Exploring the Privacy-Security Antinomy

A Case Study of the Privacy-Privacy Trade-Offs in US Intelligence Policies

Universiteit Leiden
Humanities

Job Verest

s1994751

Master Thesis

International Studies

Supervisor: Dr. E. Cusumano

Word count: 14.984

31 January 2019

Table of contents

Exploring the Privacy-Security Antinomy:

A Case Study of the Privacy-Privacy Trade-Offs in US Intelligence Policies

1. Introduction

The discussion of privacy values in our lives has heated in recent years. One cause for this are the ever-growing cases of privacy scandals worldwide. The notorious scandal of Cambridge Analytica is one of the recent examples (e.g. Cadwalladr & Graham-Harrison, 2018; González, 2017; Obar & Oeldorf-Hirsch, 2018). Moreover, a multifold of large companies have been accused of not taking privacy measures seriously into account, such as Facebook, Google and Microsoft (e.g. Parmar, 2018; Rosen, 2012; Rubinstein & Good, 2013). The Snowden revelations of 2013 rekindled the public interest in privacy values. The disclosures exposed the occurrence of multiple privacy violations within the intelligence community, which is the topic this research deals with.

It all started with an article of the Guardian in June 2013 which revealed that the National Security Agency (NSA) collected phone records (metadata) in-bulk from Verizon, one of the biggest telecommunication providers in the United States of America (US) (Greenwald, 2013). The Guardian obtained its information from one of the most famous whistleblowers of all times, Edward Snowden. Snowden eventually revealed, by leaking documents, massive surveillance of Internet traffic, social media posts, telephone calls, and emails executed by the NSA (Andregg, 2016). They gather and mine data from different firms and corporations, such as Internet and telephone companies (Lyon, 2014). An example is seen in the PRISM program; in this program, the NSA got direct access to different servers of Silicon Valley technology giants, including Apple, Facebook, Google, Yahoo, and Microsoft (Lyon, 2014).

Although a lot of secrecy still exists, the way the intelligence agencies work has become more known to the public since the Snowden revelations of 2013, including what kind of data these agencies gather and their method doing so. In March 2017, Wikileaks revealed confidential documents of the Central Intelligence Agency (CIA) which showed that the agency hacks smartphones, (smart-)TVs, and PCs from US citizens (Wikileaks, 2017; Solon, 2017). In this way, it could, for example, listen to your conversations and quarrels with your wife or husband through the microphone in your smart TV.

The privacy-security debate is generally divided along two sides. One side believes that the violation of privacy by these agencies is a necessary evil in order to protect the national security. One of the most repeated arguments from this side is *"we must be willing to give up some privacy if it makes us more secure"* (Solove, 2011, p.9). The other point of view is that the privacy of the civilians of a nation should not be compromised.

After 9/11, national security became the key matter in US policy. One and a half month after the attack, acting President George W. Bush signed the USA Patriot Act, which allowed greater leeway in domestic intelligence and law enforcement collection (Lowenthal, 2016). This resulted, for example, in permission for the collection of metadata from phone records, established in the Section 215 of the USA Patriot Act (Lyon, 2014). Former President Barack Obama responded to the growing privacy concerns, after the Snowden revelations, in the following way: "*I have called for reforms that better safeguard the privacy and civil liberties of the American people while ensuring our national security officials retain tools important to keeping Americans safe. That is why, today, I welcome the Senate's passage of the USA FREEDOM Act"* (The White House, 2015, para. 1). The USA Freedom Act of 2015, which builds on the USA Patriot Act, makes it, for example, impossible for intelligence agencies to continue the bulk collection of phone records (GPO, 2015).

Next to the heated public debate on privacy, scholars' interest in this topic has been sparked as well, as privacy clashes with different social values in our lives. Different antinomies have been discussed in the academic debate, such as privacy vs security (e.g. Nissenbaum, 2010, p.108), privacy vs free speech (e.g. Rosen, 2012; Volokh, 2000), privacy vs technological innovation (e.g. Baker, 2013), and privacy vs efficiency (e.g. Nissenbaum, 2010, p.109).

Of the aforementioned antinomies, the conflict between privacy and security stands out as one of the most debated topics among scholars and it is directly linked to the work and the power of the intelligence community. Posner and Vermeule (2007) see privacy and security, or civil liberties and security, as a zero-sum trade-off; this would mean that a loss in privacy automatically leads to a gain in security and the other way around. However, recently, this notion has been criticized by many scholars. Solove (2011) contends that this is an *all-or-nothing fallacy*: Privacy-security is not a zero-sum trade-off, and one does not have to sacrifice one for the other. An example is seen in the research by Lowenthal (2016) and described as the *wheat versus chaff problem:* more privacy violations in the form of collection by using surveillance techniques makes it only harder to find the needle in the haystack. Consequently, collecting more information about citizens does not per se increase the national security. Dragu (2011) adds that it is in the interest of the intelligence agencies to violate privacy, even if this would harm the national security, because more collection of information would give more money and power to the intelligence community.

In response to the public and academic criticism, intelligence policies have been adapted to better incorporate privacy interests. While the goal of these policy amendments has been to protect privacy much better, unintended negative side-effects can happen. Pozen (2016) called this the phenomenon of privacy-privacy trade-offs: the impact of privacy measures on other sorts or forms of violations of privacy. These different aspects of privacy are based on the taxonomy of the concept of privacy made by Solove (2008). As it is very hard to define the concept of privacy, it is seen as an

umbrella term by most privacy theorists. Consequently, Solove (2008) made a taxonomy to try to cover most of the umbrella term. In this framework, sixteen broad categories of "*privacy problems that have achieved a significant degree of social recognition*" (Solove, 2008, p.101-102) have been identified. As a result of the broad concept of privacy, different categories of the concept can contradict each other. In this way, new intelligence policy to protect privacy could be counterproductive. An example is the following: surveillance and interrogation could both cause a violation of privacy. A decrease of financial resources or a tightening of rules for interrogation, could decrease privacy problems regarding interrogation. This, however, might lead to more surveillance to make up for the loss of data collection through interrogation and, as such, increase the privacy problems of surveillance (Pozen, 2016).

Although scholars have studied in-depth the topic of privacy-security trade-offs, what is still lacking in the academic work is the in-depth application of the concept of privacy-privacy trade-offs on an empirical case. Pozen (2016) touched upon the NSA and its surveillance techniques but did not go into detail about this topic. This research fills this gap in literature, by providing a case study analysis of the privacy measures, and the possible privacy-privacy trade-offs of the USA Freedom Act. It thereby adds to the literature on the privacy debate in general and privacy-privacy trade-offs in particular. In this way, the research question is as follows:

What kind of privacy-privacy trade-offs have occurred during the adoption and implementation of the USA Freedom Act of 2015?

Next to its academic relevance, this research could add knowledge and new insights for policymakers who have to take into account the protection of the concept of privacy in its broadest terms. The analysis focuses on two specific sections of law written about the US intelligence community. First, Section 215 of the USA Patriot Act which included a mandate for the NSA to collect data of phone records of US citizens in-bulk. This Section was altered by the adoption of the USA Freedom Act. Second, Section 702 of the FISA Amendments Act which includes the collection of content of Internet communications. The programs of the intelligence community under this Section can still be executed; the USA Freedom Act did not tighten the rules on these surveillance programs.

The finding of this study is that privacy-privacy trade-offs occurred, mainly because of expanded interpretations and implementation of unchanged legislation (Section 702 of the FISA Amendments Act), after, from the perspective of the intelligence community, restrictive changes that have been made on other legislation (Section 215 of the USA Patriot Act). In this way, privacy guarantees that have been made in the USA Freedom Act contradict its goal, which is to safeguard the privacy and civil liberties of US citizens.

This research contains five parts. After the introduction, a historical and theoretical background of the development of the intelligence community is given to provide insight into the functioning of this community. Thereafter, the concept of privacy is introduced, as well as the academic debate on the privacy-security antinomy. From the literature it follows that privacy and security do not have a zero-sum trade-off. Consequently, privacy should be better guaranteed within the work of the intelligence community. Therefore, the concepts of *privacy* and *privacy-privacy trade-offs* are central in the next section, where they are discussed in-depth and operationalized so that they can serve as the basis for analysis. Then, the methodological approach is discussed. The study makes use of an illustrative case study as well as a critical incident case study. In this way, this research is descriptive as it describes the context of the case, the US intelligence community, but as well explorative as it further explores the relatively new theory of privacy-privacy trade-offs. In the analysis, the framework of Pozen (2016) is used to analyse if any of the privacy-privacy trade-offs have occurred after the adoption of the USA Freedom Act. In the last section, the conclusion, an answer is given to the research question, and the relevance of the findings are addressed.

2. Historical and Theoretical Context

2.1. The Intelligence Community

Before digging into the academic debates about privacy, it is, as this paper deals with intelligence agencies, of utmost importance to discuss this community in further detail. The first section of this chapter contains four parts: 1) What is, and what is the purpose of, intelligence? 2) How is the data that intelligence agencies use collected and which kind of data is collected? 3) What does the structure of the process of intelligence, the intelligence cycle, look like? 4) What is the societal impact of the current work of intelligence?

First of all, intelligence can be traced way back in history; Machiavelli already travelled around to gather information about other monarchies and governments. The purpose of these diplomatic missions was to increase the security of Florence (Glendon, 2011). During the 20th century, the academic world started to write about intelligence, and the last twenty years this topic has gained increased attention from scholars. It is nowadays not just a sub-field of international relations and diplomatic history, but functions as a whole new terrain to be discovered and discussed (Dover, Goodman, & Hillebrand, 2014). Part of this increased importance of intelligence studies is due to the increased complexity of intelligence itself since the end of the Cold War, and more specifically since the beginning of the 21st century. As a consequence of the globalized, interconnected, and modernized world, uncertainty of individuals and states has grown. The dangers are not only coming from a military

(or economic) attack anymore, but include risks of epidemics, climate change, nuclear energy, new technologies, and the risk of a change in cyberspace and socials systems (Agrell & Treverton, 2015). Moreover, the *attack* could not only come from a state, but from one of the 7,6 billion individuals on the globe (Dover et al., 2014; Worldometers, 2018). Intelligence agencies have adapted to this globalized world by using new methods and technologies to collect, analyse and assess information.

Warner (2007) defined intelligence as follows: "*that which states do in secret to support their efforts to mitigate, influence, or merely understand other nations (or various enemies) that could harm them"* (Warner, 2007, p.17). Taking into account the new threats that nation states face today, intelligence does not only try to uncover the capabilities of other states, but as well of their own citizens (Tucker, 2014). Moreover, intelligence agencies try more and more to expose the intentions, next to the capabilities, of their enemies (Tucker, 2014). It is important to know what people do, but it is even more important to know what people think as this could say something about the actions of an individual in the (near) future. In this way, intelligence services try to avoid national failures and disasters by collecting information and analyse and assess this information (Tucker, 2014).

In the far past, intelligence agencies only focused on producing descriptive intelligence. This intelligence dealt with observable data, such as geography, government and economic changes, and data about the quantity and quality of armed forces of foreign countries (Kent, 1966). Since the second half of the 20st century, intelligence agencies, who were formed, started to gain interest in speculative intelligence, which is speculating (and analysing) about the future; examples range from what the climate will look like in the future, to what the intentions of other states, and their corresponding actions, are in the near future (Kent, 1966). In these analyses, the social science methodology is followed to get speculative results about the future, including different scenarios, or an in-depth analysis about individuals' intentions (Tucker, 2014). As Kent (1966) already argued, the quality and reliability of the methods are the most important in this speculative intelligence to get the best results.

However, here lies a problem. Speculation and analyses about the future cannot give any guarantee that the probable scenario will be the reality in the future; the social science methodology cannot take everything into account and completely predict the future (Kent, 1966). In this way, intelligence cannot eliminate the uncertainty that lies in the intentions of individuals, or groups. This means that the perception of a *zero-risk society* is an illusion, and that intelligence fails sometimes. There are plenty examples of events that were not anticipated or predicted by intelligence, for example 9/11 and the Arab Spring (Tucker, 2014). This means that intelligence faces challenges to estimate risks, frame uncertainties, and to produce actionable knowledge demanded by policymakers. These events could not be predicted by intelligence agencies, even while the intelligence agencies never collected as much information as they collect today (Dover et al, 2014). Therefore, it is worthwhile to look at what kind of data the intelligence agencies nowadays collect.

In the speculative intelligence era we live in today, intelligence agencies put more weight on collecting as much data as possible, which is a lot in today's digital world, to make sure that the relevant information is collected (Solove, 2011; Walsh & Miller, 2016). To that end, speculative intelligence focuses more on information and communication technologies (ICT). However, nowadays, the intelligence community does not only want to extract content that could be relevant today. It also wants to collect information that is not relevant right now but could be so in the future. In this way, the intelligence community tries *to fully get to know* an individual, which could reveal their personal traits and characteristics. This means that privacy is violated, while it does not necessarily lead to increased security: people are nowadays easier seen as possible suspects without any evidence (Walsh & Miller, 2016).

Privacy is not only violated in the collection step, but as well in other steps in the intelligence cycle. The intelligence cycle is "*the process by which information is acquired, converted into intelligence, and made available to policymakers"* (CIA, 1983, p. 17). This intelligence cycle, first used by the CIA, represents a loop with, in most cases, five different steps; planning and direction, collection, processing and exploitation, analysis and production, and dissemination (Omand, 2014). The first step focuses on the goals and priorities of the intelligence agencies, such as which tool is used to collect the data, and which technology is used during the process. The next step, collection, is collecting data or raw information that may be relevant for the priorities that are stated in the first step. The following step processes the collected data into a form so that it can be exploited by analysts. These analysts evaluate the data for reliability, validity, relevance, and context, and they execute analyses by using social science methodology which eventually leads to the product of an intelligence report. In the last step, the dissemination, the intelligence report is shared to those who need it: policymakers most of the time. The results of the intelligence report can give new requirements in the planning and direction step, which shows that the intelligence process is a cycle. These five steps are not always followed in the same direction; sometimes, after step 2 you are going back to step 1, or from step 4 you are going back to step 2 (Omand, 2014).

Although the intelligence cycle works well in theoretical terms, the problem is that much data which is collected does not get processed and exploited. The main cause is that a lot of process is done by human employees, without technical shortcuts. The intelligence community uses some software programs to assist employees, such as data mining and text mining, but until now, no major breakthrough has been made of reliable, effective and efficient technology that could fully take over the work of people, especially regarding the analysis of collected content of communications (Lowenthal, 2016). Metadata collection can be analysed more easily by computer software programs. As a result, suspects, and their networks, can be more easily identified from a large pool of information (Kadidal, 2016).

Next to different modes of intelligence (metadata and content data), there are different ways to produce the intelligence data used in the intelligence cycle. This study focuses on Signals Intelligence (SIGINT), because this form of intelligence has been mostly contested in the public and academic world regarding its increasing scope in the globalized and interconnected world. SIGINT intercepts (electronic) signals, including communications between people. Although SIGINT increasingly gained much more interest as the possibilities for electronic communication have exponentially grown, it is connected to a much older science, cryptography. Basically, SIGINT tries to gather information about who is talking to who, about what, on which times, and what the frequency is of these communications. Cryptography is a means to keep the message only readable by the sender and the intended recipient (Richards, 2014). In the Internet world of today, a lot of opportunities open up for the use of SIGINT; the behaviour of individuals can be more easily monitored (via the Internet) as it is almost impossible to stay off the grid. In this way, much more data is collected by intelligence agencies via SIGINT (Richards, 2014). The intelligence community argues that this increases the security. However, Solove (2011) contends that these agencies are only collecting as much as possible for the sake of collecting which increases their power as this information can be used to manipulate innocent individuals. Moreover, criminals and terrorists try to stay under the radar by using traditional communication channels; a bulk collection of SIGINT data would not help in this respect (Solove, 2011).

While SIGINT has known an exponential grow after the large increasing use of electronic communications, it is, for context purposes, relevant to discuss other forms to produce intelligence. Human Intelligence (HUMINT) is the oldest way to produce intelligence; Sun Tzu wrote in the fifth century BC already about the necessity of spies in warfare in his book *The Art of War*. Spies were used in these times to collect geographical, military and economic data; this foreknowledge is key, in the eyes of Tzu, to achieve national objectives (McCreadie, 2008). In the modern era, spies are still used to uncover secrets in these domains, however, their work has broadened to, for example, include data about (nuclear) energy systems (Richelson, 1995). Moreover, data collected by spies are nowadays used to give more context to the data which is collected by other forms of intelligence (Scott, 2014). Some other ways to produce intelligence are via Measurement and Signature Intelligence (MASINT) and Open Source Intelligence (OSINT). In today's open and globalized world more information is available in the public domain: this information is used for OSINT (Gibson, 2014). MASINT is derived from measuring specific things, by the help of sensors and other measurement tools (Aid, 2014). It was used a lot during the Cold War by the US and the Soviet-Union to measure nuclear activities and to be able to monitor airplanes and missiles of the enemy (Aid, 2014).

As we live in a *risk society*, with an increasing amount of different threats, intelligence has gained in importance. The concept of a risk society stresses the growing uncertainty surrounding the gains of modernizations, and the negative impacts on the environment, as well as the increasing risks

of technology and social systems. Science and technology create risk, but at the same time they are needed to discover and manage the risk. Handling the national security nowadays thus encompasses a broad risk matrix of societal risks that have to be managed (Agrell & Treverton, 2015).

The surveillance of intelligence agencies to manage these societal risks creates societal impacts, such as the violations of human rights. These societal impacts increased the aversion against the *surveillancization* of societies. Surveillance technologies has shown to put young, ethnic minority groups into danger of discrimination by police (Murray & Fussey, 2018) which is also known as ethnic profiling (Roehlinger, 2016). In the *Metropolitan Police Service Gangs Violence Matrix*, which is a database to identify suspected gang members in London, 40% of the total, of 3.806 who were on the list in 2017, had zero risk of causing harm (Amnesty International, 2018). Moreover, 75% of the people identified in the matrix have been victims of violence themselves (Amnesty International, 2018). Still, people, mostly young black minorities (78%), were on the list just based on an algorithm, which includes information as the clothes they wear, what music they listen to or how they greet each other (Amnesty International, 2018). Numerous other examples of negative societal impacts of mass surveillance exist (see for example: Liang, Das, Kostyuk, & Hussain, 2018). Consequently, freedom of speech (CBS News, 2015) and freedom of movement (Wang, 2017) are under threat. Obviously, because big data is collected by using surveillance techniques, privacy is violated (Liang et al., 2018).

2.2. Privacy Turn

The UN Special Rapporteur on Privacy, Joseph Cannataci, already stated that there is not a clear definition of privacy. In this way, it is hard to control the right to privacy which is set out in the human rights regime. As the Special Rapporteur puts it: "*in some cases it may prove to be next to useless if we were to have 193 nations signed up to the principle of protecting privacy if we do not have a clear understanding of what we have agreed to protect*" (OHCHR, 2016, p.9). In the academic world, there has not been any consensus on the definition of privacy either. As a consequence, a pluralistic turn has led to "*an understanding of privacy as an umbrella term that encompasses a variety of related meanings"* (Richards, 2015, p.9).

Warren & Brandeis (1890) laid the foundation for the US privacy laws. In their Law Review article, *The Right to Privacy*, they criticized the journalists, especially the photojournalists, in the US during this period as they were intruding in the personal spheres of people. Following this, they made a plea to recognize a right to privacy in the law to impose liability when these (photo)journalists invaded into someone's private life (Bratman, 2002). The influence of the article by Warren & Brandeis (1890) was much bigger than *just* the tort law their statements are primarily based on; scholars and judges are, still today, citing their work as the first work in US legal history regarding to the right to

privacy (Bratman, 2002). In the years after their publication, different states in the US adopted a body of privacy laws (Bratman, 2002). Although the right to privacy is not explicitly stated in the US constitutional law, different laws that could be considered to fall under the protection of the umbrella term of privacy are stated in its constitutional law (Solove, 2011).

Regarding to privacy law, the right to privacy has mostly been interpreted as "*the right to be left alone"* (Espinosa, 2012, p. 969). Nowadays, however, attention has been enlarged to "*the right to define and construct one's own identity, not only in isolation but in social relations"* (Espinosa, 2012, p. 969). In this way, two dimensions of privacy can be distinguished: individual privacy and social privacy (Espinosa, 2012). Social privacy could be considered as enabling to be the person you want to be in social settings without feeling restrictions because of surveillance or other forms of violations of privacy. Moreover, shared privacy, a term coined by Combs (1987), could be considered a part of social privacy. It means that we should be protected to freely choose with whom we share private information, and with whom we share our home. Although social and shared privacy gained increased attention by scholars, the most courts and judges primarily look at individual privacy and the right to be left alone (Combs, 1987; Espinosa, 2012). This creates room for SIGINT, which primarily violates the notion of social privacy.

Scholars shed different lights on the importance of the fundamentality of the concept of privacy. Thomson (1975) does not see any additional value of privacy, as all the things it covers could be protected and explained by other human rights, such as bodily security and property rights, while McGregor (2016) contends that privacy functions as a necessary enabler and guarantor of other human rights which is of key importance in the rapid changing world of technological improvements and big data. Additionally, Bloustein (1964) argues that privacy is a necessary condition for reaching human dignity.

Although different perspectives are seen in the academic world regarding to privacy, increased interest in this topic can be observed since technological innovations, and especially since the Snowden revelations (Richards, 2015). Because of the digital world, and the increased use of cameras and other smart technological systems, more and more can be collected by governments, private companies, and fellow citizens. Nowadays, (personal) data is everywhere, which means that there is almost no place for privacy anymore (Agrell and Treverton 2015).

One of the reasons that the boundaries of privacy have faded is that privacy has been traded for a greater good, such as efficiency, technological innovations and the right of free speech (Cohen, 2012; Bennett & Raab, 2006). One of the most debated trade-offs is the one between privacy and security (e.g. Lowenthal, 2016; Pozen, 2016). Solove (2011) showed that citizens do not want that all information about them is open for, and used by, intelligence agencies, or other organizations or companies. If this data increases the national security, or it fulfils a public good, people are

nevertheless more willing to give up their civil liberties, including privacy. But, is there a trade-off between privacy and security? And, to connect this with the intelligence community: would national security increase if more information about individuals will be collected by intelligence agencies?

The answer to these questions is ambiguous. On the one hand, more information would increase the chance that it includes important intelligence. On the other hand, the more information an agency collects, especially regarding to content data collection, the higher the chance that the information does not have any value (Lowenthal, 2016; Solove, 2011). Lowenthal (2016) calls this '*the wheat versus chaff problem'*: there is too much data collected to process, and to sift through all the data which have to be processed is a tough job which requires training and experience. Even then, experts could still make mistakes as unpredictable variables are into play. The risks of an attack cannot be decreased by collecting more and more data; on the contrary, it is much harder to find the needle if the haystack grows bigger and bigger (Lowenthal, 2016). Lowenthal (2016) and Solove (2011) argue, in this respect, for more focus on the analysis and processing of data instead of the collection of data.

Next to this problem, Fussey (2015) argues that the mass surveillance of intelligence agencies on citizens does not make us safer; it is the traditional work of spies that keep us safe. Anti-terrorist investigations are mostly (76%) started because of informants and community tip-offs, while NSA's bulk surveillance programs played an insignificant role in 1,8% of the cases in the same period. Moreover, Fussey (2015) observed a recurring problem that the information which is already collected is not prioritized, analysed, and responded to in the right way. The terrorists that committed the attacks in London and Paris were already known by police and intelligence agencies, but the attacks could not be prevented as the information was not processed and analysed properly (Fussey, 2015).

In conclusion, recently, most scholars (e.g. Lowenthal, 2016; Solove, 2011) argue that a zero-sum game between privacy and security does not exist. It is possible to increase the national security, without affecting the privacy, and giving up privacy does not mean that security can be guaranteed (Dragu, 2011; Solove, 2011).

3. Theoretical Concepts and Operationalization

3.1. Privacy

Since there has been a lot of debate about the definition of privacy, it is imperative to define and operationalise the concept to be able to use it in this study. Solove (2008) identified at least six broad conceptions of privacy: (1) '*the right to be let alone'*, (2) '*limited access to the self*' (3) '*secrecy*' (4) '*control over personal information'*, (5) '*the protection of one's personality, individuality, and dignity*',

and (6) '*control over one's intimate relationships or aspects of life'*. Refraining from a too narrow definition, Solove (2006) has also introduced a taxonomy of the privacy concept.

This study uses the taxonomy of Solove (2006) in its analysis. In bringing together different understandings of privacy, Solove (2008) argues that privacy should be operationalized from a *bottom-up* approach looking at *privacy problems*, and why these privacy problems are harmful, instead of a *top-down* one which focusses on conditions of its concept. The framework made by Solove (2006) consists of different privacy violations that have achieved social recognition. These privacy problems are grouped in four categories: *information collection*, *information processing*, *information dissemination* and *invasions.* Under these four categories, Solove (2006) identifies in total sixteen broad "*privacy problems that have achieved a significant degree of social recognition*" (p. 101-102):

Information Collection

Surveillance

Interrogation

Information Processing

Aggregation

Identification

Insecurity

Secondary Use

Exclusion

Information Dissemination

Breach of Confidentiality

Disclosure

Exposure

Increased Accessibility

Blackmail

Appropriation

Distortion

Invasions

Intrusion

Decisional Interference

While Warren & Brandeis (1890) merely focused on reputational harms, which could be described as a form of dignitary harm, the list made by Solove (2006) consists of much broader privacy problems. It includes other dignitary harms, such as lack of respect, incivility, and the causation of

emotional angst. Moreover, the indicators identified above could in essence be a more structural problem, or *architectural problem* as Solove (2004) calls them; this means that certain issues could harm privacy of individuals in an indirect way. Solove (2006) identified the two most common architectural problems. Firstly, the risk that a harm could occur in the future could be enhanced, as, for example, increased activities whereby personal information is involved, multiplies the risk of identity fraud (*identification*). Secondly, a person's life could be affected by a particular activity which changes the institutional power. An example would be when intelligence agencies gain power and increase the use of camera's and other *spy eyes* (*surveillance*), the behaviour of people could be altered (Solove, 2006). This second structural problem has been described as the *chilling effec*t (e.g. Michelman, 2009).

Though the list made by Solove (2006) is not exhaustive, it provides insight in the different dimensions that are important to discuss when working with the concept of privacy. Therefore, this research uses the taxonomy of Solove (2006) for the operationalization of the concept. This study primarily deals with the privacy problem *surveillance* which falls under the category of *information collection*, because US intelligence policies discussed in this research primarily deal with the topic of surveillance, which also gained the most attention in the public debate about privacy.

3.2. Privacy-Privacy Trade-Offs

As the Snowden revelations showed to the public that the intelligence agencies, and, in this respect, the government, monitored the population on a large scale, this sparked an intense public debate about privacy and the work of intelligence agencies (Lyon, 2014). Following this public debate, the White House endorsed, backed by the Senate and the House of Representatives, the USA Freedom Act to place more oversight and control on the NSA's monitoring activities to better protect the privacy of US citizens (Cohn & Reitman, 2015).

However, according to Pozen (2016), these privacy measures could result in so-called privacy-privacy trade-offs: protecting privacy along one axis could result in violating privacy along another axis (Pozen, 2016). In this way, privacy measures from governments could result in the opposite direction it was aiming for in the first place, namely to protect the privacy of their citizens.

This research uses the privacy-privacy trade-offs theory to test the reliability of its theoretical assumptions in an empirical context. Although the mentioning of privacy-privacy trade-offs is relatively new, its foundation could be traced back to ideas that have been discussed before, as scholars (e.g. Ross, 2002; Stuntz, 1999) already investigated how certain privacy aspects got increased protection from the police, while, as a consequence, other privacy interests lost their value. In this context, it is of importance to take into account the taxonomy of privacy discussed before, whereby privacy

functions as an umbrella term for different aspects of privacy. Moreover, privacy is not the only concept with internal oppositions: health, democracy, liberty, and security are examples of other concepts that have been investigated in different forms as these concepts could create clashes with itself (Holmes, 2009; Vermeule, 2008, Sunstein, 1996, Goodin, 2010). However, the term privacy-privacy trade-offs have until now only been mentioned by Henne & Smith (2013) and Pozen (2016).

Privacy-privacy trade-offs can occur in many different ways and forms. Pozen (2016) identified five different privacy-privacy trade-offs which could be the result from governmental policies: 1) *distributional trade-offs*, 2) *directional trade-offs*, 3) *dynamic trade-offs*, 4) *dimensional trade-offs*, and 5) *domain trade-offs*.

Firstly, distributional trade-offs could be considered as the ones whereby, because of a policy shift, the victims of privacy violations are shifted. This means that the privacy burden could be moved from one particular group of people to another one (Pozen, 2016). As example, if the police use ethnic profiling techniques, and they relocate policemen from a *white* neighbourhood to an area with a Muslim majority, these Muslims experience a significant increase of their privacy violations, while the people from the *white* neighbourhood experience the opposite (Strahilevitz, 2013).

The actor or party that violates the privacy can be a trade-off element as well (Pozen, 2016). For example, while you in the past bought a book in a bookstore, whereby the seller could exactly see which kind of books you read, this information is now collected by tech giants such as Amazon. The party or actor that could violate your privacy is in this way shifted from the bookseller to Amazon. These kinds of trade-offs are called directional trade-offs.

Thirdly, privacy risks could, following a change in policy, change across different time periods. This is called a dynamic trade-off (Pozen, 2016). The PreCheck program of the Transportation Security Administration (TSA) is an example of this, as people can "*leave on their shoes, belts and light outerwear and keep their laptops in their bags*" (Johanson, 2013, para. 1) which protects someone's privacy. However, in advance, one should give additional personal information to TSA to make use of this program (Johanson 2013).

Moreover, trade-offs can exist between the different dimensions that are present within the umbrella concept of privacy. In this way, following the framework of Solove (2006), targeting the privacy risk of interrogation could, as a countervailing effect, increase the violation of privacy via surveillance. These forms are called dimensional trade-offs (Pozen, 2016). A dimensional trade-off is called a domain trade-off when the trade-off risks are present between distinct domains (Pozen, 2016).

These five forms of privacy-privacy trade-offs are not exhaustive, and they could appear in a combination of different forms (Pozen, 2016). Still, these different forms of privacy-privacy trade-offs capture the key features of this phenomenon which makes them usable for analyses. The following section deals in-depth on how these trade-offs are used for the analysis in this research.

4. Researching Privacy in the US Intelligence Community: A Methodology

This research builds on the privacy-privacy trade-offs concept coined by Pozen (2016), and it uses the US intelligence community as the case to further investigate this phenomenon – it is thus a single case study. Yin (2009) defines this method as a research that discusses contemporary phenomenon within its real-life context, and whereby a variety of different sources could be consulted. This study tests the phenomenon of privacy-privacy trade-offs in the context of the intensifying debate regarding privacy, and especially with respect to the privacy issues within the intelligence community.

4.1. Case Selection

The case selected for this research is the US intelligence community. As it is the largest and most influential intelligence community in the world, it is of utmost interest to discuss the work of these agencies in further detail (Lowenthal, 2016). Although the NSA is the leading intelligence agency on SIGINT (NSA, n.d.), and therefore most used in this analysis, this study focuses on the US intelligence community as a whole.

Within the US intelligence community, particular focus of this research is given to the USA Freedom Act. This was signed in 2015 by former President Obama, and it has been called the biggest intelligence reform in the US since the adoption of the Foreign Intelligence Surveillance Act (FISA) in 1978 (Borggreen & Madhani, 2015; Swire, 2015). It is thus a landmark in the history of intelligence studies in the US. Moreover, the USA Freedom Act will expire in 2019 (Kelly, 2015) which means that this research could offer insights to policymakers in the evaluation of the current Act, and to improve the Act in the future.

Most changes in the USA Freedom Act has been made regarding to the collection of SIGINT data. As discussed in the literature review, SIGINT is the form of intelligence collection which bears the most critics from privacy advocates as a lot of (private) data is collected via these means (Solove, 2011). This research focuses on two different modes of data (metadata and content data) and on two broad forms of SIGINT (telephone communications and Internet communications). These two communication structures, and how the collection from intelligence agencies of these communications has changed after the USA Freedom Act, are analysed. Two particular Sections of the Act are analysed which deal with electronic communications. Firstly, Section 215 of the USA Patriot Act, which concerns the bulk collection of metadata of telephone communications, is analysed. This Section has been most debated after the Snowden revelations, because it violates privacy of innocent US citizens on a large scale (Medine, Brand, Cook, Dempsey, & Wald, 2014a). As a result, the USA Freedom Act did end this program (GPO, 2015). Secondly, Section 702 of the FISA Amendments Act is analysed, because the programs under this Section, PRISM and upstream collection, and its privacy harms have also been

discussed extensively (Medine, Brand, Cook, Dempsey, & Wald, 2014b). However, the USA Freedom Act did not act on these privacy concerns (Kadidal, 2016).

4.2. Case Study

Case study research can be done in many different forms. This study makes use of a combination of two; the illustrative case study and the critical incident case study. The former is more descriptive as it gives additional information or context to a given (new) concept (Hancock & Algozzine, 2016). As the privacy-privacy trade-off can be considered a new concept, the illustrative case study can be used in this research to explain the phenomenon to a broader audience.

To add exploratory research to the descriptive research of the illustrative case study approach, the critical incident case study method is applied on this research. This methodology studies variables, factors, and/or behaviours that are critical to the outcome, positive or negative, of a specific activity or event (Weatherbee, 2010). This method can therefore be used in the context of cause and effect relations. Moreover, as the name of the critical incident methodology suggest, it often criticizes a universal or generalized assumption. In this research, the assumption that the USA Freedom Act guarantees improved privacy protection is criticized, by identifying *incidents* in the form of privacy-privacy trade-offs. An incident can, in this context, be explained as a factor which was not been looked at before.

In this light, the two Sections discussed in this research measure the success or failure of the Act in providing the protection of privacy it tries to achieve. This means that the causes of the positive or negative sides of the Act are discussed in-depth considering privacy-privacy trade-offs.

4.3. Research Design and Sources

In case studies a variety of different sources can be examined to gain an extensive view of the case from multiple perspectives (Yin, 2009). This research makes use of multiple, both primary and secondary, sources. In the next chapter, the case, the US intelligence community, is discussed extensively.

Firstly, chapter 5 deals more broadly with the background of the US intelligence community until the USA Freedom Act. Mostly secondary resources are consulted in that part. Some information is derived from insights of whistleblowers.

Secondly, the USA Freedom Act itself is discussed. In this way, the factors which makes the content of the USA Freedom Act are examined. The differences to the USA Patriot Act are uncovered by doing so. The USA Freedom Act itself is used as a primary source in that section. Furthermore,

communication from the White House is included. Moreover, reports of review groups from former President Obama are used.

While aforementioned parts primarily make use of the illustrative case study, the critical incident study methodology comes into play in the discussion of Section 215 and Section 702.
All different sources that could add insights or data to the examinations of these programs are consulted, ranging from phone companies, Internet providers, whistleblowers, theoretical sources and others. Additionally, reports from the intelligence community itself are discussed. The Office of the Director of National Intelligence publishes, since 2014, yearly statistics about its use of FISA authorities and the way the intelligence community safeguards the privacy of US citizens. Following the USA Freedom Act, the Director of National Intelligence (DNI) is, by law, required to do so, including some of the statistics that were not stated in their first report(s). The *Statistical Transparency Report* about *Calendar Year 2017* (Office of the Director of National Intelligence [ODNI], 2018) is the newest version. These reports are used as the basis to analyse the trends on the numbers of targets and queries executed by the US intelligence community.

Following the exploration of the case study, the findings are analysed in connection with the taxonomy of privacy by Solove (2006) and the framework of privacy-privacy trade-offs by Pozen (2016) in chapter 6; both concepts have already been operationalized. Firstly, the analysis investigates if *dimensional* privacy-privacy trade-offs have occurred between Section 215 and Section 702. In other words, if US intelligence policy changes regarding Section 215 have had negative side-effects on the work of the intelligence community under Section 702. Secondly, Section 215 and Section 702 are separately analyzed to see if their implementation changed after the USA Freedom Act and consequently resulted in *distributional, directional, or dynamic* trade-offs (Pozen, 2016). *Domain* trade-offs are not analysed, because this research deals with telephone and Internet communications. These communications fall under the *surveillance* pillar from the taxonomy of Solove (2006). Hence, this research does not deal with Sections that are *incommensurate* from each other, which is a condition which is needed to be able to discuss a possible domain trade-off (Pozen, 2016; Sunstein, 1993). Lastly, other theoretical insights on the case study, connected with the academic debate on privacy-security, are given in chapter 6.

4.4. Limitations of Methodology

As with every research, limitations are present. First of all, the work of intelligence community is based on secrecy, which makes it harder to extract information from their work (Lowenthal, 2016). Fortunately, different whistleblowers (e.g. Snowden, Binney) revealed some information about the work of intelligence agencies in further detail (Lyon, 2014; Whittaker, 2015).

This research deals with one case, the US intelligence community, and the USA Freedom Act in particular. However, the study *only* analyses two specific sections of US intelligence law. In this respect, the results from the analysis do not necessarily lead to universally valid assumptions about privacy-privacy trade-offs existence in policy changes in the field of intelligence.

Moreover, this study is an explorative research of the phenomenon of privacy vs privacy trade-offs. As it is a relatively new theory, the framework is less reliable than theories which have been tested in a variety of case studies. Next to that, the trade-off element of *dynamic* trade-offs is time; as the time period which would result in these trade-offs could be longer then the time period of this research, this study cannot analyse this particular trade-off to its fullest.

5. The US Intelligence Community: A Case Study

Until now, the focus has been on the intelligence community in general, but it is now time to turn to the case of this study, and to discuss the US intelligence community in more detail. The purpose of this chapter is to present a complete picture about the work of the US intelligence community, especially after the USA Freedom Act, while taking into account the secrecy which still partially exist about the scope and operational work of these intelligence agencies.

5.1. Background US Intelligence community

The Japanese attack on Pearl Harbor in 1941 initiated the formation of the US intelligence community, and the first intelligence agencies were established soon after this attack. The attack came as a surprise, so the need for intelligence was clear; the US did not want to experience such surprises again (Lowenthal, 2016).

The National Security Act of 1947 laid down the legal basis of the intelligence community which created the Central Intelligence Agency (CIA), under the Director of Central Intelligence (DCI). In 1975, investigations showed that the CIA had violated its charter by spying on ordinary innocent US citizens, even if there was no relevance to the concern of national security (Jaeger, Bertot, & McClure, 2003). Before these investigations, the intelligence community was almost sacrosanct; it could never regain this status, and it had to learn to operate with less secrecy to maintain public's belief to keep the intelligence community as it is (Lowenthal, 2016). The investigations undermined public's trust in intelligence agencies. As a result of this, the Foreign Intelligence Surveillance Act (FISA) was adopted in 1978. The FISA was meant to protect the Fourth Amendment in the US which is the right of citizens to be free from unreasonable government searches and seizures (Jaeger, McClure, Bertot, & Snead, 2004). Since that moment, a surveillance warrant required the approval of a Foreign Intelligence

Surveillance Court (FISC). Only information that could relate to a criminal investigation was allowed to be intercepted (Jaeger et al. 2003). Between 1979 and 1999, the FISCs rejected none, and it granted 11.883 FISA warrants. This raises questions if the FISA really functioned as a judicial oversight of unreasonable searches and warrants of US citizens during these years (Jaeger et al., 2003).

5.2. The US Intelligence Community After 9/11

After the terrorist attacks of 11 September 2011, the intelligence community in the US significantly changed. These attacks had not been anticipated, just as the Pearl Harbor attack in 1941. This meant that the intelligence community had to change to avoid future surprises. The USA Patriot Act of 2001, adopted weeks after 9/11, allowed greater leeway for intelligence agencies and enabled them to collect as much data as they wanted for national security purposes (Lowenthal, 2016)

Mainly due to this increased freedom of intelligence agencies the NSA became the largest and most technologically sophisticated spy organization in the world (Bamford, 2008). In its constant drive for more information, the NSA enlarged its headquarters complex and other offices to store the data. Still, even considering that every year data can be stored on smaller flash drives, the NSA experiences problems in storing all its data, as it is drowning in it (Bamford 2008). The rents of the enormous *data storages* and the cohesive consumption of energy create a huge cost for the organization (Bamford, 2008). Moreover, it shows that NSA focuses on the collection of data, while whistleblower William Binney already mentioned that the organization had an ineffective *collect it all and figure it out later* mentality in 2001 (Whittaker, 2015). In the documentary *A Good American* (Moser, 2015), the former technical director of the NSA even argues that the organization had enough metadata to be able to link the relationship between the hijackers of 9/11 and to prevent it from happening if the NSA had adopted the analysing program ThinThread, which was developed by a small team in the NSA, including Binney. Instead, the NSA chose to buy and run the Trailblazer program in that time to be able to collect more SIGINT, including a lot of content of communications of ordinary citizens. Reason for this is that the NSA could earn more money when using Trailblazer. Basically, according to Binney, the NSA traded the security of US citizens to gain more money (Whittaker, 2015).

Moreover, two whistleblowers, Adrienne Kinne and David Murfee Faulk, revealed that NSA employers were busy with listening and laughing about intimate conversations of soldiers in Iraq from their offices in Fort Gordon, Georgia. If they did seriously listen to suspected relevant content, they made decisions without having followed the proper training. For example, an employee followed an education in the US in standard Arabic, but he or she could not completely understand the dialect spoken in Iraq and had to make life-and-death decisions based on one, out of context, conversation which took place in a country they had never been (Bamford, 2008). This could easily lead to making

the wrong interpretations and decisions, reinforcing scholarly critique as put forward by Lowenthal (2016) amongst others who argued that the intelligence community emphasizes too much on collection instead of making analyses more effective and reliable.

As a consequence of SIGINT, the *watch list* in the US, which contained twenty names in the past, already consisted of 1,2 million people in 2015 (Lyon, 2015). Many of them are innocent citizens and do not even know that they are on the list; they are on the list, because they were, for example, accidentally (often) at the wrong place at the wrong time, or they have an Arab/Muslim appearance and are therefore considered possibly dangerous (Ahmed, 2014; Guterman, 2013; Lyon, 2015). Results of being on the list are manifold. They could get a rejection, without any explanation, for loans to start a business or when applying for military academics, or they might be denied access to board a plane (Bamford, 2008). It could even affect the son or daughter of a person who is on the *watch list* (Bamford, 2008).

In 2006, Bazan & Elsea (2006) of the Congressional Research Service already expressed their concern about the NSA and their unprecedent increase in the collection of data. After a secret Presidential order in 2002, the NSA have been able to conduct some of its electronic surveillance without the need for warrants (Rollins & Liu, 2013). The erosion of civil liberties and privacy did not mean that terroristic attacks could be stopped. On the contrary, research has indicated that the SIGINT programs, which are too focused on collecting data instead of analysing the data, did not avoid any act of terrorism (e.g. Whittaker, 2015; Fussey, 2015)

Although concerns about the ever-increasing urge for more information from intelligence agencies grew among privacy advocates and scholars, this topic only gained attention in the public debate after the Snowden revelations of 2013. From June 2013 onwards, Snowden revealed different classified documents which showed the secret surveillance work the NSA was doing (Lyon, 2014). The first document showed that the FISC had required Verizon, the biggest telecommunication provider in the US, to give the metadata of millions phone calls within the US to the Federal Bureau of Investigation (FBI) and the NSA (Greenwald, 2013). In this way, it became clear the FISCs are not that critical on giving away their warrants, as showed earlier by Jaeger et al. (2003).

Furthermore, Snowden revealed that the NSA could have direct access to the data of big technology companies, such as Facebook, Google and Microsoft (Lyon, 2014). In the PRISM program, the NSA worked together with these tech giants to bypass privacy of ordinary citizens in the US (Gellman & Poitras, 2013). In this way, they could intercept data from Internet traffic and communications. As a response on the public debate about the privacy violations of intelligence agencies in the US, the Obama administration adopted in 2015 the USA Freedom Act.

5.3. USA Freedom Act

The '*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015'* is the full name of the so-called *USA Freedom Act* (GPO, 2015). The aim of the Act is described as follows: "*to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes*" (GPO, 2015, p.1). The White House adopted the Act in June 2015 to uphold the right to privacy and civil liberties, while making sure to keep the Americans safe (The White House, 2015).

Two commissions have been the basis for the reforms taken in the USA Freedom Act; The Privacy and Civil Liberties Oversight Board, established in 2004 but releasing its first report ten years later, and President Obama's Review Group on Intelligence and Communications Technologies (Medine et al., 2014; Clarke, Morell, Stone, Sunstein, & Swire, 2014). The latter was formed by President Obama two months after the Snowden revelations (Office of the Director of National Intelligence [ODNI], 2013), and it consisted of five members with different and complementary capabilities (Swire, 2015). Its mission has been to form recommendations to better safeguard privacy, civil liberties, and security in the rapidly changing world (Clarke et al., 2014). In a short amount of time, they developed 46 concrete recommendations to enhance the protection of these concepts (Clarke et al., 2014). The most attention has been given to the chapter which dealt with section 215 of the USA Patriot Act. Section 215 authorized the bulk data collection of phone records of US citizens (GPO, 2001). The Review group criticized the bulk collection: "*our review suggests that the information contributed to terrorist investigations by the use of Section 215 telephony metadata was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional Section 215 orders"* (Clarke et al., 2014, p.57). This means the bulk collection of these data did not improve the national security. In line with this, the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency established in 2012, showed that the bulk collection was duplicating FBI's own information gathering methods. In this way, the bulk collection did not create any additional value to the national security of the US (Medine et al., 2014). In the report of the PCLOB to improve the intelligence community and their protection of civil liberties and privacy, they therefore state: "*The government should end its Section 215 bulk telephone records program"* (Medine et al., 2014, p.16).

Following the recommendation from the Review Group and the PCLOB, the USA Freedom Act ended the bulk collection of metadata from phone records. While the Review Group already showed that the bulk collection did not make the country safer, the PCLOB has three additional arguments against the bulk collection (Medine et al., 2014). Firstly, the statute states that collection can only occur when it is *relevant* to an FBI investigation and the phone records that are collected in-bulk, unlimited

in scope, cannot be seen as *relevant*. Secondly, phone companies are obligated, by this program, to provide the calling records as they are generated directly to the NSA, which lacks foundation in the statute. Lastly, the bulk collection infringes the Electronic Communications Privacy Act (Medine et al, 2014).

Next to the breaches of the statute and the uselessness of the information gathered by the bulk collection of phone records, it violates the privacy of US citizens. Metadata of one phone call would not have enormous impact on person's individual privacy. However, if the government collects and stores all phone records of one person of the last five years, much more can be revealed about an individual, including intimate details (Medine et al., 2014). As a consequence, a *chilling effect* could occur as behaviour of an individual can be altered or even restricted (Michelman, 2009). Moreover, the government could use this data for different purposes than keeping the nation safe (Solove, 2006).

Although the end of the bulk collection of the metadata of phone records is seen as the largest difference of the USA Freedom Act in comparison to the USA Patriot Act, it is not the only amendment. As recommended by the Review Group and the PCLOB, transparency measures have been taken. To be specific, greater reporting requirements have been established to increase Congressional oversight. As a result, the number of orders to phone companies to share their (meta)data of a particular phone number or other specific search term have to be made public every year (GPO, 2015; Ombres, 2015). Moreover, some reforms have been taken regarding to the FISC. Following the USA Freedom Act, stronger requirements should be met to be able to obtain a FISC order (GPO, 2015; Ombres, 2015).

However, not all recommendations put forward by the Review Group and the PCLOB have been adopted in the USA Freedom Act. Earlier, several proposals had been suggested to make sure that at the FISC, a privacy advocate would be present on each order to defend the civil liberties and privacy interests of individuals (Fram, 2014). However, this proposal did not end up in the USA Freedom Act (GPO, 2015). Moreover, the lone wolf surveillance authority, which tells that the intelligence community has a mandate to follow individuals without having a lot evidence against them, has been extended (Clarke et al., 2014; The Washington Post, 2015). Furthermore, the roving wiretap is still in place. This makes sure that communication of a target can be followed, without losing this authority when a target throws away its phone (The Washington Post, 2015). In order words, an individual can be selected as target instead of selecting a specific device of the target, such as a phone number. Lastly, little has changed in the collection of data in the cyberspace which is still based on Section 702 of the FISA Amendments Act of 2008 (e.g. Ombres, 2015; Suarez, 2017). In this way, the intelligence community can, in-bulk, intercept international Internet communications (Gorski & Toomey, 2016). The extension of Section 702, and its consequences, are discussed later in this chapter.

5.4. Telephone Metadata Collection under Section 215 of the USA Patriot Act

As the bulk collection of Call Detail Records (CDRs) has been explicitly prohibited by the USA Freedom Act, the metadata stay, since then, with the phone companies. This means that the data is not stored on a central place by the intelligence community anymore, but on decentralised locations by the variety of telecom providers present in the US. The NSA needs an order from the FISC, when "*there is a reasonable, articulable suspicion"* (GPO, 2015, Sec. 101. Additional Requirements for Call Detail Records, para. C, ii) that the seed is on any way linked to international terrorism. After the allowance of the FISC, telecom providers are required to turn over the CDRs, both historical ones as new logs popping up, from the particular seed (ODNI, 2018).

Before the USA Freedom Act, "*NSA potentially collect[ed] billions of records per day with full knowledge that virtually all of them are irrelevant"* (Medine et al., 2014, p. 73). This number has significantly lowered, as it decreased to 151 million CDRs in the whole of 2016 (Office of the Director of National Intelligence [ODNI], 2017). However, it is important to note that *only* for 42 targets a FISC order has been obtained in 2016 to collect the CDRs, and as such, there is a large amount of CDRs collected from these targets (ODNI, 2017; Savage, 2018a). The reasons for this are manifold. First of all, FISC orders allow two hops collection of CDRs; this means that all the metadata of every person the target has been in contact with is collected as well. Secondly, some calls generate more CDRs, because the calls of users on the move could be handled by different cell towers. Thirdly, metadata of calls and text messages could be duplicated as a call between a customer of Verizon and a AT&T customer generates CDRs at both telecom providers (ODNI, 2017; Savage, 2018a).

However, the large difference has even increased in 2017 (ODNI, 2018). While less orders have been obtained (40 targets), the intelligence community collected more than 534 million CDRs; this is thrice to four times as more as in the year before. In the *Statistical Transparency Report* (ODNI, 2018), no explanation has been given to this rise. Coldewey (2018) speculates that it would just be possible that the targets in 2017 had much longer contact lists and a wider network than the ones in 2016. Another speculation could be that, as a normal FISC order is 180 days valid (NSA Civil Liberties and Privacy Office [NCLPO], 2016), orders have been extended more times in 2017. However, this is all speculation, as no information was given in the Transparency reports. In response to the questions raised, Alex Joel, the Civil Liberties Protection Officer of the ODNI, stated that *"NSA has not reinterpreted its legal authorities to change the way it collects such data*" (Savage, 2018a, para. 3).

Nevertheless, on 28 of June 2018, the NSA publicly reported that they collected some CDRs without any authority to receive it, because of *technical irregularities*. Officials of the NSA discovered the irregularities in the beginning of 2018. It is, until now, unclear what these technical irregularities exactly entailed (NSA, 2018). As a consequence, the NSA began, in May 2018, to delete all the metadata from millions of phone records which have been acquired since the adoption of the USA Freedom Act

in 2015 (Savage, 2018a). Glenn Gerstel, the NSA's general counsel, said it was infeasible to try to identify the mistakes and to delete only the contaminated CDRs.

It is unclear what caused the technical irregularities and what they exactly include, but it is clear that the NSA received information from the phone companies it was not authorized to receive. Ron Wyden, Democratic Senator of Oregon and member of the Senate Intelligence Committee, argues that phone companies have made mistakes which led to technical irregularities (Savage, 2018a). One should understand the increased responsibilities phone companies had to work on after the adoption of the USA Freedom Act which resulted in a more complex situation. Under the USA Patriot Act, the NSA stored all the data itself, and it did so-called *contact chaining* when a query was made, to show connections between phone numbers to identify the one-hop and two-hop connections of the seed number of the query (Kris, 2018). In this way, the NSA bore the responsibility of the exploitation of the collected data. However, this changed after the USA Freedom Act, as the responsibility for collecting and exploiting data was moved to phone companies. They had to collect and share metadata, and, less known but not less important, these companies had to exploit the data to make it ready for analysis by NSA. This created the complex situation; as phone companies only have the data of their own subscribers, the NSA has to consult multiple phone companies to receive all the two-hop metadata (Kris, 2018). This makes the exploitation of the metadata by phone companies both more labour- and time intensive. Moreover, these companies did not have the responsibilities of this work before, which could mean that the expertise to exploit the data was not present. In this respect, the technical irregularities show that the shift of responsibilities of the storage and exploitation of data from the NSA to phone companies resulted in problems. This includes privacy harms as much more metadata of ordinary US citizens was shared with the NSA than was authorized by the USA Freedom Act.

Another negative side-effect of the USA Freedom Act, is, while less CDRs are shared with the NSA, the intelligence community could, with a FISC order, query more easily metadata from cell phones. During the USA Patriot Act, the NSA collected all landline CDRs, but not all CDRs from cell phones. Mainly because FISC orders did not allow for the collection of location data, phone companies could not share CDRs from cell phones as it would include location data. From 2011 onwards, AT&T started to share CDRs with the NSA (1,1 billion CDRs a day), as they stripped of the location data (Angwin et al., 2015). However, there has not been any evidence that Verizon, the biggest phone company in the US, shared the CDRs of cell phones as they did not want to, or it was too much work to, strip off the location data (Angwin et al., 2015). Since the adoption of the USA Freedom Act, phone companies are required to share metadata, including CDRs of cell phones, to the NSA when a *seed* is identified and a FISC order is put in place. Location data is still excluded from the CDRs, and is, as such, stripped of by the phone companies (GPO, 2015).

5.5. Internet Content Collection under Section 702 of the FISA Amendments Act

While the metadata of phone communications is handled by Section 215, the legal framework regarding the collection of the content of the calls are set up by Section 702 of the FISA Amendments Act. However, Section 702 is more known of the Internet content data the intelligence community collects under this Section (Medine et al., 2014b). Although the exact division between Internet and phone data collected is unknown, this section assumes, following Medine et al. (2014b), that the vast majority of the data is obtained from Internet communications. Furthermore, all data collected under Section 702 is data which includes content and, as such, when this section speaks about *data,* this is data including the content of communications. Section 702 of the FISA Amendments Act has not been touched upon by the USA Freedom Act (GPO, 2015). Still, it is interesting to investigate what this means for the work of the US intelligence community, and if the scope of the work under Section 702 has changed after the USA Freedom Act.

Under Section 702, foreign persons who are not residing within the borders of the US and have been in, or are in, contact with persons who possess *foreign intelligence information* are targeted (Hanssen, 2016). This could be suspected terrorists, but also journalists and human rights researchers (Gorski & Toomey, 2016). Moreover, when a foreigner is communicating with an American, the intelligence community collects these electronic communications as well. It does not need a warrant to do this (Savage, 2018a).

Two collection forms take place under the program; downstream collection and upstream collection. Downstream collection is primarily known under its code name PRISM. Under this program, the NSA could collect SIGINT from an US-based electronic communications service provider (Medine et al., 2014b). In this way, NSA collected data directly from US-based servers from providers such as: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple (Fidler, 2015; Greenwald & MacAskill, 2013). The NSA only needs to give a *selector* to, for example, an Internet service provider, and the intelligence agency gets the content of all the Internet communications that the selector participates in (Medine et al., 2014b). A selector can be an email address, but cannot be the names of the targets, and it cannot contain key words, such as *terroristic attack*. Copies of data collected may be shared with the CIA and/or FBI (Medine et al., 2014b).

Upstream collection works in a different way. While the use of *selectors* to target particular email addresses works the same as with the PRISM program, the way the SIGINT is collected differs. Collection occurs with the help of the providers that control the transit of the telecommunications (Medine et al., 2014b). In other words, the NSA can via this way collect SIGINT directly from fiber cables. All the telephone communications which are *from* or *to* the *selector* could be acquired (Medine et al., 2014b). This is the same as in the PRISM program. However, the NSA could obtain even more SIGINT. It can, next to acquire Internet communications *from* or *to* the *selector*, also Internet

communications *about* the specified *selector*. This means that if the *selector*, an email address, is written in the content of a mail, even if the *selector* is not part of the mail conversation, the mail can be collected by the NSA. Moreover, Internet communications *about* the *selector* could involve Internet activity (e.g. website browsing) of the person who is targeted (Medine et al., 2014b). In this way, *about* communications reveals much more data about a specific target.

All this information can be searched through by the NSA without a warrant (Gorksi & Toomey, 2016). Moreover, even Internet communication between two US-based persons could be obtained if the SIGINT flows (intentionally or not) through a foreign server (Medine et al., 2014b). While the PCLOB showed that NSA acquired around 26,5 million Internet communications in 2011 alone as a result of the Upstream collection (Medine et al., 2014b), Gorski & Toomey (2016) contend that the only way to collect the information the NSA seeks to receive, is to make a copy of almost all Internet communications. This would entail trillions of Internet communications (Gorski & Toomey, 2016).

It is unclear how many electronic communications the NSA actually collects nowadays, however, the intelligence community reveals the numbers of their targets and searches they execute during the year in their *Statistical Transparency Reports*. Combining the downstream (PRISM) and upstream collection, the NSA selected 129.080 targets, non-US persons, in 2017 to obtain their electronic communications via Section 702 (ODNI, 2018). This is a large increase from the years before. From 2013 onwards, a rise is seen in the numbers of the targets under Section 702. In 2015, 5,9% more targets have been aimed at in comparison with 2013. After the USA Freedom Act, this grew further accelerated; the numbers of 2017 are an enormous increase of 36,8% compared to the figures of 2015 (ODNI, 2018).

The same development holds true for the number of search terms which concerned a known US person. While this number was 4.672 in 2015, the figure rose to 7.512 in 2017; an increase of 60,8% (ODNI, 2018). This means that of these 7.512 US-persons, all electronic communications have been possibly searched through by the US intelligence community (ODNI, 2018).

Although privacy and civil liberties advocates pushed for more warrant requirements under Section 702, the USA Freedom Act did not change its legal framework. In 2018, Congress further extended Section 702 until 2023 without any amendments (Savage, 2018b).

6. Privacy-Privacy Trade-Offs after the USA Freedom Act: An Analysis

In the previous chapter, the Intelligence community in the US has been thoroughly discussed, especially the reforms in the USA Freedom Act and Sections 215 of the USA Patriot Act and 702 of the FISA Amendments Act. The mentioned practices, implementations, and figures showed different (negative) side-effects of the adoption of the USA Freedom Act. Some of them have caused a privacy-privacy trade-off. This chapter delivers analytical insights on the amendments made in the USA Freedom Act and what privacy-privacy trade-offs have occurred so far. The analysis shows that three of all the privacy-privacy trade-offs forms laid out by Pozen (2016) are present, namely: dimensional, directional and distributional ones.

6.1. Dimensional Privacy-Privacy Trade-Offs

Firstly, the analysis shows, considering the taxonomy of privacy made by Solove (2006), that the privacy measures taken in the USA Freedom Act have created dimensional privacy-privacy trade-offs. Privacy interests are the traded-off element in these privacy-privacy trade-offs (Pozen, 2016). There did not occur a privacy-privacy trade-off *between* dimensions, but *within* the dimension of surveillance, which is part of the category of information collection in the operationalization of privacy by Solove (2006, 2008).

Collection of Internet communications and telephone communications can both be grouped under the dimension of surveillance, as surveillance can be explained as the use of *spy eyes* by the intelligence community to gain information about actions and intentions of individuals (Solove, 2006). These *spy eyes* could be used to monitor electronical communications, such as CDRs and Internet communications.

While the USA Freedom Act resulted in a marginal gain of privacy regarding the collection of telephone communications under Section 215, a marginal loss of privacy occurred in the collection of Internet communications under Section 702. Following the USA Freedom Act, much less CDRs are stored by the NSA. However, much more targets have been determined under Section 702 to collect data of mainly Internet communications. Above all, this holds true for US citizens as an increase of more of 60% is seen of the searches on US persons under Section 702 between 2015 and 2017. This could indicate that the US intelligence community has innovatively looked for a new approach to be able to receive data, and analyse this information, about US citizens.

Furthermore, another privacy interest has been traded-off by the new approach of the US intelligence community, namely: from metadata to content data. As shown, the end of bulk collection of phone communications resulted in collecting more Internet data of individuals. While the bulk collection under Section 215 consisted of metadata, the collection under Section 702 deals with

content data. Although scholars (e.g. Kadidal, 2016; Lowenthal, 2016) have argued that analysing metadata is much easier, and, as such, more effective than content data to identify possible suspects and their networks, the US intelligence community has focused more on content data after the USA Freedom Act.

Consequently, two dimensional trade-offs occurred after the adoption of the USA Freedom Act (Table 6.1.), because of an expanded implementation of Section 702 by the US intelligence agencies. In other words, the USA Freedom Act sparked incentives to the intelligence community to think about other possible ways to increase their collection. Solove (2011) already argued that the intelligence community tries to collect as much data as possible, and, as large facilitates already have been built by NSA to store data, searching for other ways to still collect data was an obvious road to take from their perspective. Expanding their data collection program under Section 702 has been one of these effects.

Trade-off Type	Traded-Off Element	From	To
Dimensional	Privacy Interests	Phone communications	Internet communications
Dimensional	Privacy Interests	Metadata	Content data
Directional	Privacy Violators	Intelligence agencies	Phone companies
Distributional	Privacy Victims	Non-US persons	US-persons

Table 6.1. Privacy-privacy trade-offs which occurred after the USA Freedom Act.

As table 6.1. shows, two other privacy-privacy trade-offs have occurred after the adoption of the USA Freedom Act. These trade-offs will be discussed separately. Firstly, Section 215 will be discussed which shows the directional trade-off as a result of the end of the bulk collection of phone records. Secondly, attention will be given to the expanding nature of the interpretation of the intelligence community regarding Section 702 which resulted in a distributional trade-off.

6.2. Privacy-Privacy Trade-Offs: End of Bulk collection of CDRs under Section 215

As a consequence of the USA Freedom Act and its changes to Section 215, the US intelligence community could not, in-bulk, collect CDRs anymore. Since 2015, the responsibility has shifted from the intelligence community to telephone companies. This means metadata of CDRs is not stored on one central place anymore, but on decentralised locations by phone companies. Moreover, phone companies have been taxed with the task to exploit the data to make it ready for analysis by the intelligence agencies. As exploitation is much harder for phone companies as it does *only* collect the metadata from their own subscribers, a complex situation emerged. This complex situation could have

led to the technical irregularities which are discussed in the previous chapter. This error has showed two things. First, exploitation of data has been much more complex under the USA Freedom Act. Second, the expertise to exploit the metadata in the correct way has not been present among the phone companies.

As, regarding to the collection, storage and exploitation of CDRs, the responsibility has shifted from the NSA to the phone companies, and privacy harms have been the result, a directional privacy-privacy trade-off occurred. Pozen (2016) identified *directional trade-offs* as the privacy harms that occur when the actor who violates privacy shifts. These privacy harms caused by phone companies are seen in the example of the technical irregularities. However, this example only points to a much broader problem. The safety expertise to protect the data and to exploit the data of the CDRs has not been present among the phone companies on a scale it was when this was dealt with by the NSA. Moreover, an enormous increase is seen in 2017 compared to 2016 on the CDRs which are handed over to the NSA, while the technical irregularities have already been present since 2015; this could show that the US intelligence community has found innovative ways to bypass the restrictions made in the USA Freedom Act. In this way, the traded-off element of privacy violators resulted in privacy harms, while it was done to do the opposite; to better safeguard privacy of US citizens.

Distributional trade-offs happen, according to Pozen (2016), when some individuals or groups lose more privacy, while other experience a marginal gain of their privacy. The victims of the CDRs collected by the NSA are people who are suspected of having links with international terrorism, or people who are in contact with these suspects. In this way, there have been less *victims* of privacy harms than in the years before the USA Freedom Act. However, the *technical irregularities* showed that CDRs of people who did not fall in the category mentioned above have been obtained by the NSA since 2015. In this way, between 2015-2018, the US intelligence community could use these CDRs, which could belong to ordinary and innocent citizens, for their analyses. As it is unclear which CDRs exactly have been unprecedented collected by the NSA, it is unknown if a distributional trade-off occurred after the USA Freedom Act under Section 215.

The same conclusion is stated concerning dynamic trade-offs. Pozen (2016) identified these trade-offs as the ones that change privacy risks across time periods. A theoretical example would be that the USA Freedom Act, with its privacy measures, produces a too complex system, which is more labour intensive, increases costs, and makes more room for mistakes or technical irregularities, which would eventually result in making new policies. When these new policies set up a system which is worse, in respect to privacy, than before, a dynamic trade-off can be identified. As there have not been any amendments of the USA Freedom Act until now, it is yet unclear if a dynamic trade-off will emerge.

6.3. Privacy-Privacy Trade-Offs; Expanded Interpretations and Implementations under Section 702

The USA Freedom Act did not change the operational work of the intelligence agencies under Section 702, however, in the response of the end of bulk collection of CDRs, the intelligence community expanded its interpretation and implementation of Section 702. Following the *Statistical Transparency Report* of 2017 (NSA, 2018), more targets have been determined in the last years. However, the amount of Internet data and communications collected by the US intelligence community is unclear. This is still shrouded in secrecy, or just unknown. Moreover, it is hazy to differentiate the scope of the two programs operated under Section 702: the PRISM program and the upstream collection.

Following the end of bulk collection of phone records, the US intelligence community expanded its scope under Section 702 which resulted in a distributional trade-off: it used more information from US citizens, collected under Section 702, in their analysis than before the USA Freedom Act. Although original goals under Section 702 of the FISA Amendments Act focus on non-US targets, search terms of US persons have significantly increased (by more than 60%) in 2017 compared to 2015 (ODNI, 2018). This shows that the intelligence community tries to gather more information about US persons than it did in the past. Given the context of the prohibition of bulk collection of CDRs, the US intelligence community have shifted their attention to Internet communications via this Section to obtain the information of their own citizens that it is looking for.

As the actor that violates the privacy did not change (intelligence agencies), there has not been any inducement to argue that a directional trade-off occurred in Section 702. As mentioned earlier, dynamic trade-offs are hard to discuss as these trade-offs could occur in the future. However, to this moment, no evidence has been there either that could point to such a trade-off. Moreover, as Section 702 has not been revised the last years, the probability of a dynamic trade-off is less present compared to the revised Section 215.

6.4. Privacy Measures in the USA Freedom Act

Although aforementioned privacy-privacy trade-offs showed (unintended) negative side-effects of the USA Freedom Act, some privacy measures taken in the Act resulted in better safeguarding the privacy interests of US citizens. Firstly, transparency measures have been taken, such as the requirement for the intelligence community to present different statistics in their yearly Transparency Reports (GPO, 2015; ODNI, 2018). Secondly, more oversight has been put in place to obtain a FISC order (GPO, 2015; Ombres, 2015).

However, these measures do not directly contribute to protecting privacy of US citizens, e.g. it does not safeguard "*the right to be left alone"* (Espinosa, 2012, p. 969) as privacy has been interpreted by privacy law standards. Still, it makes the policies of the US intelligence community better

discussable. In this way, these measures could, to some extent, prevent intelligence agencies in just collecting whatever they can.

Moreover, the case study showed that light has been shed on the collection phase of intelligence with the end of bulk collection under Section 215 as paramount example. However, less attention has been given to the processing and analysing phase of the intelligence cycle. Following the taxonomy of Solove (2006), privacy harms occur during these phases as well, seen in the forms of queries and secondary use of data (Solove, 2011). This part has been missing in the USA Freedom Act.

Lastly, many privacy harms have not be touched upon by the USA Freedom Act, including the lone wolf surveillance authority, and the roving wiretap mandate. Furthermore, the proposal to have a privacy advocate at the FISC on every order did not end up in the Act.

6.5. Privacy-Security Antinomy?

Following the technical irregularities observed by NSA employees, they decided to delete all the CDRs collected since 2015. This shows that the deletion of these records did not increase risks of the national security, as avoiding national failures should be the main task of these intelligence agencies (Gazis, 2018; Tucker, 2014).

In this way, this example fits within the argument of different scholars (e.g. Solove, 2011; Dragu, 2011) that there is not such a thing as a zero-sum game between the concepts of privacy and security. It is therefore useless for the intelligence community to just collect whatever they are able to collect from a national security perspective (Solove, 2011). There are better ways to increase the security, while preserving the privacy and civil liberties of citizens. Firstly, the intelligence community could make more use of HUMINT, spies and informants, instead of the surveillance via SIGINT (Fussey, 2015). A good practice is seen in the work by Mubin Shaikh, an informant, and former extremist, who foiled the terrorism plot of the 'Toronto 18' (Speckhard & Shaik, 2014). Secondly, intelligence agencies could put more emphasize on the analysis step of the intelligence cycle, as in many instances finishing the puzzle is more crucial compared to finding new puzzle pieces (Fussey, 2015; Lowenthal, 2016). As shown earlier, the puzzle pieces of the terroristic attacks on the US (9/11), Paris and London were already in possession of the intelligence community, however, the puzzle could not be finished before the attacks happened (Fussey, 2015; Moser, 2015). In conclusion, the response of the NSA to the *technical irregularities* adds evidence to the notion of Solove (2011) and others that privacy harms do not necessarily lead to additional security.

7. Conclusions and Discussion

This research dealt with privacy-privacy trade-offs after the adoption of the USA Freedom Act. Dimensional, directional and distributional privacy-privacy trade-offs have occurred after the adoption and implementation of this Act in 2015. The study shows that the unchanged US intelligence policy of Section 702 from the FISA Amendments Act have been implemented and interpreted in a broader manner after the changes in the USA Freedom Act on Section 215 of the USA Patriot Act. Consequently, the intelligence community switched its focus under Section 702 from the collection of phone communications to Internet communications, and from collecting metadata to content data (*dimensional* trade-offs). Furthermore, the victims of privacy have, under Section 702, changed considerably. Although privacy violations are still made to non-US persons to receive foreign intelligence information, the information queried from US-persons has grown exponentially and is used for multiple analyses (*distributional* trade-off). Next to the privacy-privacy trade-offs under Section 702, a *directional* trade-off occurred under Section 215. The actor that violates privacy under Section 215 has changed: the intelligence agencies were storing all the data, but this responsibly now lies by phone companies. Consequently, exploitation of metadata has been more labour- and time intensive. Moreover, expertise about exploitation of metadata has not been present at phone companies, which possibly have led to the disclosure of the *technical irregularities* and the cohesive privacy harms that occurred.

The study has shown that policies made under the Obama administration to safeguard privacy, through the adoption of the USA Freedom Act, led to changed interpretations of other legislations which actually created violations to privacy. Hence, the possibility of privacy-privacy trade-offs after a change in policies, which this study exposes with respect to its presence after the USA Freedom Act, has not been considered in the decision making. This observation points to multiple lessons for the future. Firstly, it shows that all stakeholders present in the process of decision-making should take into account these, often forgotten, (indirect) side-effects of policy-making. Secondly, it uncovers the importance to focus on integrated policymaking strategies instead of 'separate', or ad-hoc, policymaking. These lessons should be incorporated in the decision making of the extension of the current USA Freedom Act, which will take place at the end of 2019.

From an academic perspective, as the concept of privacy has still not been well understood, more and new theoretical studies on its components are very welcome, including research on the concept of social privacy which is more relevant than ever before considering the globalisation of communications. Then, new categories of privacy violations could be exposed in the future. This can lead to a better understanding of the privacy-security antinomy. Nationals risks will be present in the future, as a *zero-risk society* is an illusion. However, the intelligence community should protect the

nation and adapt to societal impacts such as new technologies, without having too many impacts on the society itself (e.g. by using surveillance techniques initiating a *chilling effect*). To prevent the latter from happening, it is of paramount importance to better understand privacy, and the phenomenon of privacy-privacy trade-offs.

As the theory of privacy-privacy trade-offs is relatively new, it is of utmost importance to test and validate the framework in a variety of studies. Future research could further analyse the trend of the numbers given in the transparency reports of the intelligence community. However, the theory can be useful in other fields than intelligence as well. Moreover, new theoretical research on privacy-privacy trade-offs could present new trade-off elements that should be taken into account; the five privacy-privacy trade-offs laid out by Pozen (2016) do not necessarily give a complete picture of the phenomenon.

All in all, this study provides new insights to policymakers, scholars, security officials, privacy advocates, and citizens on the broad range of privacy topics and issues, and primarily on privacy problems in the intelligence community. Privacy should stay on the agendas of the international community, because it is an important guarantor of other human rights. The process of policymaking should incorporate many views and interpretations to be aware of the privacy with all its facets. Then, policymakers can prevent privacy-privacy trade-offs from happening and they can actually realize to better safeguard the privacy and civil liberties of the people.

Bibliography

Agrell, W. & G.F. Treverton (2015), *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*. Oxford University Press.

Ahmed, S. (2014), *The Cultural Politics of Emotion*. Edinburg University Press, pp. 62-81. DOI: 10.3366/j.ctt1g09x4q.

Aid, M.M. (2014), Measurement and Signature Intelligence. In R. Dover, M.S. Goodman & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies*. Routledge.

Amnesty International (2018), Trapped in the Matrix: Secrecy, Stigma, and Bias in the Met's Gangs Database. *Amnesty International United Kingdom Section.*

Andregg, M. (2016), Ethical Implications of the Snowden Revelations. *The International Journal of Intelligence, Security, and Public Affairs*, vol. 18 (2), pp. 110-131. DOI: 10.1080/23800992.2016.1196942.

Angwin, J., J. Larson, C. Savage, J. Risen, H. Moltke & L. Poitras (2015), NSA Spying Relies on AT&T's 'Extreme Willingness to Help'. *ProPublica*. Retrieved from: https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help. Accessed on: 29-01-19.

Baker, S.A. (2013), *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism*. Hoover Press.

Bamford, J. (2008), *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America.* New York: Doubleday.

Bazan, E.B. & J.K. Elsea (2006), Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information. *Congressional Research Service*.

Bennett, C.J. & C.D. Raab (2006), *The Governance of Privacy*: *Policy Instruments in Global Perspective*. The MIT Press.

Bloustein, E. (1964), Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review,* vol. 39, pp. 962-1007.

Borggreen, C. & B. Madhani (2015), What the USA Freedom Act Does – And Why It Matters for Europe. Retrieved from: https://www.ccianet.org/2015/06/what-the-usa-freedom-act-does-and-why-it-matters-for-europe/. Accessed on: 29-01-19

Bratman, B. (2002), Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy. *Tennessee Law Review*, vol. 69 (3), pp. 623-652.

Cadwalladr, C. & E. Graham-Harrison (2018), The Cambridge Analytica Files. *The Guardian*. Retrieved from: http://davelevy.info/Downloads/cabridgeananalyticafiles%20-theguardian_20180318.pdf. Accessed on: 29-01-19.

CBS News (2015), China tests 'social credit score' system to crack down on critics. Retrieved from: https://www.cbsnews.com/news/china-communist-party-social-credit-score-silence-critics/ Accessed on: 29-01-19.

CIA (1983), *Fact Book on Intelligence*. Washington, DC: CIA.

Clarke, R.A., M.J. Morell, G.R. Stone, C.R. Sunstein & P. Swire (2014), *The NSA Report: Liberty and Security in a Changing World: The President's Review Group on Intelligence and Communications Technologies*. Princeton University Press: Princeton and Oxford.

Cohen, J.E. (2012), *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

Cohn, C. & R. Reitman (2015), USA Freedom Act Passes: What we Celebrate, What we Mourn, and Where we Go From Here. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here Accessed on: 29-01-19.

Coldewey, D. (2018), NSA Triples Metadata Collection Numbers, Sucking up Over 500 Million Call

Records in 2017. *Tech Crunch.* Retrieved from: https://techcrunch.com/2018/05/04/nsa-triples-metadata-collection-numbers-sucking-up-over-500-million-call-records-in-2017/. Accessed on: 29-01-19.

Combs, M.I. (1987), Shared Privacy and the Fourth Amendment, or the Rights of Relationships. *California Law Review*, vol. 75 (5), pp. 1593-1664. DOI: 10.2307/3480488.

Dover, R., M.S. Goodman & C. Hillebrand (2014), *Routledge Companion to Intelligence Studies.* Routledge.

Dragu, T. (2011), Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention. *The American Political Science Review,* vol. 105 (1), pp. 64-78. DOI: 10.1017/S0003055410000614.

Espinosa, M.J.C. (2012), Privacy. In M. Rosenfeld & A. Sajó (eds.), *The Oxford Handbook of Comparative Constitutional Law.* Oxford University Press. DOI: 10.1093/oxfordhb/9780199578610.013.0048.

Fidler, D.P. (2015), *The Snowden Reader*. Bloomington, IN: Indiana University Press.

Fram, R.D. (2014), A Public Advocate for Privacy. *Inside Privacy*. Retrieved from: https://www.insideprivacy.com/united-states/a-public-advocate-for-privacy-1/. Accessed on: 29-01-19.

Fussey, P. (2015), After Paris, It's Traditional Detective Work that Will Keep us Safe, not Mass Surveillance. *The Conversation*. Retrieved from: https://theconversation.com/after-paris-its-traditional-detective-work-that-will-keep-us-safe-not-mass-surveillance-50830. Accessed on: 29-01-19.

Gazis, O. (2018), Trump Calls out NSA for Deleting Data: Here are the Facts. *CBS News*. Retrieved from: https://www.cbsnews.com/news/trump-calls-out-nsa-for-deleting-data-here-are-the-facts/ Accessed on: 29-01-19.

Gellman, B. & L. Poitras (2013), US, British Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program. *The Washington Post*. Retrieved from:

https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Accessed on: 29-01-19.

Gibson, S.D. (2014), Open Source Intelligence. In R. Dover, M.S. Goodman & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies*. Routledge.

Glendon, M.A. (2011), Advising the Prince: The Enigma of Machiavelli. In M.A. Glendon (ed.), *The Forum and the Tower: How Scholars and Politicians Have Imagined the World, From Plato to Eleanor Roosevelt*. Oxford University Press.

González, R.J. (2017), Hacking the Citizenry? Personality Profiling, 'Big Data' and the Election of Donald Trump. *Anthropology Today,* vol. 33 (3), pp. 9-12. DOI: 10.1111/1467-8322.12348.

Goodin, R.E. (2010), Global Democracy: In the Beginning. *International Theory*, vol. 2 (2), pp. 175 209. DOI: 10.1017/S1752971910000060.

Gorski, A. & P. Toomey (2016), Unprecedented and Unlawful: The NSA's 'Upstream' Surveillance. *ACLU*. Retrieved from: https://www.aclu.org/blog/national-security/privacy-and-surveillance/unprecedented-and-unlawful-nsas-upstream. Accessed on: 29-01-19.

GPO (2015), *H.R. 20148, USA Freedom Act of 2015*. 114th Congress, 1st Session. Authenticated U.S. Government Information, Public Law 114-23.

GPO (2001), *H.R. 3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. Authenticated U.S. Government Information, Public Law 107-56.

Greenwald (2013), NSA collecting phone records of millions of Verizon customers daily. The Guardian. Retrieved from: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Accessed on: 29-01-19.

Greenwald, G. & E. MacAskill (2013), NSA PRISM Program Taps into User Data of Apple, Google and others. *The Guardian*. Retrieved from: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Accessed on: 29-01-19.

Guterman, K. (2013), The Dynamics of Stereotyping: Is a New Image of the Terrorist Evolving in American Popular Culture? *Terrorism and Political Violence*, vol. 25 (4), pp. 640-652. DOI: 10.1080/09546553.2013.814506.

Hancock, D.R. & B. Algozzine (2016), *Doing Case Study Research: A Practical Guide for Beginning Researchers.* Teachers College Press.

Hanssen, B. (2016), Why the NSA's Incidental Collection Under Its Section 702 Upstream Internet Program May Well Be Bulk Collection, Even If the Program Engages in Targeted Surveillance. *Medium*. Retrieved from: https://medium.com/@BHanssen/why-the-nsas-incidental-collection-under-its-section-702-upstream-internet-program-may-well-be-a01817e161c4. Accessed on: 29-01-19.

Henne, B. & M. Smith (2013), Awareness About Photos on the Web and How Privacy-Privacy-Tradeoffs Could Help. In A.A. Adams, M. Brenner, M. Smith (eds), *Financial Cryptography and Data Security*. Springer: Berlin, Heidelberg. DOI: 10.1007/978-3-642-41320-9_9.

Holmes, S. (2009), In Case of Emergency: Misunderstanding Tradeoffs in the War on Terror. *California Law Review,* vol. 97 (2), pp. 301-356. DOI: 10.15779/Z38PM67.

Jaeger, P.T., J.C. Bertot & C.R. McClure (2003), The Impact of the USA Patriot Act on Collection and Analysis of Personal Information Under the Foreign Intelligence Surveillance Act, *Government Information Quarterly*, vol. 20 (3), pp. 295-314. DOI: 10.1016/S0740-624X(03)00057-1.

Jaeger, P.T., C.R. McClure, J.C. Bertot & J.T. Snead (2004), The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts, and Questions for Libraries and Researchers. *The Library Quarterly*, vol. 74 (2) pp. 99-121. DOI: 10.1086/382843.

Johanson, M. (2013), 7 Questions about TSA's PreCheck Program Answered. *International Business Times*. Retrieved from: https://www.ibtimes.com/7-questions-about-tsas-precheck-program-answered-1402795. Accessed on: 29-01-19.

Kadidal, S. (2016), Surveillance After the USA Freedom Act: How Much Has Changed? *Huffington Post*. Retrieved from: https://www.huffingtonpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html?guccounter=1. Accessed on: 29-01-19.

Kelly, E. (2015), Senate Approves USA Freedom Act. *USA Today*. Retrieved from: https://eu.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/. Accessed on: 29-01-19.

Kent, S. (1966), *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press.

Kris, D. (2018), The NSA and the USA Freedom Act. *Lawfare*. Retrieved from: https://www.lawfareblog.com/nsa-and-usa-freedom-act. Accessed on: 29-01-19.

Liang, F., V. Das, N. Kostyuk & M. M. Hussain (2018), Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, vol. 10 (4), pp. 415-453. DOI: 10.1002/poi3.183.

Lowenthal, M.M. (2016), *Intelligence: From Secrets to Policy.* Washington, DC: CQ Press.

Lyon, D. (2014), Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, vol. 1 (2). DOI: 10.1177/2053951714541861.

Lyon, D. (2015), *Surveillance after Snowden.* Polity.

McCreadie, K (2008), *Sun Tzu's the Art of War: A 52 Brilliant Ideas Interpretation*. Oxford: Infinite Ideas.

McGregor, L. (2016), First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council. *European Journal of International Law*. Retrieved from: https://www.ejiltalk.org/first-report-of-the-un-special-rapporteur-on-the-right-to-privacy-to-the-human-rights-council/. Accessed on: 29-01-19.

Medine, D., R. Brand, E.C. Cook, J. Dempsey & P. Wald (2014a), *Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court*. Privacy and Civil Liberties Oversight Board.

Medine, D., R. Brand, E.C. Cook, J. Dempsey & P. Wald (2014b), *Report on the Surveillance Program Operate Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. Privacy and Civil Liberties Oversight Board.

Michelman, S. (2009), Who Can Sue over Government Surveillance? *UCLA Law Review*, vol. 57 (1), pp. 71-114.

Moser, F. (2015), *A Good American*. Austria: Blue+Green Communication.

Murray, D. & P. Fussey (2018), Police are using Big Data to Profile Young People, Putting them at Risk of Discrimination. *The Conversation.* Retrieved from: https://theconversation.com/police-are-using-big-data-to-profile-young-people-putting-them-at-risk-of-discrimination-96683. Accessed on: 29-01-19.

Nissenbaum, H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

NSA (2018), NSA Reports Data Deletion. *NSA*|*CSS*. Retrieved from: https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/. Accessed on: 29-01-19.

NSA (n.d.), Mission & Values. *NSA*|*CSS.* Retrieved from: https://www.nsa.gov/about/mission-values/ Accessed on: 29-01-19.

NSA Civil Liberties and Privacy Office [NCLPO] (2016), *Transparency Report: The USA Freedom Act Business Records FISA Implementation*. NSA|CSS.

Obar, J.A. & A. Oeldrof-Hirsch (2018), The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society,* pp. 1-20. DOI: 10.1080/1369118X.2018.1486870.

Office of the Director of National Intelligence [ODNI] (2013), Review Group on Intelligence and Communications Technologies Releases Public Comments. *Office of the Director of National Intelligence*. Retrieved from: https://www.dni.gov/index.php/ctiic-who-we-are/239-

about/organization/review-group/960-review-group-on-intelligence-collection-and-communications-technologies-releases-public-comments. Accessed on: 29-01-19.

Office of the Director of National Intelligence [ODNI] (2017), *Statistical Transparency Report Regarding Use of National Security Authorities For Calendar Year 2016*. Office of the Director of National Intelligence.

Office of the Director of National Intelligence [ODNI] (2018), *Statistical Transparency Report: Regarding Use of National Security Authorities – Calendar Year 2017 - Office of Civil Liberties, Privacy, and Transparency*. Office of the Director of National Intelligence.

OHCHR (2016), *Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci*. Human Rights Council, Thirty-first session.

Omand, D. (2014), The Cycle of Intelligence. In R. Dover, M.S. Goodman & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies*. Routledge.

Ombres, D. (2015), NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform. *Seton Hall Legislation Journal*, vol. 39 (1), pp. 27-58.

Parmar, M. (2018), Microsoft's Windows 10 is Again Facing User Privacy Violation Accusations. *Windows Latest.* Retrieved from: https://www.windowslatest.com/2018/04/28/microsofts-windows-10-is-again-facing-user-privacy-violation-accusations/. Accessed on: 29-01-19.

Posner E.A. & A. Vermeule (2007), *Terror in the Balance: Security, Liberty, and the Courts*. Oxford University Press.

Pozen, D.E. (2016), Privacy-Privacy Tradeoffs. *University of Chicago Law Review,* vol. 83 (1), pp. 221-248.

Richards, J. (2014), Signals Intelligence. In R. Dover, M.S. Goodman & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies*. Routledge.

Richards, N. (2015), *Intellectual Privacy*. *Rethinking Civil Liberties in the Digital Age*. Oxford University

Press.

Richelson, J.T. (1995), *A Century of Spies: Intelligence in the Twentieth Century.* Oxford University Press.

Roehlinger, F. (2016), Why Privacy Matters to Everyone (and not only Those Who've done Something Wrong). *Androidpit.* Retrieved from: https://www.androidpit.com/why-privacy-matters-to-everyone?_gl=1*1gep973*_ga*YW1wLTdaSkhlQzM5TFJJY19LTmNtWlRBTlNua0E3ZVFLOVd1cmFmaUFqQkxGVE0yNHNPNDZRRVJacWJPLTRiczlndXc. Accessed on: 29-01-19.

Rollins, J.W. & E.C. Liu (2013), *NSA Surveillance Leaks: Background Issues for Congress*. Congressional Research Service.

Rosen, J. (2012), The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google. *Fordham Law Review,* vol. 80 (4), pp. 1525-1538.

Ross, J.E. (2002), Tradeoffs in Undercover Investigations: A Comparative Perspective. *University of Chicago Law Review,* vol. 69 (3), pp. 1501-1542.

Rubinstein, I.S. & N. Good (2013), Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Technology Law Journal,* vol. 28 (2), pp. 1333-1414.

Savage, C. (2018a), N.S.A. Triples Collection of Data from U.S. Phone Companies. *The New York Times*. Retrieved from: https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html?module=inline. Accessed on: 29-01-19.

Savage, C. (2018b), Congress Approves Six-Year Extension of Surveillance Law. *The New York Times*. Retrieved from: https://www.nytimes.com/2018/01/18/us/politics/surveillance-congress-snowden-privacy.html?module=inline. Accessed on: 29-01-19.

Scott, L. (2014), Human Intelligence. In R. Dover, M.S. Goodman & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies*. Routledge.

Solon, O. (2017), With the latest WikiLeaks revelations about the CIA – is privacy really dead? *The Guardian.* Retrieved from: https://www.theguardian.com/world/2017/mar/09/with-the-latest-wikileaks-revelations-about-the-cia-is-privacy-really-dead. Accessed on: 29-01-19.

Solove, D.J. (2004), *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.

Solove, D.J. (2006), A Taxonomy of Privacy. *University of Pennsylvania Law Review*, vol. 154 (3), pp. 477-564. DOI: 10.2307/40041279.

Solove, D.J. (2008), *Understanding Privacy*. Harvard University Press.

Solove, D.J. (2011), *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press.

Speckhard, A. & M. Shaikh (2014), *Undercover Jihadi: Inside the Toronto 18 – Al Qaeda Inspired, Homegrown, Terrorism in the West*. Advances Press.

Strahilevitz, L.J. (2013), Toward a Positive Theory of Privacy Law. *Harvard Law Review*, vol. 126 (7), pp. 2010-2042.

Stuntz, W.J. (1999), The Distribution of Fourth Amendment Privacy. *George Washington Law Review*, vol. 67 (5), pp. 1265-1295.

Suarez, S. (2017), Is America Safer? The USA Freedom Act of 2015 and What the FBI and NSA Have, Can, and Should be Doing. *Seton Hall Law.*

Sunstein, C.R. (1993), Incommensurability and Valuation in Law. *Michigan Law Review,* vol. 92 (4), pp. 779-861. DOI: 10.2307/1289693.

Sunstein, C.R. (1996), Health-Health Tradeoffs. *The University of Chicago Law Review*, vol. 63, pp. 1533-1571. DOI: 10.2307/1600280.

Swire, P. (2015), The USA Freedom Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years. *Privacy Perspectives*. Retrieved from: https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years/. Accessed on: 29-01-19.

Thomson, J.J. (1975), The Right to Privacy. *Philosophy and Public Affairs,* vol. 4 (4), pp. 295-314.

Tucker, D. (2014), *The End of Intelligence: Espionage and State Power in the Information Age.* Stanford University Press.

Vermeule, A. (2008), A New Deal for Civil Liberties: An Essay in Honor of Cass R. Sunstein. *Tulsa Law Review*, vol. 43 (4), pp. 921-932.

Volokh, E. (2000), Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop people from Speaking about You. *Stanford Law Review,* vol. 52 (5), pp. 1049-1124. DOI: 10.2307/1229510.

Walsh, P.F. & S. Miller (2016), Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security*, vol. 31 (3), pp. 345-368. DOI: 10.1080/02684527.2014.998436.

Wang, M. (2017), China's Chilling 'Social Credit' Blacklist: A Lawyer is Barred from Buying a Plane Ticket Because a Court Found His Apology 'Insincere'. *Human Rights Watch*. Retrieved from: https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist. Accessed on: 29-01-19.

Warner, M. (2007), Sources and Methods for the Study of Intelligence. In L. Johnson (ed.), *Handbook of Intelligence Studies*. London: Routledge.

Warren, S.D. & L.D. Brandeis (1890), The Right to Privacy. *Harvard Law Review*, vol. 4 (5), pp. 193-220.

The Washington Post (2015), USA Freedom Act: What's in, What's out. Retrieved from: https://www.washingtonpost.com/graphics/politics/usa-freedom-act/. Accessed on: 29-01-19.

Weatherbee, T.G. (2010), Critical Incident Case Study. In A.J. Mills, G. Durepos, & E. Wiebe (eds.), *Encyclopedia of Case Study Research*. SAGE Publications.

The White House (2015), Statement by the President on the USA FREEDOM Act. *The White House.*

Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act. Accessed on: 29-01-19.

Whittaker, Z. (2015), Drowned in Data, Whistleblowers Speak of NSA's 'Largest Failure'. *ZDNet*. Retrieved from: https://www.zdnet.com/article/nsa-whistleblowers-security-thinthread-largest-failure-in-nsa-history/. Accessed on: 29-01-19.

Wikileaks (2017), Vault 7: CIA Hacking Tools Revealed. *Wikileaks*. Retrieved from: https://wikileaks.org/ciav7p1/. Accessed on: 29-01-19.

Worldometers (2018), Current World Population. *Worldometers*. Retrieved from: http://www.worldometers.info/world-population/. Accessed on: 29-01-19.

Yin, R.K. (2009), *Case Study Research. Design and Methods (Applied Social Research Methods)*. London and Singapore: Sage.