules on when and how it would be allowed to use video surveillance in the whole of U.S. without breaking the law or the Constitution. The FISA Act is a good example of this kind of regulation because it requires more oversight of surveillance, so there is no reason there shouldn't be a similar law for video surveillance.

[1] http://www.nytimes.com/2004/09/21/us/chicago-moving-to-smart-surveillance-cameras.html?_r=0

6. Snowden revelations: New surveillance programs

Since its beginning in WWI, surveillance in the United States underwent constant development and improvement. We can see it in all the cases mentioned so far: it has grown from intercepting mail to tracking telephones and Internet activity, mobile phones, smartphones… The consequence of the technological advancement of our age is that more and more private information is now stored online, making it even easier to gather information on someone. Shamsi and Abdo argue that the combination of technological advances and governmental anxiety about terrorism has created "a massive and secret surveillance-industrial complex" (5), through which the government can track any U.S. citizen and his habits, conversations etc. (6). The U.S. government's ability to track any individual it wants is almost a common fact, but it is still true that the exact methods by which the government can obtain data or even the scale of surveillance was unknown until June 2013 and the revelations made by the whistleblower Edward Snowden. The information that Snowden made public were shocking because they showed that the massive system of surveillance was far greater than anyone could have imagined. The disclosure showed that not only was the volume of the data gathered through this system enormous, but also that it was picked up and stored completely indiscriminately, without any probable cause or suspicion.

Glen Greenwald is one of the three journalists that Snowden decided to contact to help him expose the information he gathered about the NSA surveillance programs. Greenwald's book *No Place to Hide: Edward Snowden, the NSA & the Surveillance State* is perhaps the best source of information on those programs precisely because he was in direct contact with Snowden, who provided him with the actual NSA documents detailing the scale of illegal activities[2]. Each surveillance program used a specific means of gathering

[2] Besides the book, the documents from the Snowden archive can also be found on gleengreenwald.net.

information and was aimed at different targets, but in the end, they were all intertwined into one enormous web of surveillance.

The most shocking program was probably PRISM because it focused on social media and internet companies, which is something that many consider a vital part of their daily life. Through PRISM, which started in 2007, the National Security Agency (NSA) gathered data from all the major internet service providers, including Facebook, Microsoft, Yahoo, Google, AOL and Skype. As explained in the previous chapter, under FISA the NSA no longer needed a warrant to conduct surveillance of U.S. citizens, as long as they were communicating with foreign nationals. This allowed the NSA to simply order U.S. Internet companies to provide them with access to all communication of non-U.S. citizens, which of course included communication with U.S. citizens (Greenwald 74). In other words, after amendments and legislative changes that happened after 9/11, the NSA had the ability to obtain unrestricted access to online communication and conduct massive surveillance of any foreign population and a large part of domestic communication. E-mails, chats, videos, photos, file transfers…; basically everything was accessible (Greenwald 110).

Greenwald points out that the companies involved in the program did not fight back and allowed the NSA unlimited access to their servers, the only exception being Yahoo!, which unsuccessfully tried to fight the order in the FISA court (109). Even more shocking was the fact that the companies even provided the NSA with a direct "search" system with all the information on all customers, regardless of their suspicion of illegal activity. According to Snowden, all messages and calls were cataloged and stored in 'Massive Data Repositories' and could have been accessed at any time (Greenwald 24). In short, all the major Internet service providers in the end cooperated with the NSA and provided them with global access to all communication and customer data.

Online communication was covered with PRISM, but the NSA did not stop at that. The documents provided by Snowden show that with a FISA court order the NSA ordered the telephone company Verizon to hand over *all* telephone records for communication inside the U.S. and between the U.S. and abroad. The previous chapter explains how the reason to obtain a FISA order for foreign intelligence gathering was lowered to “significant purpose”, which caused Henderson, Shamsi and Abdo to state concern about this change. Their fears were well founded, as Greenwald states that the US government used FISA on Verizon to collect telephone records of tens of millions of Americans "in bulk and indiscriminately", and most importantly, without any proof of wrongdoing (28).

It is enough to look at the data in BOUNDLESS INFORMANT, a program designed to quantify surveillance activities done by the NSA, to understand the reach of this global surveillance network. The data shows that in only one month period, "one unit of the NSA collected more than *three billion* pieces of communication data from U.S. communication systems alone" (Greenwald 30). To put this into perspective, this would amount to roughly 3 pieces of communication data on every U.S. citizen. This type of data (metadata) gathered from U.S. communication systems shows only information about the calls (e.g. when the call was made or the number that was called) and does not record conversations, but it can still reveal a lot of information about tens of millions of innocent and unsuspecting people. Greenwald argues that this information, which shows the size of the NSA’s surveillance activities, was clear proof that the government deceived Congress when Director of National Intelligence denied that the government gathered data on millions of Americans (Greenwald 30). He was an official in the president’s administration and still lied to Congress about the program because he knew that it was illegal and would provoke a public outcry.

The information is equally disturbing when it comes to international surveillance. Although many of the programs revealed by Snowden were aimed at U.S. citizens and their

correspondence with the rest of the world, Greenwald provides evidence that there are dozens of countries around the planet that were targets of "indiscriminate mass surveillance" (92). A document from the BOUNDLESS INFORMANT shows that the quantity of data gathered from other countries in a 30-day period is enormous: Germany (500 million), Brazil (2.3 billion), India (13.5 billion), with several other European countries targeted for mass surveillance (Greenwald 92). To provide more information on the NSA's surveillance ability, Greenwald writes that in 2005 the NSA collected "all communications from the entire Iraqi population" (96), while after 2007 it could analyze and store any British citizen's mobile phone, e-mail and IP address data (122).

The documents that the whistleblower Edward Snowden decided to share with the world in 2013 reveal a new stage of surveillance: massive indiscriminate global surveillance. It is not an exaggeration to describe it as massive because all the files show that data was collected in bulk: gathering *all* communication data from U.S. internet providers like Facebook and Google; collecting *all* telephone records on tens of millions of Americans; surveillance of the entire Iraqi population; access to every British mobile phone… Some reports suggest that the NSA intercepted and stored *1.7 billion* e-mails, phone calls and other type of communication *daily* from U.S. citizens alone (Greenwald 99). These numbers show the magnitude of the surveillance system that few believed was that enormous. The most worrying part of these disclosures is that data was gathered indiscriminately and then stored for further analysis, meaning that millions of completely innocent people were targeted by this surveillance program unbeknown to them, while their personal data might still be stored by the government. To put it differently, it seems that the NSA's policy when it comes to surveillance was "everyone is guilty until proven innocent". After these revelations, which showed that communication from around the world was collected in bulk and stored, we can no longer claim that our communication is private.

In June 2015 a new act called the USA Freedom Act was introduced to replace the USA PATRIOT Act, marking an important first step towards more transparency and oversight[3]. The act contains two important changes, the first one being the end of the bulk metadata collection program and focusing on a more targeted approach. The second significant change is introducing advocates on privacy and public concerns that would serve as an external check on the FISA court. The act was introduced only one month after a court ruled the NSA bulk collection program was illegal[4]. It is debatable whether this act represents a real change for the better, as security agencies can always find loopholes and new methods of surveillance, but it is nonetheless a positive move suggesting more significant changes could occur in the future.

[3] https://www.theguardian.com/world/2013/oct/10/the-usa-freedom-act-a-look-at-the-key-points-of-the-draft-bill

[4] https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html

7. The fear of terrorism

After a historical analysis of surveillance in the U.S., this chapter will deal with the reasons behind surveillance. Whether starting a new surveillance program, extending an existing one or changing the legislation regarding surveillance, the U.S. government has always used the same tactic: the fear of a foreign threat. This tactic was repeatedly used to supposedly start surveillance to combat that threat, but in the end the target always turned out to be different. Going back to the time of WWI, the reason to start surveillance was the fear of German agents, only to turn the given powers to silencing dissent that was coming from the African American community. After WWII, the Soviet Union was the new threat that had to be monitored, only to be revealed that the government used the broader power of surveillance to track journalists, civil rights movements and even the political opponents of the administration. The target of surveillance always turned out to be removed from the alleged threat that was used to justify surveillance.

Conolly-Smith explains there are many repeating patterns when this method is applied: Congress is always easily influenced in time of war to pass the needed legislation, but that legislation always remains active long after the war or crisis has passed (8). Later, when it becomes obvious that the law was breached and legislation is brought to its previous use, nobody is held accountable because "retroactive immunity simply renders moot all instances of prior legal transgressions" (Conolly-Smith 8). The latest American crisis similar to war was 9/11, shortly after which President Bush introduced the USA PATRIOT Act and the FISA Amendments Act. The justification for the changes was the fear of terrorism and prevention of further terrorist attacks. The circumstances under which the USA PATRIOT Act was passed are very similar to those described by Conolly-Smith: Congress was called upon to pass the legislation within a week, in the Senate it went “behind closed doors”, the legislators were not able to debate parts of the act and there was no chance of amendment

(Donohue 1101). The haste was important to the government because they wanted to avoid any debates and possible changes in the act itself and basically keep it intact. Donohue further argues: "Throughout this process the Executive made it very clear that either one supported what the Administration proposed or one was pro-terrorist" (1101), which shows the government used the fear of terrorism in the wake of the attacks to gain not only public approval but also to force the legislators to support the act. The second part of Conolly-Smith's claim, that nobody is held accountable after violations have been found, is also true in President Bush's case. He was never held accountable for his warrantless domestic wiretapping program because he could always use the excuse of terrorism to justify the program, just like he did for the USA PATRIOT Act. Snowden's previously cited claim, that The New York Times's omission allowed Bush to be re-elected is also highly debatable for the same reason – Bush had a justification that he could use at any time: the country was at war.

When the surveillance programs after 9/11 are examined closely, that same "terrorism" justification turns out to be false, because there is simply no evidence to prove that these programs prevented any terrorist attacks. Donohue claims that the previously discussed NSLs are ineffective, since the "Bush administration has not offered a single example of when a use of an NSL interrupted a terrorist attack" (1112). The same is true for other programs, since the Justice Department also could not cite a single case in which the analysis of the bulk metadata programs such as PRISM stopped a terrorist attack (Greenwald 202). Furthermore, Obama's advisory panel on the metadata program concluded it is "not essential to preventing attacks" (Greenwald 203), while the senators on the Intelligence Committee stated that "the usefulness of the bulk collection program has been greatly exaggerated" (Greenwald 203). In an article from *The New Yorker*, Lawrence Wright claims that the metadata program would not have prevented even 9/11 attacks, since the CIA had

had all the intelligence on the terrorists before the attacks but failed to act on it. Several terrorist attacks were actually prevented since the introduction of the bulk metadata programs, but they were detected and prevented either by alert bystanders or by using traditional police methods (Greenwald 203). In short, not one terrorist attack was prevented with the use of bulk metadata programs, which shows either that it was not effective for this job or that it was not used for this intention.

The documents provided by Snowden point to the real purpose of the NSA programs. The U.S. government used terrorism to defend the bulk metadata programs, but it turned out that most them were not even used to fight terrorism. Greenwald argues that "great quantities of the programs manifestly had nothing to do with national security. The documents left no doubt that the NSA was equally involved in economic espionage, diplomatic spying and suspicionless surveillance aimed at entire populations" (94). When it comes to the use and purpose of the surveillance programs, the documents show that economic interests were as important as counter-terrorism. Greenwald calls this kind of surveillance *economic espionage* and lists what the documents revealed:

> eavesdropping and email interception aimed at the Brazilian oil giant Petrobras, economic conferences in Latin America, energy companies in Venezuela and Mexico, and spying by the NSA's allies – including Canada, Norway and Sweden - on the Brazilian Ministry of Mines and Energy and energy companies in several other countries. (135)

Several other targets are listed in the book, such as the SWIFT banking system, the Russian airline Aeroflot and the Russian oil company Gazprom (Greenwald 135). One document, entitled "Serving Our Customers", lists Departments of Agriculture, Commerce and Energy (Greenwald 136), which shows the NSA is responsible for gathering information for these economic agencies. All of these documents clearly show that the bulk metadata

program is used to gain diplomatic advantage and economic gain and not to fight terrorism, which was supposed to be its primary goal.

The tactic that was repeatedly used by the U.S. government to broaden surveillance provided fear from a foreign threat as a justification. After 9/11 that was fear of terrorism, but we have shown it is false for two reasons. The first one indicates that not a single terrorist act was prevented or disrupted in its planning stage with the help of bulk metadata programs. The second reason is that many of the Snowden documents show the programs were primarily used for economic espionage to gain advantage over potential trade partners, which is far from its intended purpose.

8. The way forward

To avoid only criticizing the surveillance programs, this section will deal with the ways to minimize abuses of government surveillance in the future and discuss methods to achieve balance between national security, privacy and surveillance. In his article, Moore critiques three views in which the advantages of security trample over privacy rights. These three views can be seen as justifications for increased surveillance, which Moore analyzes to show why the idea that security should dominate over privacy is wrong.

The first view that Moore criticizes is “just trust us”, in which the people should trust their government and believe that it will use the power of surveillance wisely (Moore 143). The main problem with this idea is that history tells us this is not true. Moore warns that "In a crisis, even the most noble among us are susceptible to favoritism, stubbornness, and suspect reasoning" (143), confirming our previously argued notion about radical moves made in a time of crisis. The argument that people should believe that their government is doing the right thing works until a sudden unexpected emergency arises, and Moore lists several accounts in U.S. history when this was done, e.g. Lincoln suspending the legal rights of citizens in border states during the Civil War or Roosevelt interning Japanese-Americans during World War II. Moore writes that both decisions were made when a crisis emerged, adding that "liberty and privacy rights were suspended based on the subjective evaluation of a politician" (144). These politicians were trusted to do the right thing and they made a decision that completely disregarded civil rights. Other accounts when the government has not reacted well in a time of crisis or misused surveillance were already mentioned in this work: COINTELPRO programs, Watergate wiretapping, illegal programs after 9/11… They all show that governments cannot be trusted to use this power wisely.

Moore calls the second view “nothing to hide.” In this view surveillance is defended with an argument that if you didn’t do anything wrong you have nothing to worry about.

Moore argues the main problem is that almost everyone has certain information that they want to hide, even if it doesn't point to criminal activity (146). Medical history, party affiliation, religion or sexual orientation do not point to any criminal activity, so people should not be afraid that the government has collected that information, but in some contexts it can be very useful. It is possible to assume that at some point a government could use information of that sort to attack sexual or religious groups like LGBTQ groups or Jews. This notion is now more real than ever, as the current President Donald Trump even suggested he would support creating a database of all American Muslims[5]. The view that we have nothing to hide from the government becomes even more invalid when we see that certain ethnic or religious groups were often targets of surveillance: Muslims and Arabs after 9/11, African Americans during WW I … We can never know what the next criterion for surveillance will be, i.e. which social group will be targeted next, and that is why it is important to keep a certain level of privacy.

The last view often used to justify increased surveillance is "security trumps." The argument of this view is that security is more important than privacy, i.e. the interests of security always come first. Moore here offers three counterarguments: bodily privacy is at "least as fundamental or intuitively weighty as security" (147), an increase in security should not entail a decrease in privacy, and finally, certain safeguards are necessary before setting aside privacy for security (Moore 148). The conclusion to be drawn from this section is that security and privacy are both equally important and neither should have a dominant position.

After showing why putting security before privacy is wrong, we will focus on concrete proposals to achieve balance between the two. It is important to note that transparency and accountability are the integral part of almost every proposed solution. Shamsi and Abdo argue that reforming and updating the laws governing electronic

[5] http://www.politifact.com/truth-o-meter/article/2015/nov/24/donald-trumps-comments-database-american-muslims/

communication is necessary to ensure the protection of privacy (9). The next step should be ensuring protection from collecting communication without a probable cause or a warrant, to which Posner offers a solution in the form of a Congress committee that would monitor national security electronic surveillance and assure compliance with the Constitution (257). Other possible measures are to require the NSA to submit a list of all people that had been targeted without a warrant (257), using the intercepted information only for national security purposes and excluding ecoterrorism, animal-rights terrorism and political violence from the scope of surveillance because they do not represent a real threat to national security (258). Massive indiscriminate surveillance has proven to be dangerous when it comes to privacy rights and inefficient when it comes to stopping terrorist attacks. According to Greenwald, the solution for this is targeted surveillance aimed at individuals for whom there is evidence of illegal activity, which would enable security agencies to analyze data far more effectively (251).

The judicial branch plays a big part in ensuring these rules. FISA courts were supposed to be a solution for the breach of executive power, but we have argued before that they turned out to be ineffective. In order to fix this the courts have to be more effective in overseeing government action and, most importantly, "act as an independent check on the executive authority" (Henderson 208). This can be done by excluding the evidence without “significant purpose” for national security from investigation or by requiring the government to report back on a regular basis when authorizing roving surveillance (Henderson 209).

It is important to raise awareness of the dangers of massive, unrestricted surveillance. A notion that emails, text messages and data about calls from tens of millions of unsuspecting Americans are collected from network providers and then stored for analysis is not something from a work of fiction. It is happening today, as this is the current surveillance capability level of U.S. security agencies. It is crucial to bring this situation under control, i.e. to

increase and maintain oversight and control in the field of surveillance, because otherwise the number of people that are affected by this will only rise. Maintaining national security is important to prevent terrorist attacks, but a reasonable balance between privacy and security has to be recognized and maintained. The USA Freedom Act is a step towards more balance, but a larger and more efficient oversight of surveillance procedures is needed to prevent misuse of this power.

It seems that the current Trump administration is likely to undo even those small changes that were made for the better, as President Trump states that he supports legislation which would allow the NSA to keep bulk metadata collection programs[6]. At this pace, it is not unlikely that we will soon reach the point where *every* conversation, email and message are recorded and then stored for further use by the government. It is up to us to prevent this by supporting legislation that intends to curtail unconstitutional surveillance and by criticizing acts that want to broaden it.

[6] http://www.newsweek.com/where-do-presidential-wannabes-stand-patriot-act-334968

9. Conclusion

This thesis deals with the topic of surveillance done by U.S. security agencies and its effect on privacy and civil rights. There are several main arguments that were presented: the surveillance often clashed with the privacy and civil rights of American citizens; it was aimed at groups that presented no real threat to the security of the country but were actually a voice of dissent; and finally, it constantly expanded and grew bigger in a time of crisis.

The first topic that was discussed is the surveillance of African Americans during WWI. Here we have shown how a suspicion that the African American community was under the influence of German agents led to their surveillance because they opposed the American involvement in the war and protested the treatment of their community. This case is important because it is only one of the first in a series of targeting social groups that were not a threat to the security of the country.

We have argued that the FBI surveillance during the Cold War was an unprecedented breach of executive power, as it was unconstitutional and operated without any oversight or control by the Senate. We showed that surveillance programs of this period were aimed at civil rights groups and anti-war activist that again represented no real threat to the country, while the Watergate scandal further deepened the problem with the information that even political opponents and the opposition were under surveillance.

In the following chapter, the Foreign Intelligence Surveillance Act (FISA) was presented as a logical consequence of the findings of the Church Committee. The focus here was on the inefficiency of the FISA Act; while it was supposed to bring more transparency and provide a system of oversight, we have argued that the FISA Court is not an effective body when it comes to imposing control on surveillance.

A new crisis brought significant legislative changes in the ways surveillance was conducted. In other words, we have argued that 9/11 was regarded at that time as an

emergency, a war crisis which resulted in the introduction of surveillance acts that were devastating for privacy and civil liberties. This chapter offers arguments that the USA PATRIOT Act removed limitations previously posed by the FISA Act, lowered the level of significance that was needed for surveillance and in general impacted privacy and constitutional rights. Similarly, the FISA Amendments Act is presented as an act that to a great degree expanded the scope of surveillance, which was done by making it possible to gather information on any U.S. citizen without a warrant or judicial oversight if that person communicates with a non-US citizen. This chapter also contains a short look at public video surveillance, the dangers of it eroding privacy rights and the need for regulation in this field.

The following chapter deals with the revelations that were made public by Edward Snowden in 2013. The main argument here is that every development in the field of surveillance that was discussed so far led to the point of massive indiscriminate surveillance. We have argued that the information provided by Snowden shows the NSA surveillance programs were unconstitutional because they gathered tens of millions of data on American citizens without any proof of wrongdoing and without warrant. Furthermore, the final result of all the legislative changes discussed in the previous chapters of the thesis can be seen in the analysis of the programs such as PRISM and BOUNDLESS INFORMANT.

The focus of the penultimate chapter is on terrorism and the ways it is used to justify surveillance. We have shown that on numerous occasions the same pattern was used to justify the broadening of surveillance, and every time the target was different than the one stated. We have also argued that the latest justification for broader surveillance (terrorism) is false: it did not prevent any terrorist attacks and the analysis of the documents shows that economic interests were behind many of the surveillance programs.

The final chapter is entitled “The way forward” and focuses on ways to improve the current situation and ideas on how to bring balance to the surveillance-privacy conflict. First

we have analyzed three views that are used to justify surveillance in order to offer counter-arguments on why these views are false. In the end we have listed steps that need to be taken to improve the current imbalance between privacy and security.

Works Cited

Brown, Jeremy. "Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places." *Berkley Technology Law Journal*, vol. 23, no. 1, 2008, pp. 755-81. JSTOR, www.jstor.org/stable/24118339.

Cinquegrana, Americo R. "The Walls (And Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978." *University of Pennsylvania Law Review*, vol. 137, no. 3, 1989, pp. 793–828. JSTOR, www.jstor.org/stable/3312277.

Conolly-Smith, Peter. "'Reading Between the Lines': The Bureau of Investigation, the United States Post Office, and Domestic Surveillance During World War I." *Social Justice*, vol. 36, no. 1 (115), 2009, pp. 7–24. JSTOR, www.jstor.org/stable/29768523.

"Developments in the Law: The National Security Interest and Civil Liberties." *Harvard Law Review*, vol. 85, no. 6, 1972, pp. 1130–1326. JSTOR, www.jstor.org/stable/1340060.

Donohue, Laura K. "Anglo-American Privacy and Surveillance." *The Journal of Criminal Law and Criminology* (1973-), vol. 96, no. 3, 2006, pp. 1059–1208. JSTOR, www.jstor.org/stable/40042805.

Doyle, Richard B. "The U.S. National Security Strategy: Policy, Process, Problems." *Public Administration Review*, vol. 67, no. 4, 2007, pp. 624–29. JSTOR, www.jstor.org/stable/4624613.

Eggert, David S. "Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches." *Duke Law Journal*, vol. 1983, no. 3, 1983, pp. 611–44. JSTOR, www.jstor.org/stable/1372386.

Ellis, Mark. *Race, war, and surveillance: African Americans and the United States government during World War I*. Indiana University Press, 2001.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA & the Surveillance State*. Penguin Books, 2015.

Henderson, Nathan C. “The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications.” *Duke Law Journal*, vol. 52, no. 1, 2002, pp. 179-209. JSTOR, www.jstor.org/stable/1373134.

Johnson, Wray R. "Black American Radicalism and the First World War: The Secret Files of the Military Intelligence Division." *Armed Forces & Society* (0095327X), vol. 26, no. 1, 1999, pp. 27–54. EBSCOhost.

Kent, Andrew. “Disappearing Legal Black Holes and Converging Domains: Changing Individual Rights Protection in National Security and Foreign Affairs.” *Columbia Law Review*, vol. 115, no. 4, 2015, pp. 1029-84. JSTOR, www.jstor.org/stable/43387029.

Lyons, Carrie Newton, et al. “National Security.” *The International Lawyer*, vol. 42, no. 2, 2008, pp. 811–19. JSTOR, www.jstor.org/stable/23828493.

Moore, Adam D. “Privacy, Security, and Government Surveillance: WikiLeaks and the New Accountability.” *Public Affairs Quarterly*, vol. 25, no. 2, 2011, pp. 141–56. JSTOR, www.jstor.org/stable/23057094.

Posner, Richard A. “Privacy, Surveillance, and Law.” *The University of Chicago Law Review*, vol. 75, no. 1, 2008, pp. 245–60. JSTOR, www.jstor.org/stable/20141907.

Reedy, Neil, and Justin Miller. “The Evolution of Homeland Security and the War on Terror.” *America’s War on Terror*, 2nd ed., edited by Tom Lansford, Robert P. Watson and Jack Covarrubias, Ashgate Publishing Limited, 2009, pp. 119-35.

Shamsi, Hina and Alex Abdo. “Privacy and Surveillance Post-9/11.” *Human Rights*, vol. 38, no.1, 2011, pp. 5-9, 17. JSTOR, www.jstor.org/stable/23032368.

Sunstein, Cass R. “Judging National Security Post-9/11: An Empirical Investigation.” *The Supreme Court Review*, vol. 2008, no. 1, 2008, pp. 269–91. JSTOR, www.jstor.org/stable/10.1086/597024.

Theoharis, Athan G. “FBI Surveillance during the Cold War Years: A Constitutional Crisis.” *The Public Historian*, vol. 3, no. 1, 1981, pp. 4–14. JSTOR, www.jstor.org/stable/3377157.

Abstract

The purpose of this paper is to analyze the effects of surveillance on privacy and civil rights in the United States, and to provide an overview of the evolution of surveillance by focusing on legal changes in the field. The research covers a longer period, starting with the WWI and ending with the latest developments in the field of surveillance in 2015. The common objective in the analysis of all surveillance programs was to explore their legality and intended target.

This paper first examines the surveillance of the African American community in WWI and argues that this group was targeted under false claims that it was influenced by German agents, while the real purpose was to silence the critique of the government. A similar notion is argued in the part on the FBI surveillance during the Cold War, where it is proven that the surveillance programs were misused to spy on journalists, civil rights activists and even the opposition. The FISA Act is then presented as a consequence of these violations and analyzed for its significance in future surveillance programs. The thesis then focuses on 9/11, an event defined as a national crisis and then further analyzed for the significant legislative changes it caused in the surveillance field. The impact of these changes is then examined in the part that focuses on the Snowden revelations. Before turning to an approach that provides ideas and theories on how to achieve balance between privacy and surveillance, the thesis looks into the use of terrorism for the justification of surveillance.

In conclusion, the thesis argues that the history of surveillance in the U.S.A. is filled with government abuse and unconstitutional practice with complete disregard for privacy and civil liberties, which is proven by providing an analysis of surveillance acts along with the recorded abuses from that period. The thesis also shows that justifications used for surveillance were often false because in several cases the intended target turned out to be

social groups that were not a security threat to the country, but were still targeted for being a voice of dissent, while in other cases it was done for economic interest.

Keywords: surveillance, privacy, national security, the United States, National Security Agency