Snowden’s revelations and norm emergence in the United States

By Stijn Jalvingh
Student number: s1598996
Email: szjalvingh@hotmail.com
Supervisor: Professor Giles Scott-Smith
Program: MA International Studies
May 2016

Leiden University
Table of contents

Introduction 1

Chapter 1 6

- Literature review 6
- Observations 9
- Methodology 10

Chapter 2 12

- A history of domestic spying 12
- Snowden’s revelations 12
- FISA Court order for Verizon 13
- Prism 14
- Boundless informant 15

Chapter 3 17

- ACLU v. Clapper 17
- Court’s opinion 19
- USA FREEDOM Act 20
- Effective changes? 23
- A new norm of privacy 25

Conclusion 26

Bibliography 28
Introduction

Edward Snowden worked his way up from a high school drop out to a high level cyber security expert at the CIA. In 2013 he was an employee of the powerful private defense contractor Booz Allen Hamilton, a company that was working for the National Security Agency (NSA). He was just a small part of a very big machine until he decided to become a whistleblower and inform the world about the massive surveillance programs the United States were secretly running. These revelations shocked the world. Massive arbitrary phone and internet surveillance programs targeting Americans as well as foreigners were made public by Snowden with the help of several journalists.

It was not the first time the NSA was at the center of a scandal. In 2005, the New York Times reported that the Bush administration had ordered the NSA to eavesdrop on American citizens without obtaining the necessary warrants. The program had been running since the September 11 attacks on New York and relied on a very broad interpretation of Article Two of the constitution, which grants power to the president as commander in chief of the armed forces. Ten years ago this was a scandal but in Bush’s war on terror in the years after the 9/11 attacks, the fear of terrorism pushed the issue somewhat to the background. Ironically, just two months after this first disclosure, speakers in Congress condemned China’s use of internet as a tool for suppression. It took another scandal, Snowden’s revelations, to bring these issues to the attention of Americans and the rest of the world. They shed a new light on what policies based on fear of terrorism have brought forward. The volume of the documents he obtained, the way they were brought to the public and the massive scale of the NSA’s operations created a worldwide debate regarding privacy. Different then in 2005, attitudes towards privacy started to change now, and privacy concerns started to outweigh concerns over security.

In the public and scholarly debates about whether these programs are violations of privacy, a connection is often made with (national) security. In public statements, president Obama and former NSA chief Keith Alexander often draw on arguments highlighting the security values of the programs. Obama has proclaimed himself eager to debate the balance of liberty and security, thereby acknowledging the fact that in order to gain more security, a part of citizens’ liberty has to

---

1 G. Greenwald, No place to hide. Edward Snowden, the NSA and the surveillance state (London 2014) 1.
3 Greenwald, No place to hide, 2-5.
4 See for example: House select Intelligence Committee hearing on disclosure of National Security Agency Surveillance programs, 18 June 2013.
be sacrificed. Many scholars however highlight the universal human right of privacy and the Fourth Amendment in the United States constitution that are in place to avoid violations of privacy. This essay will look into the following question: To what extent did Snowden’s revelations contribute to the acceptance of the international norm of privacy as a human right in the United States?

To answer this question the domestic culture in which the United States formulate their security policy will be discussed in light of the norm of privacy. Two cases, one from the judicial branch (ACLU v. Clapper) and one from the legislative branch (the passing of the USA FREEDOM Act) of the United States will be used to illustrate developments in this domestic culture. Also Finnemore and Sikkink’s theory about norms and their conception of the norm “life cycle” will be used to put the scholarly debate about privacy and security in context. This essay will not look at security in terms of quantified intelligence. Instead, it tries to use the framework that is provided by constructivist international relations theory to put the debate about privacy as a human right versus desired security in perspective, in order to find out if Snowden’s revelations to the public are contributing to creating an environment in which the United States will value privacy norms to a greater degree.

This essay will use the theory about emerging norms in Finnemore and Sikkink’s article ‘International norm dynamics and political change’ along with theory of other constructivist writers like Katzenstein, Wendt and Jepperson. Identities that states project, and the interests they pursue are seen as partly constructed by their environments, or the culture in which these states are embedded. The identity of a state is being seen as an important factor for the creation of national security policy. In ‘Norms, identity, and culture in national security’ an important notion is that actors do not have an intrinsic identity, but that this identity is formed through a cultural environment. Norms are an important part of the cultural or institutional environment of states. They shape both the national security interests or the security policy of the state directly as well as the states’ identity. Another effect of identity configuration of a state is to be seen on the international level. It shapes interstate normative structures, like security communities or regimes. What an actor understands to be in its interest depends on the cultural context in which it operates.

---

7 Ibidem, 35.
8 Ibidem, 52-53.
9 Ibidem.
A norm has to be shared among a number of different actors to be called a norm. Katzenstein looks at the state in relation to society. The identity of the state and social actors in civil society can be understood as mutually constitutive.\(^\text{10}\) This process of identity exchange is what is happening in the two cases that will be studied in this research. Certain civil society actors like the ACLU, NYCLU and their supporters share a certain norm of privacy which is not shared with the rest of the country, nor do they think it is sufficiently reflected in the law. This research will focus on the quest of these actors and the people supporting these organizations or their privacy goals to establish their norm as a country wide one. By suing government officials in ACLU v. Clapper, these actors are trying to alter the environmental structure of the United States by attempting to change the law. This environmental structure, or cultural structure, shapes both the national security interests or the security policy of the state directly as well as the states’ identity. By altering the law, they hope to alter the identity and policy of the United States to a country where privacy is respected to a greater degree.

Norms come in various strengths according to Legro as quoted in Finnemore and Sikkink.\(^\text{11}\) This is something that Jepperson et al. also highlight by pointing out the difference between a “prominent” and “internalized” norm. The extent to which a community agrees on a certain set of values can be understood by examination of the “life cycle” of a norm. This theory is therefore useful in answering the main question of this essay. The norm life cycle itself can be used to describe the aforementioned process of civil society actors trying to internalize their conception of the norm of privacy in the United States. By altering the environmental domestic structure (in this case: the law) they try to be successful norm entrepreneurs. The theory identifies three stages in a norm’s life cycle: norm emergence, norm cascade and internalization. The first two stages are separated by a “tipping point” or critical mass of actors necessary to move to the next stage. The international norm of privacy as well as the domestic version will be looked at in light of this theory, with a greater focus on the domestic. Finnemore and Sikkink provide us with a way to understand the influence of international norms on the domestic area. Domestic norms are intertwined with international norms. International norms firstly always have to work their way through the domestic structures. These structures can influence the end form or interpretation of the eventual international norm. In turn, domestic norm entrepreneurs are often seen using international norms in their argument.\(^\text{12}\) The aforementioned difference in strength is important to take into account here. The international norm of privacy

\(^{10}\) Ibidem, 51.


\(^{12}\) Ibidem, 893.
seems to have lost strength in the US. The civil society actors that are actively trying to alter the identity and policy of the US regarding privacy can be seen as norm entrepreneurs who are trying to embed their version of the norm of privacy in the United States.

Their desired norm of privacy lies close to the long established human right to privacy as is codified in the International Covenant on Civil and Political Rights (ICCPR) article 17. This article states that

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.”

ACLU uses this treaty often in their arguments to stop NSA surveillance programs. There are four primary requirements to surveillance that follow from article 17 of the ICCPR that are being quoted by ACLU as relevant to the NSA programs and which are being violated. These requirements to surveillance are about limitations by statute in nature and scope of the surveillance, the narrow tailoring of surveillance programs to address governmental objectives, the need of independent oversight systems and the equal treatment of people with a different nationality. This international treaty reflects the international norm of privacy and ACLU’s finding that the US violates this norm is an important part of their argument to change the national norm.

This essay will go over two cases that influence the amount of oversight the U.S. government and the public have on mass surveillance operations. First it will go over the appeal in the case ACLU v. Clapper. This verdict of the Second Circuit Court is the appeal of civil rights organizations and current and former Verizon customers suing government officials. They claim that the government’s bulk telephone metadata collection program exceeds section 215 of the PATRIOT Act and the First and Fourth Amendment to the Constitution. In December 2013, the District Court granted the government’s motion to dismiss injunction and the plaintiffs now decided to appeal this decision. The result of this appeal can be summarized as recognizing the incompatibility between security and privacy and it addresses the problem that is being brought to the court by civil society actors, namely

their concern about the legality of the bulk telephone metadata collection program that Snowden exposed.

The second case this essay will go over in order to answer the central question is the passing of the USA FREEDOM Act (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act), which amends several pieces of legislation, like the PATRIOT Act, on which the telephone metadata collection was based. This essay will analyze this Act by looking at the problems that are identified by scholars and civil society actors after Snowden’s revelations and compare them to the contents of the Act. It will use the constructivist theory of emerging norms to identify what these two cases contribute to the acceptance of the norm of privacy in the United States. Both cases address the issue of oversight and are found in the legal sphere, therefore being part of the ‘cultural environment’ of the country as defined by Katzenstein.15

These cases are chosen because they are recent results of the public and Congressional efforts to change the practices that have been exposed by Edward Snowden. The USA FREEDOM Act will be compared to previous legislation that enabled the NSA to conduct their massive surveillance operations in order to identify strong and weak points of change in the law.

While the ACLU v. Clapper case only deals with the telephone metadata collection program and the Second Circuit Court refuses to deal with the issue of constitutionality, it is very useful because it addresses all the citizens’ concerns. It demonstrates the standing of the Court on the issue of reduced privacy. The two cases are in other words answers of both the judicial and the legislative branch to concerns from civil society actors about the executive branch. In combination with norm formation theory, these cases can help to establish whether the international norm of privacy has won terrain in the United States.

Chapter 1

In the first chapter, this essay will discuss scholarly literature that has been written on the balance between privacy and security. Scholars take different approaches to the issue and are not in agreement about certain aspects like the nature of the problem or the solution. Nevertheless, this chapter tries to get a good idea of what aspects are being discussed and it will deduct some generalities from the discussions that can be used to answer the main question. Articles of Etzioni and Sinha will be used to frame the incompatibility of the norm of privacy with the norm of security. The White-van Buuren discussion will be used to highlight different approaches to solving the posed problem. After that, the theory and methodology that will be used to frame this essay will be discussed further.

In the second chapter, a brief history of electronic surveillance in the United States will be provided together with an overview of Snowden’s revelations.

The third chapter will go into the two cases that were mentioned in the introduction and a connection will be made with the previous chapter. In the conclusion an answer to the main question will be provided.

Literature review

Some scholars believe civil liberties are being undermined by the NSA programs. Etzioni however takes a more balanced approach. In his article ‘NSA. National security vs. individual rights’ he advocates that small intrusions of privacy are tolerable as long as they contribute significantly to our security.\(^\text{16}\) He believes that the NSA programs are within this balance (even the huge storage of call records that will be discussed in the second chapter) and if a better framework of accountability will come into being, the programs can stay in place.\(^\text{17}\) Sinha, like White and other scholars, draws upon international law to show that the United States fail to adhere to the international norm of privacy as a human right. He argues that human rights law should be looked at while assessing legality and propriety of the NSA programs.\(^\text{18}\) But where Sinha takes the ICCPR article 17 as a starting point for his claims, Etzioni dismisses the value of this ratified treaty. He quotes William A. Schabas in saying that although the United States Congress ratified the ICCPR, they did so with an “unprecedented number

---


\(^\text{17}\) Ibidem, 129-134.

of reservations, understandings, and declarations” effectively “rendering the treaty powerless under domestic law”.\textsuperscript{19}

Sinha takes the debate into the international arena where scholars like Etzioni keep it more in the domestic sphere. Even though Etzioni’s argument that the US can’t be held accountable internationally if privacy rights are violated is true, Sinha argues that the normative foundation this treaty lays for the United States leaves no room for transgression.\textsuperscript{20} These approaches reflect a debate in the normative sphere. Sinha believes that the internationally accepted norm of privacy should guide the US government when implementing programs that are possibly a danger to peoples’ privacy. Etzioni believes the government has thought the programs through and problematizes the norm of privacy vis-à-vis the norm of security. The possible misuse of these programs are recognized in his article, but he considers the programs covered under section 215 of the Patriot Act. He provides solutions to privacy concerns that include an increased government accountability. However when formulating his argument that favors security over privacy, he uses legal arguments to counter the claim that privacy is being violated without questioning the legitimacy of these laws.

White discusses the solutions of increased accountability and transparency. He problematizes the obligation of businesses to protect human rights (codified in the Ruggie principles\textsuperscript{21}) and their obligation to follow state law. An Internet Service Provider (ISP) like Facebook or Twitter is obligated to cooperate with the US government in providing data about their customers, but this conflicts with their obligation to protect human rights. White suggests more transparency of ISP’s towards their customers about government interceptions, but the problem with this is that this would mark a shift in responsibility to protect human rights from the government to the private sector. He believes the international community has a role to play in developing acceptable accountability.\textsuperscript{22} However in the end, it is the states’ responsibility to respect the ICCPR rights, but also to protect them by actively putting legislation and administrative machinery in place and to fulfill them by promoting these rights and providing them to people.\textsuperscript{23} Van Buuren argues that international cooperation between intelligence agencies contributes to the undermining of civil liberties. He quotes Sepper while making

\begin{itemize}
\item \textsuperscript{19} Etzioni, ‘NSA. National security vs. individual rights’, 123.
\item \textsuperscript{20} Sinha, ‘NSA surveillance since 9/11 and the human right to privacy’, 866-867.
\item \textsuperscript{23} Ibidem, 5-6.
\end{itemize}
the argument that the battle to regain control over international intelligence activities by liberal democracies is long lost. This problem of the loss of democratic control over the international intelligence collection is a reflection of post-democratic tendencies according to Van Buuren. Post-democracy is explained by him to be the development that national democratic structures have been failing to keep up with certain aspects of globalization, intelligence being one of them. This fundamental shift in power relations is according to him not recognized enough by scholars attempting to develop ways to increase democratic systems of oversight. He suggests the introduction of personal ownership over data instead, taking the oversight question out of the institutional sphere. However, this would be strengthening the globalizing market structure that has also been a part of the problem of the diminishing democratic oversight. He also highlights the fact that all the major intelligence scandals were exposed by investigative journalists and whistleblowers, not by institutions that were put in place for the purpose of providing oversight. Empowerment of these civil ‘undersight’ networks is also suggested by Paquette, Wright, Greenwald and Mann. Van Buuren in short has a more pessimistic view than White, suggesting that states are no longer able to enforce effective intelligence oversight. The major oversight actors are in civil society, where they promote the international norm of privacy. White’s suggestion that states have to put effective frameworks in place that reflect their responsibility to respect the ICCPR does not find resonance with Van Buuren, who believes that states don’t have the capacity even if they wish to do so.

Other authors like Greenwald suggest that some countries have no interest in creating these oversight frameworks and adhering to their ICCPR commitments, especially the United States. It is argued in this essay that the American system has a perceived need to “collect it all” in order to prevent the next intelligence failure, this need keeps the country from developing convincing oversight frameworks. Greenwald and some scholars argue that collecting it all is the wrong method to achieve complete security but it is the perceived right way to go in the United States. Van Buuren’s proposed solutions are based on the assumption that this will not change. White’s article works from the assumption that an institutional solution coming from the state itself is a possibility.

---

26 Ibidem, 248-250.
27 See for example: House select Intelligence Committee hearing on disclosure of National Security Agency Surveillance programs, 18 June 2013.
Van Buuren and Aldrich believe the internationalization of the collection of data has led to a situation in which the intelligence community has gained a free hand in practicing their trade with decreased oversight. National institutions have been unable to keep effective oversight because of globalization, Aldrich argues.  

28 His historical inquiry in the growing power of intelligence agencies after 9/11 sheds some light on the subsequent weakening power of the European Convention on Human Rights that was incorporated in the statutes of European intelligence agencies. Where operations relied on secrecy in the Cold War, this changed to reliance on legality in the post-Cold War world. The return to secrecy is attributed to intelligence failures like 9/11.  

29 National efforts have since been seen to increase oversight over intelligence activities, reflecting the need to have more accountability, but that clashes with the by Greenwald highlighted culture of “collecting it all”. Aldrich’s article points out problems that European states now also face on the subject of the violation of international human rights. He highlights a dilemma intelligence agencies face.

“Intelligence agencies cannot, at one and the same time, be tough enough on some of the more intractable transnational problems of the world and soft enough to please the human rights lawyers.”

This observation reflects the spirit of this essay, that looks into the development of the norm of privacy as a human right. This essay will look into the contribution of the Snowden revelations to the acceptance of the international norm of privacy as a human right in the United States. At the basis of this question lies the privacy-security axis. Will the revelations provide a shift to the privacy side?

Observations

What follows from the Etzioni-Sinha discussion is that the human right to privacy is internationally accepted, but not always followed by the US. The norm of security is often favored. The White-Van Buuren review shows us that there is a role to play for the international community in protecting privacy rights, but in the end it’s the states’ responsibility. Oversight is a common denominator in identifying the problem of privacy violations in an international and domestic context. It is recognized to be vital in gaining privacy rights back. The question that is raised by looking at the White-Van Buuren review is about what actor has to provide this oversight. The state has obviously failed according to Van Buuren, who believes civil society should be strengthened. White believes in an institutional solution coming from the state. Two cases that will be discussed in this essay will reflect

30 Ibidem, 55.
the government’s effort to come up with an institutional solution, but also the role of civil society in realizing this change. In doing so, it focuses on the domestic culture of the United States that shapes the identity of the country.

**Methodology**

The elements from civil society that created the opportunity and momentum for the ACLU v. Clapper decision and the passing of the USA Freedom Act were informed by norms regarding privacy. Examples of these actors are Edward Snowden, the journalists helping him publish his documents, civil rights organizations and private citizens expressing concern. Their belief is that the privacy norm is not being adhered to by the United States. The constructivist idea that norms shape national security policy and the states’ identity lies at the foundation of the central question of this essay. The two cases that are chosen in this essay are being seen as good indicators of the domestic culture in the United States that is forming its identity.

Finnemore and Sikkink’s theory of the “norm life cycle” is about norm emergence in the international arena. When they talk about actors, they mean states. What this essay tries to do is to look at domestic norm emergence, but the concepts they use and the theory on which they build are still very useful for this essay’s approach. For the first stage of the norm life cycle, norm emergence, you need norm entrepreneurs. Domestic norm entrepreneurs, like the ACLU in the United States, can use international norms in their arguments, which is what you also see when looking at the Sinha article that is being discussed here. The threshold, or tipping point that separates norm emergence from norm cascade is harder to define in the domestic context. It is important to note that Finnemore and Sikkink also only work with an hypothesis on when a critical mass of actors is reached for the norm to cascade. Their notion that the specific actors that adopt the norm are important will come back later in discussing the passing of the USA Freedom Act. A previous version of the Act was not supported by a few specific groups in the political spectrum, namely the intelligence ‘hawks’. It was only when they could support the contents of the Act as well as the ‘doves’ that the Act was passed and its contents became law. The discussion about the establishment and contents of the Act can be seen as part of the norm life cycle, it illustrates the changing norm of privacy and its contents are an indicator of whether and how strongly the norm is changing. The norm cascade in Finnemore and Sikkink’s theory is all about spreading the norm to states who didn’t accept the norm earlier, it is argued here that in the domestic case of this essay, the norm needs more spreading as

---

well, even when the law reflects a domestic culture that values privacy more. In order for a norm to be completely accepted, so to have a “taken-for-granted” quality, a spreading amongst actors need to occur which Finnemore and Sikkink call ‘socialization’. The answer to the central question lies in defining where the international norm of privacy is located in this domestic norm life cycle, while the strength of the norm needs to be taken into account as well. The two case studies are being used to this end.

---

Chapter 2

A history of domestic spying

Established in 1952 by president Harry Truman, the NSA had known many successes but had few legal limitations to their surveillance work. This changed when the Senate established the Church committee in 1975 in order to identify illegal practices of the NSA, CIA and FBI and to find out whether there was enough oversight from different branches. The committee exposed many scandals in all agencies, among them efforts of the FBI to destroy Martin Luther King. The NSA proved to be involved in domestic spying on activists in civil rights movements and against anti-Vietnam protesters. In assessing the balance between liberty and national security during the Cold War, the committee had shown to Congress that change was necessary. In 1978 it passed the Foreign Intelligence Surveillance Act (FISA) that required search warrants for domestic spying cases concerning national security. These warrants were to be given out by a secret court in order to maintain operational secrecy. Michael Hayden, who became NSA director in 1999, started actively promoting the NSA as an institution that relies on legality after the NSA kept appearing in popular culture as an organization with a dubious agenda. James Risen and Eric Lichtblau however revealed that after the terrorist attacks, the agency started warrantless spying on Americans on a large scale again, targeting thousands of citizens. A broad interpretation of the second article of the Constitution apparently lay at the base of this warrantless spying. Like the introduction of this essay mentioned however, it took more than this eavesdropping scandal to create a debate on a national and international level.

Snowden’s revelations

Snowden released a large amount of documents detailing the inner workings of the NSA in pursuit of equal protection from unreasonable search for all people. In order to achieve that, he believes the law has to catch up again on science, which develops faster. By releasing the documents in cooperation with journalists like Greenwald he aimed for a bigger public understanding of the mechanisms through which our privacy is violated. The great quantity of the documents exposed how the NSA works, where their priorities are and how ambitious they are in expanding their reach. It has become clear that the NSA has eavesdropped on financial institutions, international

---

36 Ibidem, 43-44.
37 Greenwald, No place to hide, 13.
organizations, foreign energy companies, EU officials and even heads of state in order to gain a diplomatic or economic advantage. So besides surveillance for security, the NSA also has programs in place for diplomatic or economic purposes. But however shocked other countries’ populations were when they heard the US had been spying on their leader, as happened in Germany, Greenwald and Snowden find these revelations less significant than the discovery of the NSA’s massive surveillance of whole populations. Intelligence collection enjoys a great deal of independence from official foreign relations according to Herman, it operates in a different playing field then political relations. It can be used to support or enhance foreign relations, but it does not undermine foreign relations equally. In short, governments know they’re being targeted by foreign intelligence agencies and they deal with that in the sphere of (counter)intelligence, not in the political sphere. The vast amount of files and the stories behind the revelations of mass surveillance contain files on three programs of major importance for this research and for the privacy debate in the United States that will be discussed here.

**FISA court order for Verizon**

The first story that was published by Greenwald and the Guardian had an enormous impact and became the lead story on every main national news channel. It consisted of an order from the FISA court, an institution established to prevent the government from engaging in abusive electronic surveillance. The order said that Verizon Business, the largest mobile network operator in the US, was obliged to turn over to the NSA “all call detail records” for “communications (i) between the US and abroad; and (ii) wholly within the US, including local telephone calls”. Call detail records in this case don’t mean the content of each call, but the ‘metadata’ of the call, basically everything but the exact call content. This metadata consists typically of the time of the call, duration, receiving and incoming telephone numbers. While it is regarded by a few scholars (like Etzioni) to be not excessively intrusive and justified by our need for security, many scholars (like Kadidal) and tech-analysts point out how this seemingly harmless information can reveal a lot about people. Examples of how this information can be harmful are countless. It can for example reveal religious affiliations, drug problems, relationship status and political beliefs but as Kadidal points out it can also compromise sources of reporters covering an embarrassing government secret or compromise attorneys’ communication with clients. Soon it became clear that the bulk phone record collection program had been going on for years and was directed not only Verizon, but at all big telephone

---

38 Ibidem, 139-141.
39 M. Herman, *Intelligence power in peace and war* (Cambridge 2010) 218.
40 Ibidem, 71.
41 Etzioni, ‘NSA. National security vs. individual rights’, 112-113.
companies. This court order also specified that the bulk collection of telephone records was justified by section 215 of the Patriot Act. This is a very radical explanation that will be further discussed in the third chapter.

**Prism**

The NSA’s ‘Prism’ program was legally covered by the 2008 FISA Amendments Act. A law that was enacted after the aforementioned NSA eavesdropping scandal and which effectively legalized the core of Bush’s illegal program. The Act differentiates between ‘US persons’ (Americans and those who are legally on American soil) and ‘non-US persons’. If the NSA wants to target a US person’s phone records or email it still has to get a warrant but for the rest no warrant is needed, even if they are communicating with a US person. The Prism program thus targets every non-American citizen outside the United States and every American who is communicating with a non-US person. It focuses on private electronic communication and gets its data from all the major online providers such as Facebook, Google, Yahoo, Microsoft and Skype. The articles in the *Washington Post* and *The Guardian* about this program caused a similar reaction as the ones about the Verizon court order but this time indignant reactions came the international community since it was clearly targeting the major means of communication of millions of people all over the world.

Greenwald aptly points out that users of Skype felt especially betrayed because when Microsoft bought Skype in 2011, it assured customers that “Skype is committed to respecting your privacy and the confidentiality of your personal data, traffic, and communications content.”

---

42 Greenwald, *No place to hide*, 72.
43 Ibidem, 74.
45 Greenwald, *No place to hide*, 75-77.
46 Ibidem, 113.
This picture is part of the documents Snowden released and shows the scope of the NSA’s access to internet data.47

Boundless Informant

The NSA program ‘Boundless Informant’ was designed to keep track of the amount of interceptions the NSA made. It is mentioned in this research because it proved that NSA employees have been lying to Congress for years about the extent of their data collection. Two examples are mentioned by Greenwald, the first one is that senators have been asking the NSA for estimates of how many Americans were having their calls and emails intercepted. The NSA claimed that they did not maintain data containing that information, but Boundless Informant proves otherwise. Also in an open hearing before the Select Committee on Intelligence of the US Senate in 2013, Senator Wyden asked Director of National Intelligence James Clapper whether the NSA collects any type of data at all on millions or hundreds of millions of Americans.48 His answer was no. Both the Verizon and Prism documents prove otherwise and Boundless Informant just emphasizes how well the NSA documented their data gathering.

What has become clear after these revelations is that the law has been bent or neglected by the executive branch of the government in order to fulfill a need to gain more security since 9/11, when the norm was bent towards security with the implementation of the Patriot Act. That was the reason the government was able to justify the data collection on the scale that has been exposed by these and other cases and NSA projects. The fact that FISA became involved indicates the norm change. Many citizens and civil rights organizations believe laws have been insufficient in protecting privacy rights and are calling for a change. The following chapter will look at two cases that are the result of the call for a new identity for the United States, an identity that includes a domestic norm of privacy that is closer to the international norm. By altering the domestic culture, in this case the law, norm entrepreneurs hope to make sure the US becomes a nation with greater respect for privacy. Whether they are succeeding will be made clear using the theory of the life cycle of a norm.
Chapter 3

Two developments in the domestic culture of the United States, or the law in this case, will be looked at in this chapter. The theory of the “life cycle” of a norm will be used to describe the process of civil society actors, or norm entrepreneurs, trying to internalize their conception of the norm of privacy in the United States.

ACLU v. Clapper

The first case that will be looked at is ACLU v. Clapper. This decision of the Second Circuit court of appeals is the result of a lawsuit of civil society actors against government officials. The case is concerned with the legality of the collection of telephone metadata “on an ongoing and daily basis” from and to Americans and the storage of this data, as was revealed by Snowden’s leaked Verizon court order. The plaintiffs, or suing parties, consist of American Civil Liberties Union (ACLU), New York Civil Liberties Union (NYCLU) and the New York Civil Liberty Union Foundation (NYCLUF). The defendants are government officials James Clapper (Director of National Intelligence), Michael Rogers (Director of the NSA and chief of the Central Security Service), Ashton Carter (Secretary of Defense), Loretta Lynch (Attorney General of the United States) and James Comey (Director of the FBI).49

In section 215 of the Patriot Act, that passed Congress after the 9/11 attacks, the Foreign Intelligence Surveillance Act (FISA) was amended. The government argues in ACLU v. Clapper that section 215 justifies their telephone metadata collection program. The original version of section 215 required the government to obtain orders from the FISA court (FISC) to provide them with business records for the purpose of intelligence investigations where there were

“specific and articulable facts giving reason to believe that the person to whom the records pertain [wa]s a foreign power or an agent of a foreign power”.50

The Patriot Act revised it to cover not only business records but also “any tangible things”. The information the government has to provide the FISC changed to

50 Ibidem, 11.
“a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation [...]”.\textsuperscript{51}

The most noticeable difference here is the change from “specific and articulable facts” to “reasonable grounds”. The FISC order for Verizon, like any order from the FISC, had to be renewed every 90 days and has therefore been renewed 41 times between the court date and the first issue of the order. The US government also does not contest the plaintiffs’ claim that virtually all major telephone companies are under similar orders.

The data that is collected is subsequently put into a major NSA database, ready to be inspected. Might there be “reasonable grounds” to believe a certain telephone number or person is associated with a foreign terrorist organization. The numbers that have been in contact with this suspected number and the metadata associated with it will be accessed too, signifying the first “hop”. Then the NSA can search for all the numbers and metadata associated with them that have been in contact with numbers that are part of the first “hop”, signifying the second “hop”. Also a third hop would be collected shortly after conducting a second. Although President Obama announced in a speech on January 17, 2014 that this third hop would not be pursued anymore. Another change he announced was that a FISC judge needs to agree reasonable suspicion exists instead of an NSA official.\textsuperscript{52} These measures were followed by a series of debates about the adjustment of certain laws by Congress. The USA FREEDOM Act that will be discussed later in this chapter is a result of these deliberations.

Where the government argues that the collection of metadata in a database is only harmful when they unjustly review the data, the plaintiffs believe the collection \textit{an sich} is a violation of their rights. Not only do they believe the Verizon program exceeds the authority granted by section 215 of the Patriot Act. They also believe it violates the First and Fourth Amendment of the Constitution.\textsuperscript{53} The First Amendment guarantees “freedom of association”, which according to the plaintiffs is violated by the program because it could disclose affiliation with certain groups as argued in the second chapter. The Fourth Amendment protects against unreasonable “searches and seizures”. The fact

\textsuperscript{51} Ibidem, 12.
\textsuperscript{52} Transcript to Obama’s 17 January 2014 speech. Weblink: https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bc8d84_story.html, Last accessed 11-01-2016.
\textsuperscript{53} G. Lynch et al., \textit{ACLU v. Clapper}, 23.
that the government ‘seizes’ the data by putting it in a database is reason for the plaintiffs to believe their Fourth Amendment rights are violated too.\(^54\)

**Court’s opinion**

The government’s argument is based on the broad interpretation of the word “relevant”. The plaintiffs argue that relevance is not an unlimited concept and that the fact that the government does not use much of the data in the database they put together proves that not all data is relevant.\(^55\) The analytical techniques the NSA uses however, need the database to filter out the relevant data. The court is of the opinion that the expansive concept of “relevance” the government uses is unwarranted and unprecedented in any criminal investigations under similarly formulated laws. Finding every piece of data available, as well as all future data, regardless of suspicion or relevance, is not proven to be helpful to an “authorized investigation” and the government has not specified what investigation requires all American phone data.\(^56\) A specific investigation is a necessity specified in section 215, thus necessary for the government in order to collect data, the general counterterrorism effort of the United States is not seen as an authorized investigation here. The court also found the privacy implications of the program too big to be justified by a broad interpretation of this section. It invited politicians in other words to extensively debate this matter and if it was decided the program is necessary to protect the country, Congress should write a law that says so in clear wordings.

The appellants’ Constitutional concerns are being addressed in this opinion, but left out of the ruling because the Second Circuit court of appeals already concludes that the statute on which the government bases its legal authority (section 215 of the Patriot Act) is not sufficient to let the program legally continue. It leaves the appellants’ Constitutional claims outside its ruling because the appellants’ goal of dismissing the program is already met by the dismissal on a statutory basis.

The ruling notes that it is up to Congress to decide whether this program is necessary for national security and the belief is expressed that the legislative branch is considered more capable of tackling the issue of privacy in this technologically fast-developing world.\(^57\) The court decided that with the ongoing debate in Congress concerning this specific program, the concerns of the civil society actors could possibly be taken away without a judge’s interference on Constitutional matters or

---

\(^{54}\) Ibidem, 28-31.

\(^{55}\) Ibidem, 54-55.

\(^{56}\) Ibidem, 59-66.

\(^{57}\) Ibidem, 90-91.
otherwise.\textsuperscript{58} The process of creating a bill that alters this program was ongoing at the time the decision was published. This bill is called the USA FREEDOM Act and it will be the subject of the second part of this chapter, since it is the next step in the norm entrepreneurs’ quest towards more privacy.

**USA FREEDOM Act**

While the ruling of the Second Circuit Court was considered a victory for the people who have been challenging the government’s surveillance programs and the system of oversight, more action is needed for the norm entrepreneurs to get their idea of privacy to be embedded in the law. They are trying to alter the environmental domestic structure of the United States in order to change its identity as well as its security policies. For something substantial to change, more is needed then just the Second Circuit court's decision. The fact that the court called for Congress to clearly word their stance on the mass data collection programs is a step in the direction desired by the civil rights organizations and the dismissal of section 215 of the Patriot Act as legal grounds for the program was a blow for the government. Whether a substantial change in the domestic culture of the United States would come into being depends on the actions Congress took in the form of the USA FREEDOM Act.

Republican representative Jim Sensenbrenner was the first to introduce the USA FREEDOM Act in the House of Representatives in October 2013. At the same time Democratic senator Patrick Leahy introduced the bill in the Senate. The bill gathered extensive bipartisan support, uniting libertarian Republicans and Democrats alike.\textsuperscript{59} The House Intelligence and Judiciary committees however made several amendments to the originally proposed version from Sensenbrenner. NSA supporters managed to dilute the bill significantly and several original supporters of the bill were not willing to back it anymore. For example the definition of a “specific selection term”, the term which the NSA will use to search the database and that is the subject of the court order of the FISC, changed from information that “uniquely describes a person, entity or account” to “a discrete term, such as a person, entity, account, address or device”. Senator Ron Wyden, a longtime critic of the NSA was among those who were worried about the watered down version of the House bill, believing it would not effectively end mass surveillance. The Senate version remained strong in his opinion.\textsuperscript{60} A civil society actor that is known to champion online privacy rights, the Electronic Frontier Foundation,

\textsuperscript{58} Ibidem, 92-93.


strongly supported the original version of the bill, noting it would bring new levels of transparency to the FISA Court and effectively putting statutory limits on mass surveillance by the NSA.\textsuperscript{61} Opsahl and Reitman were cautious in their optimism though in positing that the originally proposed bill still leaves a lot of issues unaddressed, for example NSA programs to sabotage encryption standards or the building of backdoors in hardware, the targeting of non-US persons and the providing of guidelines to obtain standing in legal cases against privacy intrusions. They were calling the bill a success, but with the side note that it is only a first step in a longer process of reclaiming privacy rights.\textsuperscript{62} The original version of the bill was however amended several times and the version that got “watered down” by the House Intelligence and Judiciary committees is the version that made it past the House and Senate and that got signed into law by the President. The bill ends the bulk collection of all records under section 215 of the Patriot Act, the FISA pen register authority and national security letters, which are subpoena’s the government can issue that require the recipient to hand over information. Credit card companies, ISP’s and cell phone providers could receive these letters for example. It also prohibits large scale, indiscriminate collection of data such as all records from an entire city or state. It is attempted to create more transparency by allowing national security letter nondisclosure orders to be challenged by companies. The appointment of an Amicus Curiae at the FISC and declassification of significant constructions or interpretations of the law by the FISC are meant to create more transparency as well, although there are some critiques that will be discussed below. The Act however also gives the government new tools to combat terrorism. It allows them to track foreigners longer on U.S. soil and creates new procedures for the use of section 215 in case of an emergency which will also be discussed below.

According to Neema Singh Guliani, legislative council for ACLU, the passing of the USA FREEDOM Act in May 2015 marks the first time since 1978 that Congress has taken steps to restrict surveillance practices, rather than expand them. However she also mentions a few steps that still need to be taken in order to get to a level of privacy desired by ACLU. Among those is the reform of section 702 from the Foreign Intelligence Surveillance Act which allows the government to collect content of American’s communications with individuals abroad.\textsuperscript{63} The ACLU also stresses that the version of the


\textsuperscript{62} Ibidem.


bill that passed is not ideal yet, noting that the definition of the “specific selection term” is not sufficiently narrow because it could still be interpreted as to allow government agencies to collect data on for example all hotel records within a given area, or hundreds of people who share an IP address, or an entire company. Another concern is that the “relevance” standard is not mentioned to be applicable for the second hop.

Language that was included in the original version of the bill (section 201) but that didn’t make it in the final version was related to minimization procedures regarding irrelevantly collected records. It required destruction of material that was collected but not used. With the exclusion of that language in the final version that got signed into law, the possibility still exists that the government will build a big database consisting of privacy sensitive information of innocent people.

ACLU is happy with the improvements that are made concerning the dissemination of information to the public regarding to important FISA decisions or surveillance programs operating under section 702 and 215 (in section 602). They do however believe that this improvement of the status quo is not enough yet. The measures they would like to see included in the bill are obligatory reporting of searches for US persons in the section 702 database and disclosure of the full amount of US persons and accounts impacted by section 702 surveillance authorities. Also only communications, not other records collected under section 215 are required to be reported on. This leaves account information or other data out of the public disclosure clause.

Following the Second Circuit court decision, it is attempted in the USA FREEDOM Act to let a voice be heard in FISC hearings on behalf of privacy and civil liberties as a counterbalance to the government. The Act provides for that in the form of an Amicus Curiae, that may be appointed by the court in novel or significant cases. ACLU finds that this section (903) could be made stronger because it is still possible for the court to appoint a lawyer who is not forwarding arguments in favor of privacy and civil liberties. Next to that, it would like to see the word “may” change to “is required”, so that it is not only up to the discretion of the court as to when to appoint an Amicus Curiae, but that one is required to be present by law in all novel or significant cases.

---

64 ACLU letter to the House of Representatives, Weblink: 
65 Ibidem, 2.
66 Ibidem 2-3.
67 Ibidem, 3.
In the current bill, the surveillance capabilities regarding to non-US persons within the US are expanded. It permits continued surveillance in the first 72 hours in the United States in case of threat of death or serious bodily harm. ACLU finds this an unnecessary provision, seeing that under the Foreign Intelligence and Surveillance Act a provision already exists that surveillance is possible in case of extreme circumstances. This addition makes it look like new loopholes are being created in order to violate privacy rights.

The USA FREEDOM Act does in its current form not provide protection against bulk collection under other authorities than section 215. It is known that the Drugs Enforcement Agency used to collect international call communications data of Americans using the administrative subpoena statute. The fact that this new bill does not try to amend such authorities in order to prevent abuse and mass collection of data raises concern with the ACLU.

**Effective changes?**

As is shown above, the bill doesn’t cover a number of issues that are desired by civil rights organizations that are working to alter the domestic and international privacy culture. First of all the bill covers only US-persons and leaves the communication they have with foreigners out. Also any non-US person is still subject to privacy intrusions by the United States government. Neither the Second Circuit court case nor the USA FREEDOM Act goes over measures to change this, and ICCPR article 17 is not recognized as legally binding to state and federal courts. Even though the targeting of non-US persons is not a vital part of the Verizon case and the USA FREEDOM Act that subsequently followed, many civil society organizations like ACLU and Electronic Frontier Foundation that promote a new norm of privacy would like to see a greater respect for privacy internationally as well. ACLU has pointed out that the international norm of privacy is not adhered to. Furthermore, it is not based on modern technological capabilities or based on knowledge of the NSA’s practices that Snowden revealed. This is why norm-entrepreneurs are advocating the norm of privacy again domestically, pointing to the basic principles of privacy that are set in ICCPR article 17. The fact that the new bill does not include language that curtails spying on non-US persons is a first indication that the desired

---

68 Ibidem, 4.
69 Ibidem, 4-5.
norm of privacy is still in its early stages of the norm life cycle. Privacy for everyone, what is described in the ICCPR, is still not reflected in the bill.

NSA programs to sabotage encryption standards were mentioned above as another issue that remains unaddressed. NSA works together with British counterpart GCHQ in weakening encryption, which puts online transactions at risk of being compromised.\textsuperscript{72} The building of backdoors in hardware and encryption systems weakens systems and computers for everyone, making them easier to penetrate for other foreign intelligence services and malicious hackers.\textsuperscript{73} This is an issue that is not only concerning privacy breaches from the government, but it is about the government enabling other groups from getting access to personal data. The fact that it remains unaddressed in the USA FREEDOM Act indicates that there is still work to do for the privacy norm entrepreneurs. Legally, it is still hard to make a case against the government in case of potential unwarranted privacy intrusions. The government has been using the ‘state secret privilege’ increasingly after 9/11, exempting entire cases from judicial review at the outset. This state secret privilege makes sure that government documents can be held back in court if the head of the responsible department deems them ‘dangerous for national security’. The Electronic Frontier Foundation is wary of the impact of this increasingly used legal precedent stemming from 1953 and points out that more measures could be taken to obtain legal standing in spying cases.\textsuperscript{74}

As is pointed out above, there are a few issues that are either left out or could be made stronger in the bill. It is clear that this is partly due to the Second Circuit Court case that embodied the main concerns of American citizens and civil society organizations, the Verizon case and the collection of telephone metadata in general. The focus of change was therefore only on a part of the scandals that Snowden revealed. The concerns that were raised all over the world by the Prism program don’t seem to be taken away by the new legislation. The bill did take away the possibility to use section 215 of the Patriot Act for the collection of call data and other business records, thereby taking the Second Circuit Court’s decision into account. Also an attempt is made to create more transparency in the NSA’s orders to companies by giving those companies options to challenge non-disclosure clauses that accompany NSA orders (‘gag orders’) and also the public will be getting more insight as

\textsuperscript{72} Greenwald, \textit{No place to hide}, 94.
\textsuperscript{73} Ibidem, 118.
to when the government requests information under section 215.\textsuperscript{75} The addition of a civil rights advocate in FISC hearings also seems to be a step in the direction of bigger influence of privacy advocates in the secret court.

\textbf{A new norm of privacy}

The strong behavioral violations of the US against the international norm of privacy that was exposed by Snowden invalidated the norm. The cultural-institutional context of the United States changed after 9/11 in a way that reshaped the national security policies and political culture of the country. This, backed up by Snowden’s revelations that provided evidence for this phenomenon, prompted new norm entrepreneurs to try and alter this political culture from a nation that needs security above all and has a need to “collect it all” to a nation that puts more value in privacy. According to Katzenstein, history is a process of change that leaves an imprint on state identity. The identities states project through their national security policies and cultural environment emerge from their interaction with different environments, both domestic and international.\textsuperscript{76} This research has been looking at a change in the domestic environment and briefly at the international-.

As mentioned before, it is important to note that norms come in various strengths, depending on the level of agreement within the norm’s operating area.\textsuperscript{77} The norm of privacy that is shared among the civil society actors that acted as plaintiffs in the Second Circuit Court case and those trying to make the USA FREEDOM Act stronger is not shared among enough people in the United States and their proxies in Congress to be able to embed it in the law. However their entrepreneurial efforts have successfully challenged the laws that were in place. The contested laws were part of the domestic culture of the United States that supported the norm of ‘security first’ that arose after 9/11. Changes in the domestic culture of the country were realized by the enactment of the USA FREEDOM Act and the new law does have widespread support. This changed domestic environment could support the transition towards a country that respects privacy to the desired degree. A step towards their desired norm, that is supported by the international norm, is therefore definitely taken, although it is clear that the desired norm of the civil society actors is not completely internalized yet. But by altering the domestic structure, a change is already made possible since the structure can influence the actors into changing their standards of appropriate behavior (norms).

\textsuperscript{75} Sheketoff, ‘USA FREEDOM Act of 2015 passes’, 401.
\textsuperscript{77} K. Finnemore, and M. Sikkink, ‘International norm dynamics and political change’, 892.
Conclusion

Each stage in Finnemore and Sikkink’s norm life cycle is characterized by different actors, motives and mechanisms of influence. The mechanism that defines the first stage (norm emergence) is persuasion by norm entrepreneurs who try to convince a critical mass of actors to embrace a new norm. In this case that process consists of two parts. Firstly they challenged the status quo by going to court about the Verizon case. That subsequently led to the second part of their endeavor, the altering of the domestic structure, when Congress started to deliberate about the contents of a new bill. By trying to influence the law making process with letters to Congress and the rallying of public opinion an attempt was made to create a new domestic structure that is favorable for their desired norm. Here they only succeeded partly because the law did change in their favor, but not as much as they would have liked to see, as is described in the third chapter.

The second stage, norm cascade, is separated from the first stage by a tipping point, a point where a critical mass of actors accepts the new norm. Its characteristic mechanism is norm leaders attempting to socialize other actors into following the new norm. The exact motivation for various non-followers to start following the norm can vary, but what the norm entrepreneurs were trying to accomplish here was a change in the domestic structure of the country (by altering the law) that would create a domestic cultural environment that is favorable for their norm to gain more followers. The second stage here is where a divide occurs between the norm entrepreneurs’ desired norm and a milder version of their norm, but a new norm nonetheless. The change they were able to make in the domestic structure has not been what they hoped it would be, however it did constitute a change in the desired direction. The debates about the contents of the new law reflect a changed attitude towards privacy. This new attitude suggests there is a new norm that is shared among many different actors from across the political spectrum and within different branches of government that value privacy to a greater degree. This new norm is however not the one that is desired by civil society actors, but a change in the domestic culture that is favorable for their norm did occur, it was only not the big change they had wished for. Snowden’s revelations did in this way contribute to a greater acceptance of the international norm of privacy in the United States, although the new norm that has been detected through the deliberations of the content of the USA FREEDOM Act is not completely informed by the international norm of privacy. As is shown before, there are still many

78 Ibidem, 895.
79 Ibidem.
changes civil society actors would like to see in the law before it becomes part of a domestic environment that is favorable for their norm.

The domestic culture in which the United States formulate their security policy has been altered with the adoption of the new bill and the Second Circuit Court’s decision. By successfully altering the law, which is part of the domestic culture in the United States, the norm entrepreneurs have made sure that a new norm of privacy can get a foothold in the country through this new environment, that came into being with support of many different actors. Their shared version of the norm of privacy which is reflected in the USA FREEDOM Act, has reached the stage of norm cascade, in which the norm will be spread more broadly throughout the country through a process of ‘socialization’. This different version of the norm of privacy will move faster towards internalization and achieve the ‘taken for granted’ status than the norm that is advocated by the norm entrepreneurs. The latter did not reach the threshold yet, but it has become clear that the norm entrepreneurs are not quite willing to give up yet. It seems to be that the weakened version of the USA FREEDOM Act is at this point the biggest alteration of the American domestic culture that could be realized and the new norm that will be enabled by this alteration may not be the desired version of the norm entrepreneurs that were discussed here, but it is the version that Americans are willing to adhere to.

Snowden’s revelations have created a group of norm entrepreneurs with the desire to introduce a new norm of privacy in the United States. Firstly by challenging the status quo in the Verizon case, which opened the way to the formation of the USA FREEDOM Act, which they helped take shape. These two case studies, combined with the theory about the norm life cycle have demonstrated that the acceptance of the international norm of privacy as a human right in the United States is not complete yet. This is to be seen in the end result of the efforts made in the Verizon case and the USA FREEDOM Act. It reflects the process of the establishment of a weaker norm of privacy than the one that is being adhered to by the norm entrepreneurs. However, the case studies have shown us that the revelations gave way for civil society actors to secure better frameworks of oversight, to stop the NSA’s strategy of “collect it all” by stopping mass surveillance and to create more transparency in the government. It has become clear that because of the revelations, a shift has taken place on the privacy-security axis in favor of privacy. According to civil rights organizations that have been partly responsible for enabling it, this shift is not big enough, but it is a step in their desired direction. A new domestic culture has been created that is more favorable for the acceptance of the international norm of privacy as a human right in the United States, but it seems like there are more changes that need to be made in order for this to happen.
Bibliography


Greenwald, G., No place to hide. Edward Snowden, the NSA and the surveillance state (London 2014).


Herman, M., Intelligence power in peace and war (Cambridge 2010).


Transcript to Obama’s 17 January 2014 speech. Weblink: [https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html](https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html).
