4. Norm Regression: Surveillance and Privacy in US History

Like other human rights, the norm of privacy has also been in conflict with counterterrorism measures in recent time (Heller et al. 2012: 278 f.). The NSA surveillance activities that were disclosed by Edward Snowden have been seen as the endpoint of this process for the moment. As it was argued with regard to the prohibition of torture (McKeeown 2009), it is logical to assume that a norm regression has taken place. This chapter aims to explain how this development has occurred. It will explore whether the spiral model can help to explain this norm regression. This should be done in a case study focusing on US behavior with regard to mass surveillance procedures and privacy concerns.

4.1. Surveillance, Security and Privacy

Ironically, surveillance is something that is said to be as old as the human need for privacy. As a human practice, the concept of surveillance is already inherent in a mother’s practice of looking after her child. It is an intrinsic feature of the human nature to care for each other. This is why surveillance is claimed to be natural. This need of care automatically results in monitoring the behavior of others. The surveillance of others, therefore, is a normal process in social settings. The aim of these monitoring processes is to nullify unaccepted behavior of members of a social group (e.g., a family or a religious group). Especially within religious beliefs, concepts of surveillance are embedded eminently. The image of an omniscient and all-seeing God helps to ensure rule consistent behavior (Goos et. al. 2015: 51 f.). “The concept of care and protectionism also transcends to the level of the state when it assumes the role of watching or surveilling its population, supposedly for
its own good. This can take the form of surveillance for safety and national security” (Goos et al. 2015: 52).

State-led surveillance is not only a direct response to contemporary terror threats. In fact, surveillance was inherent to the development of the modern state. Since states have begun to raise taxes, personal information was needed. Due to this, officials started to inaugurate censuses and to establish house numbers (and faced enormous headwind by many people who were concerned about their privacy at that time). At the time of political absolutism, monarchs already decided to establish identity cards to control inhabitants in specific situations. Beside the necessity of this information for tax collection, surveillance was always justified with improving public security, in our days called national security (Schmale & Tinnefeld 2014: 55ff.). This is expressed in the evolution of the police in France and Britain as well as the invention of biometrics and the fingerprinting and photographing of offenders in the 19th century (Diffie & Landau 2007: 128; Agamben 2015: 7). An increase in administering public services and the creation of welfare states led to a rising demand for personal information. This is why today some scholars describe the modern bureaucracy as infocracy (Goos et al. 2015: 54). Indeed, this process of increased public administration normalized surveillance to some extent, “whereby citizens are being increasingly and routinely required or encouraged to provide information in exchange for access to services” (Goos et al. 2015: 54).

The establishment of electronic surveillance encouraged the increase of bureaucratic structures. It was at the end of the 19th century when the first tabulating machines were invented. These machines were necessary because of a dramatic increase of data sets during the censuses: The count of the 1880s census in the USA took more than seven years. Thanks to the first tabulating machines this interval could be reduced to three years during the 1890s US census. Until the 1960s, electronic-mechanic tabulating machines and punch cards remained the primary way of information processing and were used by government agencies and companies. But the invention of the first computer in the 1940s challenged this process. In 1951, the US Bureau of the Census acquired the first commercially marketed computer. This development – in addition to the emergence of databases – made it easier
and faster to analyze data for the purpose of surveillance (Goos et al. 2015: 55).

The 1960s and 1970s can be considered as a time of general crisis. From the end of colonialism via the Cold War and Vietnam War to the beginning of the end of Fordist capitalism and the new threat through communism regimes, these developments were responded to by terms of surveillance. Specifically, the eagerness of the USA and the Soviet Union to participate in the Cold War led to the invention of powerful technologies to collect, store and process data. Hence, criminal records and other state-led databases emerged (Goos et al. 2015: 55ff.). And also “[i]ntelligence services augmented their capacities to monitor citizens through the use of information technology for the surveillance systems applied for national security” (Goos et al. 2015: 57). After the 9/11 terror attacks, surveillance practices increased. Although surveillance had been increasingly accepted as a part of everyday life before 2001 (since the 1990s the term surveillance society took shape in public discussion (Lyon 2015: 28)), heretofore it has become more obvious (Goos et al. 2015: 71 ff.).

Surveillance merely describes the process of information collection in order to manage control (Lyon 2015: 3). Surveillance, thereby, creates a power structure between the controller and the surveilled person. This power structure is always in support of the controller. This phenomenon is of increasing importance in an information society, because more and more data emerge. But the bare process of informatization of society and the collection of emerging data is not what challenges the norm of privacy. It is the normative argument that is brought forward to implement surveillance (Zurawski 2015: 14 ff.).

First and foremost, security and surveillance are two different things. Security is an even broader term than privacy. Only that much is clear: Security describes a condition. What kind of condition that can be, is dependent on the context. Hence, and unsurprisingly, security can be connected to plenty of areas and can be defined in multiple ways. By talking of security in this and the following chapters, a conception of security is meant that consists in the protection of a state’s population and infrastructure. This is the same understanding of security that is held by security agencies (Zurawski 2015: 20).
The connection of both security and surveillance resides in the usage of security as a rhetoric device to describe a condition that can only be achieved with surveillance measures. Hence, security can justify the implementation of surveillance measures (Zurawski 2015: 22). By the argumentative use of the term security, it can create a norm itself. The following case study explores the influence of the norm of security to the regress of the norm of privacy. While having taken a look at the concept of the norm of privacy, we also need to briefly consider the conception of the security norm as well as the contrast to the privacy norm.

As mentioned above, given the rise of the Cold War and the emerging intelligence capabilities of states, surveillance practices are increasingly justified with *national security*. The term was shaped by the National Security Act of 1947, which, among other things, created the Central Intelligence Agency (CIA). Albeit the term was the name of a legal act, the term was never defined29 (Theoharis 2011: 35 f.).

With the term of national security, the norm of security was constructed in a way that challenges the norm of privacy progressively. Not only because the security norm had broadened since the 1950s (Daase & Rühlig 2016: 13 f.; Katzenstein 1996: 10 f.) privacy was encountered, but also because this security norm is by definition a con-

29 One of the most exact attempts to confine this term can be found in the 1950s when efforts failed to legalize wiretapping in Congress. Accordingly, national security was delineated as acts encompassing “treason, sabotage, espionage, sedition, sedition conspiracy, violation of the neutrality laws, violation of the Act requiring the registration of agents of foreign principals, … violation of the Act requiring the registration of organizations carrying on certain activities within the United States … [and] violation of the Atomic Energy Act of 1946” (US House 1953, cited in Theoharis 2011: 35 f.).

Although the term *national security* was never defined, government officials tried from the 1950s on to introduce that term into the debate. With the upcoming and ever more escalating Cold War, state officials wanted to ensure that sufficient juridical leeway existed to ensure the permissiveness of bugging and wiretapping practices. Hence, they started to “theorize about a ‘national security’ exception to the Fourth Amendment” (Atkinson 2015: 11). As an example, Herbert Brownell, Eisenhower’s Attorney General, held that “in some instances the use of microphone surveillance is the only possible way of uncovering the activities of espionage agents, possible saboteurs, and subversive persons [thus] the national interest requires that microphone surveillance be utilized by the Federal Bureau of Investigation” (Brownell 1954, cited in Atkinson 2015: 11).
tradiction to the norm of privacy. The theoretical foundation of the security norm is the Hobbesian thinking of a state. People have to give up their freedom to gain security. Their unification creates the all-seeing Leviathan with God-like attributes protecting the people from the state of nature. The threat of the *bellum omnium contra omnes* makes the people create a state as a protection device (Schweidler 2014: 93; Hempel et al. 2011: 7).

This thinking drives the justification of surveillance, which also challenges the existing rule of law in liberal states (Opitz & Tellmann 2011). To govern, that means to ensure the security of people, visibility is necessary. Monitoring is inevitable for the Leviathan to exercise power, to create security. This kind of thinking counters the norm of privacy fundamentally, because privacy rests on the idea of Kantian autonomy. Privacy means the possibility of invisibility! The individually determined distribution of visibility is the expression of a liberal state conception with emancipated individuals. Thus, according to Warren and Brandeis, privacy means freedom, a freedom that is guaranteed by the absence of state interventions, by the right to be let alone. The ideal of the privacy norm is to secure people from the state

(Haas 2014: 29 f.; Hempel et al. 2011: 12 f.).

The development of globalization as well as the consequently emerging *risk society*, a term shaped by Ulrich Beck (1986), enhanced the security norm immensely. The emergence of a pre-crime society is the result of the will to avoid risks of the future. As a result of the ideal of precaution, more and more data are collected and shared internationally with the aim to foresee future risks; the collection activities of the NSA and the sharing of information with other agencies, disclosed by Snowden, are examples. Although there is no reliable evidence that the underlying assumption – more data, better prevention – is true, the alleged effectiveness of surveillance measures is an important argument in the public debate in favor of enhanced surveillance authorities of the state (Hegemann & Kahl 2016). This makes sense with regard to the Hobbesian theory, which is first and foremost a state concept of en-

---

30 This does not mean that the norm of privacy is in general incompatible with the Hobbesian state conception. Indeed, in a liberal state conception individuals rely also on state interventions, but interventions that secure their privacy (Hempel et al. 2011: 12).
lightenment and rationality (Hempel et al. 2011: 7). Hobbes created one of the first state theories that does not rely on transcendental arguments; the creation of the Leviathan is driven by the rational choice of the people. Hence, the justification of measures to create visibility has to rely on rational arguments.

Krasmann (2011) has shown that these developments do not necessarily end in the classical conception of a repressive surveillance state. Instead, security measures including the collection of personal data without probable cause are increasingly accepted. This is considered to be a change of the norm: Non-action is seen as too risky, permanent collection and the enduring search for risks are considered to be logical (Hegemann & Kahl 2016: 202). NSA chief Keith Alexander gave an example of this point of view when he expressed that, instead of finding the needle in the haystack, “let’s collect the whole haystack. Collect it all, tag it, store it… And whatever it is you want, you go searching for it” (cited in Nakashima & Warrick 2013).

The implementation of new surveillance tools is often justified in reference to an impending threat and the resulting necessity. Privacy concerns are often swept aside by putting security and liberty (or privacy, respectively) in the metaphor of a balance and by arguing that the necessity outweighed privacy, especially in cases of counterterrorism policy. Although the struggle for the correct balance between these two values is often conceived as age-old, President Truman made the first reference in 1951 when he designated Admiral Nimitz to head a presidential commission on secrecy by asking him to “seek the wisest balance that can be struck between security and freedom” (cited in Cullather 2015: 21). Such a commission was necessary after government programs had been revealed with the aim to secure the loyalty of civil servants in the McCarthy era and during the war against Communism (Cullather 2015: 21 f.) Although this metaphor suggests that both security and privacy interests should equally be acknowledged, this is not as obvious as it seems. Indeed, this metaphor is problematic because it takes security and liberty as a zero sum game. Thereby, it follows the Hobbesian roots, whereupon 100 percent security is only possible by giving up 100 percent of one’s liberty. And the maximum amount of liberty is only possible without any security. Furthermore, in practice this balance mostly contains the security interests of the
majority and the civil liberties of a few, which results in tipping the balance in favor of security. Additionally, whereas liberty is a present interest, security is a norm bound to future uncertainties. From the standpoint of the security norm, it is always more favorable to avoid future uncertainties instead of keeping present interests (Zedner 2009: 135ff.).

The balance metaphor is one main argumentative figure to encounter human rights norms. It aims to redefine the scope of a norm and to justify its violation or non-applicability. Especially in the following two chapters, this kind of argumentation is of importance.

Surveillance\(^{31}\) is the collection of information in order to manage control (Lyon 2015: 3). For the purpose of this paper, surveillance is defined as the routine control of human beings or their devices with the intention to protect, understand, ensure entitlement, control or influence groups or individuals (Lyon 2015: 3). This kind of surveillance can be done in two ways: personal surveillance and mass surveillance. Clarke (1988) defines both as follows:

Personal surveillance is the surveillance of an identified person. In general, a specific reason exists for the investigation or monitoring. Mass surveillance is the surveillance of groups of people, usually large groups. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organization. (Clarke 1988: 499)

\(^{31}\) Contrary to the field of privacy, the concept of surveillance is highly undertheorized. The main concept to theorize surveillance has been the panopticism Michel Foucault invented in the 1970s. His work was crucial to initiate the emergence of surveillance studies (Lyon et. al. 2014: 4 f.). Unfortunately, scholars have lacked to emancipate and failed to develop new convincing approaches to theorize surveillance. The first scholars that criticized the supremacy of the panopticon model were Haggerty and Ericson (2000). They questioned if this concept was still useful to understand modern surveillance in all possible aspects. It is also queried by economics, as they see multiple aspects of surveillance conducted by more than one actor as well as individuals shifting between being the controller and being controlled (Brivot & Gendron 2011). Horowitz (2017) voiced similar criticism. That is why some scholars avoid the term surveillance. Instead, they use new terms like monitoring and tracking. This should avoid the automatic conjecture that surveillance was performed from above, “as subjects of surveillance are monitored by those in authority or more powerful than them” (Nissenbaum 2010: 22).
Personal surveillance does not contradict the norm of privacy generally, because it is targeted. Especially in modern democracies, the need for law enforcement and the human right to privacy are balanced: A court warrant is needed for the intrusion of the private sphere of an individual. Mass surveillance, also called dragnet surveillance, is not possible without violating the norm of privacy in general. This is why I am going to concentrate on the development of mass surveillance in this chapter.

It is beyond the scope of this paper to consider every possible kind of mass surveillance. This is why one special approach should be considered. “One of the classical approaches to surveillance is the eavesdropping of communication and interaction between citizens, originally over the telephone network, but more recently also over the Internet” (Goos et al. 2015: 57). In this chapter, I will concentrate on this approach of surveillance, because it is specific enough to guarantee efficient research, and it was conducted over a long period in history, which guarantees an insight into the development of mass surveillance and privacy. Other, newer forms of mass surveillance, like the surveillance of public places by cameras (CCTV) or surveillance measures at airports, will not be considered in order to reduce the scope of mass surveillance measures I am going to talk about.

This approach is also in line with the definition of privacy in the previous chapter. According to rulings by the Supreme Court (in 1937), there exists a reasonable expectation of privacy regarding the content of phone calls. Also, the collection of metadata is considered to be a breach of the norm of privacy. Although the Supreme Court had ruled as recently as 2010 and 201532 about the unlawfulness of metadata collection, this judgment was anticipated by state officials as soon as the metadata collection came up in the 1990s, as I will show below.

Since this chapter explores the surveillance of communications and interactions of citizens conducted by a state, this chapter will mainly focus on the policy of intelligence activities, because most often they are the state organizations that are best skilled to conduct mass surveillance.
surveillance. This chiefly includes two areas of intelligence: communi-
cations intelligence (COMINT) and signals intelligence (SIGINT)\textsuperscript{33}.

Hence, in this case study we will explore the policy of mass surveil-
lance conducted by the USA – mainly by the Federal Bureau of Investi-
gations (FBI), the CIA and the NSA – through the use of COMINT
and SIGINT, that aim to monitor the communications and interactions
of US citizens as well as, in the last part of the chapter, foreigners. I will
not only concentrate on the activities of intelligence agencies but also
on the normative justification of these procedures by politicians and
officials as well as on the legislation regarding surveillance practices by
intelligence agencies.

The focus on domestic surveillance is necessary, because general
surveillance practices are commonly conducted by states\textsuperscript{34}. Since the
emergence of the first multiethnic states, state leaders have made their
officials engage in surveillance in order to learn the attitudes and plans

\textsuperscript{33} COMINT, defined as extracting information from communications, is the oldest
way of state agencies to intercept one’s privacy. The steady migration of communi-
cation from older, less accessible medias to new and more accessible ways of com-
municating has made signals intelligence (SIGINT, which means “the information
obtained by analyzing signals emitted by a target” (Diffie & Landau 2007: 93)) very
important to COMINT. The huge accessibility of communications in these days
makes experts speaking of “a golden age” of COMINT (Diffie & Landau 2007: 104).
This unfortunately very often leads to a confusion of SIGINT and COMINT
or to the constellation that one might think SIGINT was another term for
COMINT. But this is wrong, since there are other areas of SIGINT that are not re-
lated to COMINT, e.g. radar intelligence, telemetry intelligence and emissions in-
telligence. Hence, COMINT is just one aspect of SIGINT. Besides that, the main
target of COMINT is the acquisition of signals in any form (paper, radio waves,
electrical currents in wires, disks, tapes etc.), thus, COMINT can also be conducted
without using SIGINT (Diffie & Landau 2007: 88ff.).

\textsuperscript{34} A picturesque example, which makes this point very clear, is the conference in
1945 where the UN was founded. At the same time as the delegates of the world’s
nations debated in San Francisco about the foundation of the organization that
should later be an advocate to the right to privacy, the USA spied on every delega-
tion and read the telegraphs they sent to their headquarters at home. It is also no
coincidence that the UN headquarter is placed in New York. Among other reasons,
the USA wanted to encourage and simplify the work of their agents that are en-
gaged in surveillance activities (Hager 2015: 10).
of opponent states.\textsuperscript{35} Hence, there has never been a right to privacy for states. Also international law does not prohibit intelligence activities. As there is a difference between domestic and foreign surveillance, it is not surprising that in many countries two different agencies are concerned with these two practices (e.g., the MI5 and MI6 or the FBI and CIA/NSA). The Snowden revelations have caused a discussion about the validity of this fragmentation. I will address this topic at the end of this chapter; nevertheless this is a very new development. In order to reach a comparability with older forms of mass surveillance, one must first focus on mass surveillance of US citizens, because, as Mills (2015: 196) put it: “Domestic surveillance creates an inevitable collision of two legal principles and basic human instincts – security and privacy.” Thus, to find out if the norm of privacy is still in place it makes sense to look at the domestic level of surveillance.

\section*{4.2. From Roosevelt to the Church Committee}

As surveillance is an omnipresent part in and of humanity and in the history of mankind, it is unsurprising that the story of US mass surveillance starts at the very beginning of US history. When the Founding Fathers of the US created the Fourth Amendment that protects citizens against unreasonable searches and seizures, a grievance against the behavior of the British occupiers was expressed. British soldiers and officials commonly conducted general searches. The hostility against occupiers going door-to-door and person-to-person was huge;

\textsuperscript{35} There is one famous exception to this rule in history: Shortly after Henry Stimson was appointed US Secretary of State in 1929, officials told him about Japanese communication that had been intercepted and deciphered by the Cipher Bureau, informally known as the \textit{Black Chamber} and a predecessor of the NSA. His reaction to this was harsh. He judged that this behavior was “highly unethical” and concluded with a statement that should become famous: “Gentlemen do not read each other’s mail” (cited in Chesterman 2011: 1). It should stay a rare glimpse of the norm of privacy in international state-to-state relations. As a consequence, the \textit{Black Chamber’s} budget was reduced and finally closed (Chesterman 2011: 1).
the corollary was the adoption of the Fourth Amendment (Cate 2015: 39)\textsuperscript{36}.

However, this did not prevent officials of the USA to try and break this rule. The first case of mass surveillance in US history can be found during the Civil War in the 1860 s. Abraham Lincoln founded the first intelligence-collection agency in the USA, headed by Allan Pinkerton who was highly interested in a new invention: the telegraph. With the beginning of the Civil War, the government sought to gain control over the wires. In addition to that, they seized copies of all telegrams that had been sent in the last twelve months (companies held these copies for reasons of account keeping). After the war the US government continued to ask for copies of all telegrams that were sent. This caused a privacy advocacy process to be led by the telegraph companies, which wanted to assure their costumers that their communications would be private. The companies claimed that the same legal protection should be provided to telegrams as to US mail. Because the government neglected these claims, the telegram providers went to court. In 1879, the Missouri Supreme Court did not follow the approach of the telegram companies, but it ruled that request for telegram copies would have to specify the date and the subject of the message and thus prohibited a mass surveillance approach (Atkinson 2015: 8; Diffie & Landau 2007: 146 f.).

As a matter of course, this case cannot be fully analyzed with the spiral model. First, the right to privacy was not yet invented – albeit it was already in the air – and although the government tried to get access to all telegrams, telegraphs were not widespread; not every individual had its own telegraph. Nevertheless, already in this early case, after the first technical invention that made communication more accessible, one can observe a government that is not acting on behalf of the privacy norm (here: privacy as a social norm, not as a human right), and actors who activate and the advocacy process that led in the very end to the limitation of governance actions, ensuring that government actions were set straight.

\textsuperscript{36} Whereas the norm of privacy is reflected in the Fourth Amendment without mentioning the word \textit{privacy} in particular the norm of security – often used to justify surveillance – is included in phrases like “provide for the common defense” or “secure the Blessings of Liberty to ourselves and our Posterity” (Mills 2015: 196).
The second case in US history where US officials conducted mass surveillance was brought to light one century later, in the 1970s. The surveillance of suspected communists, civil rights activists and journalists had its roots in the 1930s. With the evolvement of new technical opportunities and the development of modern, technology-based intelligence agencies in the early 20th century, the opportunities for the violation of the right to privacy grew, as I will explore in the following.

Ironically, none other than President Franklin Roosevelt, one of the main supporters of the idea of universal human rights, authorized wiretapping activities, which were done by the FBI, for the first time. These wiretaps could be conducted by secret orders from presidents, Attorney Generals or the FBI director. With this authorization, the focus of FBI work shifted from pure law enforcement to monitoring subversives. This happened in 1934, the very same year in which Congress banned wiretapping in general by adopting the Communications Act, the first legal framework for such operations. FBI officials claimed that this prohibition was not valid for federal agents and that it only needed to be respected by private individuals and corporations. This is why

37 Most Western intelligence agencies have their roots in the early years of the 20th century. The reason for the establishment of such agencies was an increasing fear of spies. In the USA as well as in Europe countries feared not only that in case of war foreigners or people with foreign ancestors could hand on national secrets but also that they could act as a fifth column, always ready to support their home countries. In the USA, at the beginning of the century a need for federal capacities of criminal investigation was identified, and Attorney General Bonaparte founded an unnamed investigative bureau in 1908, which was named the Bureau of Investigations one year later. Because of domestic bombing attacks as well as the increasing fear of spies during World War I, the General Intelligence Division was founded within the Bureau of Investigations, headed by the young and ambitioned commander J. Edgar Hoover (Boghosian 2013: 71 f.).

38 The first years of domestic surveillance activities in the USA are the ones that have not been broadly studied yet. Due to the absence of a broad research literature, the first part of the following chapter is mainly based on the work of Athan Theoharis (2011), which is one of the first comprehensive works on this field (together with Greenberg 2010). Before, monographs were only covering special events of surveillance, like the surveillance of the Martin Luther King movement or Hollywood stars. The historian Theoharis is an expert on the field of FBI research. In the absence of further research, there seems no other opportunity than to rely on Theoharis’s work.
Justice Department officials continued to authorize wiretaps during criminal investigations. But the Supreme Court disagreed and ruled in 1937 that the ban of wiretapping also applied to FBI agents. Nonetheless, FBI director J. Edgar Hoover instructed his agents to continue the wiretapping. But after a second Supreme Court ruling against this practice, Hoover had reservations about continuing this performance and stopped illegal wiretapping. As a consequence, he informally pushed for new legislations maintaining that certain FBI investigations are impossible under this law, e.g., the prevention of kidnapping, espionage and national catastrophes (Atkinson 2015: 8; Theoharis 2011: 24ff.).

As one can see, denial and justification were used to circumvent the norm of privacy. At this point, we can observe the first activation of the spiral model. The government allowed an intrusion into the private sphere without a court order. Hence, the USA declined from step five the rule-consistent behavior to step four the prescriptive status where the domestic laws are still adjusted to the norm of privacy. Also the mainstream discourse upholds the norm of privacy; otherwise the actors (in this case, the President as well as the FBI director) would not fear to make their actions and supporting arguments public. But they did. This shows that the validity of the right to privacy is still accepted in general, although actors try to challenge this norm by creating a competing security norm. It is maintained that this new norm is more valuable than the existing norm and that new laws should be created to establish this new norm (new laws allowing the surveillance of possible spies). Nevertheless, when the misconduct became public, an advocacy network set in – in this case, the advocate was a plaintive one and a court, not a NGO – to punish the misbehavior, because the arguments advocating the encountering norm (security) are not valued higher by the court. Therefore, the USA rose from step four to step five again.

However, the next decline was not long in the coming: President Roosevelt shared Hoover’s view in parts and secretly authorized FBI wiretappings again in May 1940. Roosevelt was especially worried about potential German and Soviet spies in the USA. He circumvented the Supreme Court ruling with the argument that the court never made a dictum that applied “to grave matters involving the defense of the nation” (Roosevelt 1940, cited in Theoharis 2011: 27). Roosevelt
tried to build up a challenging narrative: A special area, one of national interest, exists in which the existing privacy norm cannot be applied. This moment can also be considered to be the trigger to enhance a normative dynamic that created a norm that should later be connected with the word national security. The window of opportunity for the creation of this norm was World War II.

With this argumentation, Roosevelt authorized wiretaps “on the prior review and approval, on a case-by-case basis, of the attorney general” (Theoharis 2011: 27) and only in cases that are “confined to investigations ‘of persons suspected of subversive activities against the United States, including suspected spies’ and were to be ‘conducted to a minimum and to limit them insofar as possible to aliens’” (Theoharis 2011: 27).

According to Attorney General Jackson, this was against the law, and he was afraid of a public debate in the case of discovery. In other words: He was aware of the existing privacy norm. Thus, Jackson decided that Hoover should not provide a detailed record of the secret wiretaps. Thereby, he wanted to reduce the risk of discovery. Roosevelt’s requirements for wiretapping were hereby subverted. Future Attorney Generals could only learn about existing secret wiretaps through the FBI director. In addition to that, Jackson did not demand reauthorizations of existing wiretaps. Hence, FBI agents were not required to explain after a certain amount of time if the originally stated security threat was still existent. This modus operandi was in place until the 1970s when Attorney General Edward Levi discovered these practices inadvertently (Theoharis 2011: 27).

One has to give credit to Jackson that he did not plan to uphold this procedure for an indefinite amount of time. Instead, he asked Congress in 1940 for a change to the law so wiretaps would be legal in cases of espionage. But his bid failed, and Congress did not approve of the bill proposed by Congressman Celler notably because liberals doubted that wiretaps would be confined to legitimate security threats and assumed that the government would use such a law to spy on political activists and ordinary people (Theoharis 2011: 29 f.).

The Pearl Harbor attacks in December 1941 and the following US involvement in World War II made Celler again propose a bill for the legalization of wiretapping. Expecting headwind in Congress, Celler’s
proposal limited wiretapping to the duration of the war and to counterespionage activities. But his attempt failed again. Nonetheless, the FBI continued wiretapping, based solely on Roosevelt’s secret directive, maintaining that these procedures were necessary in times of war. However, during the war the FBI engaged in wiretapping activities that had not been covered by the Roosevelt doctrine: Political activists of labor union and civil-rights movements were under scrutiny, and the FBI conducted spying on them; these mass surveillance practices were later conducted under the name Counter Intelligence Program (COINTELPRO). After World War II was ended, Hoover pushed for the authorization of these measures by President Truman. The president’s broader conception of national security threats as well as the upcoming Cold War made this attempt successful. In a letter to Truman, Hoover asked for an extension of wiretaps to cases “virtually affecting the domestic security, or where human life is in jeopardy” (Hoover 1946, cited in Theoharis 2011: 31). In addition to that, he skipped Roosevelt’s sentence that required such practices to be conducted at a minimum level. By signing this letter, Truman unleashed the FBI’s wiretapping measures. Nevertheless, the FBI actions were authorized but not legalized (Theoharis 2011: 30 f.). Because it was again a secret order that allowed wiretapping, the actors were aware of the existing norm of privacy.

In addition to this, after World War II, the USA started the intelligence operation SHAMROCK. During the war, the American telegraph companies ITT World Communications, Western Union International and RCA Global had transmitted all incoming and outgoing telegraphs to military intelligence. This was legal under wartime legislation. But military intelligence officials wanted to keep this procedure going after the end of the war. Hence, they established SHAMROCK in August 1945, and persuaded the chiefs of the telegram companies that this procedure was legal (Theoharis 2011: 162 f.). This was necessary because the norm of privacy was still in place. Whereas Western Union just handed over the telegrams of and to intelligence targets, both the ITT and RCA provided the full bulk of all telegrams they received. Analysts of the Armed Forces Security Agency (AFSA; the predecessor of the NSA) read the communications of foreigners and Americans who were placed on a watch list (Diffie & Landau 2007: 158).
It took until 1949, until surveillance hit the public debate: Judith Coplon was arrested and accused. The Russian spy Coplon was detained while meeting a Russian agent to deliver 28 secret FBI reports. During the proceedings the reports were submitted to her attorney to face the charge. Hence, the 28 reports came to light in public and it turned out that not one of it revealed national secrets. Instead, it became apparent that the FBI investigated American political activists and that the information that were obtained from wiretaps. Public furor was the result of the seeming confirmation of extensive FBI wiretapping activities and it forced the Justice Department to publish a statement in March 1949, which stated that wiretaps were only conducted “in limited cases with the express approval in each instance of the Attorney General. There has been no new policy or procedure since the initial policy was stated by President Roosevelt and this has continued to be the Department’s policy when the security of the nation is involved” (cited in Theoharis 2011: 32). Hereinafter, the White House staff scrutinized these cases and came to the result that the Hoover letter signed by Truman dropped any boundary to wiretaps (Theoharis 2011: 32 ff.).

Truman responded immediately and drafted a new wiretapping authority that restricted wiretapping to “cases where the national security requires it” (cited in Theoharis 2011: 33); furthermore, the Attorney General should be asked to assure control of these measures. But this conviction was short-lived. President Truman never executed this directive because of the high anti-Communist climate of that time, often framed as McCarthyism39. The White House came to the conclusion that it would be too costly to reduce the FBI’s wiretapping authority. Instead, they pushed Congress to legalize wiretaps to the prior ap-

39 McCarthyism was defined by President Truman in 1953 (cited in Doherty 2003: 15) as “the rise to power of the demagogue who lives on untruth; it is the spread of fear and the destruction of faith in every level of our society.” The word goes back to the Republican Senator Joseph R. McCarthy. Until today his name symbolizes the “demonic zeitgeist, a shorthand term for the stifling of free debate and the denial of constitutional rights by the imputation of communist sympathies” (Doherty 2003:14). This anti-communist zeitgeist was predated and postdated to McCarthy’s public appearance in the 1950’s. The first roots of it can be found in the 1920’s and it lasted until the end of the Cold War (Schrecker 2002: 12ff.). After World War II McCarthyism was also linked to the development of the national security term that
proval of the Attorney General, but these attempts failed again (Theoharis 2011: 33).

Here the spiral model fails to explain the developments. According to the model, an advocacy process should have set in after the Coplon case, but this did not happen. The political climate at that time blocked this process. Instead, in this climate it was of high value to spread the norm of security to other state actors.

Hereinafter, the Justice Department also internalized the security norm. According to the Attorney General, every discussion in Congress about legalizing wiretaps could lead to the unwanted result that eavesdropping is only allowed on grounds of a court warrant. In fact, this was the controversial point for an entire decade in which President Eisenhower came to power. Five times in the 1950s – in 1953, 1954, 1955, 1958, and 1959 – Congress debated about legalizing eavesdropping. Unlike the White House, the Justice Department and the FBI preferred to allow eavesdropping under the sole supervision of the Attorney General. But Congress denied authorizing these drafts. On the contrary, some Congressmen wanted wiretaps to be established by court warrants so that the privacy norm would be still unimpaired, but FBI officials heavily opposed this solution and they lobbied Congress to prevent such a result. A big discussion was held about the question of what should be defined as national security (Theoharis 2011: 34 f.). At the same time, in 1952, Truman founded the NSA, which would later become “the largest, most expensive, and most tech-
nologically advanced spy organization on the planet” (Bamford 2009: 13).

Of all these developments, the practices of the FBI remained relatively unaffected. Eisenhower won the election with a militant anti-communist stance and his Attorney General, Brownell, also reflected this point of view. In May 1954, he issued a secret directive allowing FBI officials to install wiretaps and bugs – including means of trespass. These measures of eavesdropping were authorized “in connection with matters related to internal security” (Brownell 1954, cited in Theoharis

The founding of the NSA was the result of the bad condition of US SIGINT at that time. Originally, SIGINT was in the responsibility of the Army. The Signal Security Agency (SSA) was the Army’s SIGINT collecting organization (the Navy’s organization was named Naval Security Group (NSG) and also the Air Force had her own SIGINT organization, the Air Force Security Service (AFSS)). All its intercepted material was sent to the Special Branch, a component of Army G-2, a department founded after the Pearl Harbor attacks. Whereas the Special Branch was responsible for analyzing SIGINT materials, the rest of Army G-2 worked on other materials like military attaché reports. During World War II, the Americans aggregated considerable SIGINT capabilities.

From 1943 on, the US Army’s SIGINT collections focus shifted from classical military communication to diplomatic communications because of the dramatic changes in the global geopolitical balance of power. With this shift the US wanted to win the peace, expecting massive advantages in future peace talks that would inevitably follow the war. After the war, the SSA was redesigned as the Army Security Agency (ASA) – but had one big problem: The war was over, and all the intelligence analysts were not needed anymore. 120 days after Japan surrendered, the army and navy lost 80 percent of their COMINT analysts, which were part of the SIGINT collection departments.

In 1949, the Armed Forces Security Agency (AFSA) was founded to combine the agencies of the army, navy and air force. But AFSA lacked money, personnel and equipment. Hence, they were totally unprepared for the Korean War that began in 1950. Because the AFSA throughout the whole war failed to gain essential intelligence insights into the Chinese/North-Korean communications, the CIA director, the minister of defense as well as the minister of foreign affairs demanded an investigation of these occurrences. The result was the Brownell Committee Report. This report recommended to replace the AFSA with a new unified SIGINT agency that should centralize the SIGINT effort of the US government. In October 24, 1952, Truman signed an eight-page directive, which created the NSA. The new agency was placed out of the rubric of existing intelligence agencies and was not, like all others, supervised by the CIA. Instead, the NSA was placed within the ambit of the Defense Department. The formation of this new agency happened widely unnoticed by the public – also because November 4 was Presidential Election Day: Eisenhower won against Stevenson (Aid 2009: 2–45).
In addition to that, he holds that for the FBI to “fulfill its intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest” (Brownell 1954, cited in Theoharis 2011: 38). However, also Brownell did not create detailed records of FBI eavesdropping requests and to what extend FBI officials were encouraged to carry out their spying activities. FBI agents, in some cases, did not even have to obtain permission for monitoring in advance (Theoharis 2011: 37 f.).

In the 1960s, Congress legalized eavesdropping for the first time in history – without lobbying efforts of the Johnson administration, instead with the support of Southern Democrats and conservative Republicans. The security norm was a matter of public debate, able to diminish the effectiveness of the privacy norm. Driven by a political climate of law and order in the face of a growing anti-Vietnam War and civil-rights movements, Congress adopted the Omnibus Crime Control and Safe Streets Act of 1968. This bill legalized wiretapping subject to a court warrant. Nevertheless, a big exception was made: Eavesdropping activities that were conducted to enhance national security did not require court warrants. Nothing in this act aimed to limit these wiretapping authorities of the President. Proponents of this legislation were not convinced that this broad language could prompt the President to authorize eavesdropping measures against political activists. Instead, John McCollan, the bill’s floor manager, maintained that this bill would protect the communications privacy of Americans (Theoharis 2011: 41).

The spiral model cannot explain this development. Step three of the spiral model – called tactical concessions – would demand that the USA withdraw from international treaties that call for the right to privacy or that the USA oppose them publicly. But this did not happen. As McCollan’s comment showed, politicians were convinced that with the Omnibus Act of 1968 the private sphere of Americans was protected. Furthermore, it can be doubted whether the legalization of wiretapping without a warrant for national security purposes can still be classified as prescriptive status. The Omnibus Act included very big concessions to the supporters of the security norm.
The FBI used the Omnibus Act extensively. The Bureau saw the mainly peaceful protests for civil rights and against the Vietnam War, as well as riots of black people as domestic upheaval. The FBI heavily surveilled black neighborhoods after riots in Los Angeles in 1965. Up to 7,400 informants worked in the black ghettos for the FBI until the early 1970s. The same happened with the women’s liberation movement and anti-Vietnam War movement. In 1970, the US Army “maintained files on at least 100,000 Americans” (Diffie & Landau 2007: 162). When Richard Nixon became President in 1969, his administration authorized political wiretapping within four months. Journalists were distinctively monitored by this approach of targeted surveillance, but also political opponents were spied on, which later became known as the Watergate scandal (Diffie & Landau 2007: 165).

The political attitude of the Nixon White House enhanced FBI surveillance activities. Nixon was highly concerned about the increasing activities of the student Left, which committed more than 250 bombings to protest against the Vietnam War. In August 1970, the FBI planned to intensify COINTELPRO, fearing extremist organizations plans to kidnap Government officials and their family members. Under the command of Nixon, the government even developed a detailed plan for domestic eavesdropping: the so-called Huston plan (Greenberg 2010: 70ff.). Nixon himself justified its development, citing security reasons, when he told the intelligence chiefs: “We are now confronted with a new and grave crisis in our country. Certainly hundreds, perhaps thousands of Americans – mostly under 30 – are determined to destroy our society” (cited in Greenberg 2010: 70).

White House staffer Tom Huston was put in charge of developing a plan to pool all intelligence resources to fight domestic unrest. This resulted in the proposal to conduct spying on dissenters directly from the White House. In his report, Huston acknowledged the existence of

---

41 Nixon was not the first president who authorized political spying. Roosevelt issued the very first political wiretap in 1940 when he requested the wiretapping of Henry Grunewald who was officially believed to head a German espionage ring. The investigation did not prove Grunewald to be a spy. But apart from that, the wiretapping revealed useful information about the tactics of politically isolated opponents of Roosevelt, because Grunewald cultivated contacts with those people (Theoharis 2011: 46 f.).
the privacy norm stating that “convert mail] coverage is illegal, and there are serious risks involved,” but denied to follow this norm because “the advantages to be derived from its use outweigh the risks” (Huston 1970, cited in Diffie & Landau 2007: 165). Nixon approved of this plan, but five days before it became effective he rescinded his approval. Hoover, of all people, objected to the plan because he feared public reaction in case the plan would reveal to the public; additionally, he was not open to sharing information with other state agencies (Diffie & Landau 2007: 159ff.). Nevertheless, the Huston plan can be considered to be the first well-structured plan of domestic mass surveillance activities in the USA that would have tipped the balance further in favor of the security norm. But due to concerns that a possible privacy advocacy process might be too strong, these attempts were not realized.

Over all these eavesdropping measures described above, a veil of silence was drawn. The success of avoiding public scrutiny ended in the early 1970s and, thus, activated an advocacy process. It all started with a revelation in 1970 saying that the FBI engaged in surveillance on people planning the Earth Day rally. Included in the surveillance was Senator Muskie, who was one of the speakers at that day (Christie 1972: 873). One year later, leftist activists burgled the FBI's resident bureau in Media and stole 1,000 classified documents. This was followed by the end of COINTELPRO of the FBI in spring 1971, fearing revelations. The disclosures were published one year later in several newspapers and they brought to light that the FBI was conducting surveillance on US citizens. The Freedom of Information Act suit by journalist Carl Stern resulted in the release of even more FBI reports revealing FBI's COINTELPRO. In 1972 and 1973, the Watergate scandal was brought to light: the exploitation of the resources of US intelligence agencies for political purposes – in particular, the surveillance of the Democratic Party – by the Nixon administration was uncovered. Furthermore, in December 1974 the New York Times published an article that exposed both the CIA's domestic surveillance program CHAOS and the CIA's attempt to undermine the government of Chile because President Allende had been too critical of the USA. Only a few months later, Attorney General Edward Levi had to confess that former FBI Director Hoover had maintained secret reports on activities of promi-
nent Americans (Greenberg 2010: 74; Johnson 2008: 38; Theoharis 2011: 141 f.).

These mixtures of occurrences initiated an advocacy process. The public upheaval that followed these developments resulted in the Year of Intelligence, “the year when the question of how to manage the nation’s secret agencies emerged as a key topic of debate in Washington” (Johnson 2008: 38). At the beginning of 1975, three investigative committees were created to scrutinize governmental and intelligence activities. All committees were named after their chairmen. The Church Committee (Senate), the Pike Committee (House) and the Rockefeller Committee42 (White House) investigated the occurrences. Because the Church Committee remained on the investigative trail for the longest period (16 months), it is the best known of all three committees (Johnson 2008: 39). Nevertheless, all committees disclosed several wrongdoings of the CIA, the FBI and the NSA.

With regard to the CIA, the committees exposed that the agency had opened 215,000 pieces of mail of Americans and photographed more than 2.7 million envelopes to get names and addresses. Through this procedure, the CIA generated a database named CHAOS (which was also the operation’s name) with 1.5 million names, all alleged subversives (Johnson 2008: 39; Theoharis 2011: 144).

In addition, the NSA-operation SHAMROCK was divulged, which monitored every telegraph message that was sent overseas or received from overseas. Originally created to monitor telegrams sent to the Soviet Union and to examine cables sent by foreign embassies, the NSA began to intercept all telegraph messages that were sent abroad, as

42 The official names of the committees are *The Senate Select Committee to Study Governmental Operation with Respect to Intelligence Activities, The House Select Committee to Study Government Operations with Respect to Intelligence Activities* and *The Commission on CIA Activities within the United States* (led by the White House) (Johnson 2008: 38 f.). Although an in-depth analysis of all three reports would be of high interest, there is no such academic analysis available. Furthermore, the research literature most commonly refers only to the Church Committee, although all three panels are said to have “produced impressively detailed and thoughtful reports” (Johnson 2008: 39). It would be interesting to explore and compare the different focuses and priorities of the reports (also in terms of wording). Unfortunately, it is above the scope of this book to provide such an examination.
mentioned before. NSA officials admitted in hearings to the Church Committee, that just in the last three years 150,000 telegrams had been reviewed monthly. Closely linked to SHAMROCK was the operation MINARET, which was focused on wiretapping within the USA. The communications of more than 1,000 US citizens and 2,400 foreign citizens had been intercepted (Johnson 2008: 39; Schwarz 2008: 25 f.; Theoharis 2008: 144).

Concerning the FBI, the committees disclosed COINTELPR. Many organizations had been wiretapped, infiltrated or influenced simply because of their political attitudes (particularly civil rights and anti-Vietnam War attitudes). COINTELPRO was founded in 1956 to combat Communists. But the scope expanded over time and included also members of other political groups. Although groups on the extreme right, e.g., the Ku Klux Klan, were also monitored, the program concentrated mainly on leftist groups (especially on the movement headed by Martin Luther King, Jr.). From 1960 to 1974, the FBI held files on one million Americans and investigated against 500,000 subversives (Greenberg 2010: 69; Johnson 2008: 39 f.). Senator Frank Church concluded that fault is to be found “in the long line of Attorneys General, Presidents, and Congresses who have given power and responsibility to the FBI [and other intelligence agencies], but have failed to give it adequate guidance, direction and control” (cited in Greenberg 2010: 95). All in all, three intelligence activities caused alarm: the physical collection of data and the following dissemination of these data as well as the purposeful targeting of individuals without a court warrant (Mills 2015: 202).

Government officials as well as Congress had the capability to detect intelligence activities before. At least with regard to the FBI, House and Senate were informed annually about their activities or had at the very least the opportunity to question the FBI director about measures taken by the FBI. For example, the building of political dossiers was a long known FBI practice. Hoover told Congress in 1960 the Bureau

43 Also military intelligence services were engaged in COINTELPRO activities. The Church Committee disclosed that military intelligence units collected data about groups involved in subversive activities. The army should have deployed more than 1,500 agents as plainclothes agents to watch demonstrators. All information was shared with FBI officials – which was also against the law (Dycus 2008: 165).
would hold more than five million files. Even so, Congress did not act, among other things, because their members feared the power of FBI director Hoover, who could undermine them with red-bait critic (Greenberg 2010: 95 f.). As Nicholas Katzenbach, a former Attorney General under Kennedy, put it:

Anyone contemplating an investigation of Mr. Hoover’s Bureau would have had to face the strong likelihood that Mr. Hoover would have vigorously resisted. [...] At worst, he would have denounced the investigation as undermining law and order and inspired by Communist ideology. No one risked that confrontation during his lifetime. (Cited in Greenberg 2010: 96)

This shows how strong this counter norm of security was. Even privacy advocates in Congress did not see a discursive opportunity to challenge the security norm. But this changed with the committees on intelligence practices. The reports of the three committees gave rise to broad changes in US intelligence policy. In 1976, Attorney General Edward Levi issued the so-called Levi guidelines. From then on, the FBI was prohibited to investigate so-called subversives and was limited to investigate individuals or groups that planned to break the law or could be considered as terrorists. Hence, the political beliefs of targets should not justify an investigation – with only one exception: if the target plans to overthrow the government (Elliff 1984). As a result, FBI investigations dropped from more than 21,000 investigations in 1973 to approximately 4,800 investigations in 1976. Also Congress reached a consensus that legislative steps had to be taken to prevent future abuses of intelligence resources – a sea change. “Most members of the [Church] Committee felt that when the United States ignored its bedrock democratic principles, it risked losing [...] its identity” (Johnson 2008: 42).

Hence, the Foreign Intelligence Surveillance Act (FISA) of 1978 came into force. With it, primarily domestic eavesdropping activities would be prevented as well as claims by the President for absolute authority to conduct wiretaps in the name of national security. For this, FISA requires a probable cause to make wiretapping legal. Thus, FISA

---

44 Johnson (2008: 45) provides a good overview of all accountability legislations concerning intelligence agencies in the USA from 1947 until 2006.
distinguishes foreign and domestic electronic surveillance (Bedan 2007: 429). Whereas foreign surveillance was not restricted, domestic surveillance was only allowed in cases where it is closely linked to foreign surveillance. So, “the target of surveillance need not be tied to a specific criminal offense. Instead, to satisfy probable cause, the government must show some linkage to a ‘foreign power’” (Harper 2014: 1130). It requires an approval in advance by a specially established court (the Foreign Intelligence Surveillance Court (FISC)) that has to judge if the target is an agent of a foreign power, a foreign power or an entity that is controlled by a foreign government. This court approval is needed in cases where the surveillance target is a US person who is located in the USA. Thereby, intelligence agencies have to justify the surveillance of individuals and why this person is a threat to national security. With the adoption of FISA, Congress superseded the previous major legislative framework governing wiretapping issues, the 1934 Communications Act\(^{45}\) (Atkinson 2015: 9; Hart 2008: 16; Theoharis 2011: 146). President Carter noted: “It [this bill] will assure FBI field agents and others involved in intelligence collection that their acts are authorized by statute and, if a US person’s communications are concerned, by a court order. And it will protect the privacy of the American people” (cited in Foerstel 2008: 29).

The spiral model can explain this development very well. The disclosures caused an advocacy process that pushed Congress to create in committees in order to examine the occurrences. At the end of this process Congress established rules that prohibited mass surveillance (and only allowed targeted personal surveillance) and that protected the privacy of the citizens.\(^{46}\) Although some scholars hold in the light of the history of increasing surveillance of ordinary peoples lifes that

\(^{45}\) According to some legal scholars, this loose internationality requirement causes expansive interpretations of this law by state officials. “This setting offers an ideal environment for the government to push statutory and constitutional boundaries. Indeed, recent revelations from Edward Snowden offer confirmation […]” (Harper 2014: 1124).

\(^{46}\) Whereas some scholars (Aiken 2008: 50 f.) hold that such a big discussion about the dos and don’ts of intelligence agencies never happened before and are – hence – a good result of democratic power, others (Atkinson 2015) hold that regulations aiming to limit the government’s responses to collected information are much more effective than limiting the collection of information generally.
“the Church Committee appears to have been a historical accident” (Ashby 2008: 57), this is not true according to the spiral model. It is rather a logical consequence.

4.3. From Reagan to 9/11

The results of the Church Committee and the Levi guidelines, which took effect in 1976, led to a sea change in intelligence surveillance policy. This caused a massive decline in surveillance activities of the FBI, resulting in the cessation of warrantless wiretaps 47. But this curbing did not last long.

In 1980, Ronald Reagan won the presidential election with a promise to alter Carter’s restrained FBI policies and to strengthen the fight against international Communism. Two legal documents cemented this change: Executive Order 12333, issued in 1981, and the Smith guidelines administered by Attorney General William French Smith in 1983. The Executive Order allowed the CIA and the Defense Department to conduct spying on American soil in coordination with the FBI. Furthermore, the FBI was allowed to investigate more widely by claiming the target had foreign ties. In addition to that, the term terrorist was broadened and also included non-violent activities. However, the Executive Order restricted for the first time foreign surveillance, which had to be “consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded” (cited in Bedan 2007: 430). This applied to investigations conducted abroad aiming to investigate the behavior of US citizens. Furthermore, the least intrusive investigation technique should be applied (Bedan 2007: 430 f.). On top of that, the Smith guidelines had a stake in this shift towards a national security approach. “Whereas the FBI could start an investigation under the Levi Guidelines only when ‘specific and articulable facts’ suggested a threat, the Smith Guidelines autho-

47 Although the wiretapping activities decreased enormously, they never stopped completely. The FBI continued to monitor, e.g., the Black Panther Party and the American Indian Movement. Nevertheless, considering the big picture, the results of the public upheavals in the 1970s can be seen as successful (Greenberg 2010: 117ff.).
ized inquiries ‘when the facts or circumstances reasonably indicate’ activities involving force or violence” (Greenberg 2010: 122). Smith also stated that the task of the FBI was to anticipate and prevent crime instead of elucidating crime – a first notion of the prevention approach (Theoharis 2011: 148). As a consequence, the FBI started to again investigate a huge number of individuals, claiming that they supported violence and terrorism. The lists of FBI surveillance covered the usual suspects: civil rights groups, anti-nuclear and peace movements, environmental activists as well as lesbian and gay rights groups, black elected officials and Arab Americans. Again, the USA fell from rule-consistent behavior to the state of prescriptive status.

The Levi Guidelines marked the transition in FBI practice from subversive to terrorist investigations. This reform ended open-ended probes to focus narrowly on groups who were thought to be committing crimes, especially political violence. [...] In a major change, Reagan ushered in a new era of surveillance by broadly linking domestic dissent to terrorism, falsely associating violence with peaceful [...] protest. [...] While all presidents struggle to balance the relationship between national security and constitutional rights, Reagan heavily tipped the scales away from protections for freedom of political expression. (Greenberg 2010: 115ff.)

In the following, the US indeed faced increasing terror attacks on their citizens. In October 1983, almost 300 US Marines were killed by a suicide bomber in their barracks in Beirut – one of the first religious suicide bombings against Americans. Further attacks on US embassies as well as US journalists and academics followed. The administration decided to go on the offensive, causing a new increase of the security norm (Harris 2010: 3, 31).

US intelligence agencies were concerned about the Beirut barrack bombing. Several warnings had been collected by US intelligence agencies but this information did not find its way to the US soldiers on the ground. The agents noticed for the first time, that their information should be shared to gain better results and that they must prevent such attacks. They decided to go this new preventive way secretly, without approval by the Congress, only with presidential directives and executive orders (Harris 2010: 24ff.). This indicates that the actors were aware that the norm of privacy was existent and that for them it seemed to be difficult to push for new laws in Congress.
The Fall of the Berlin Wall ended the Cold War. The communist superpower, the Soviet Union, symbolizing the main threat to the USA, eroded in the aftermath. In Washington, politicians in Congress discussed the so-called *peace dividend*, as it was debated in many Western countries. That meant a shortage of defense and military budget. Although the military spending of the USA decreased in the 1990s, this did not happen to the intelligence section. One example is the FBI: President Clinton had to explain one of the biggest expansions of the FBI in history. From 1990 to 1999, the FBI budget increased from $1.7 billion to $3.1 billion, with the highest increase in the final three years. In 1997, the FBI employed more than 11,000 agents – the biggest number in history. This increase was justified by the creation of a new enemy: the terrorists (Greenberg 2010: 151ff.).

In 1998, President Clinton appealed to the UN General Assembly to enforce the efforts to combat terrorism:

> Terror has become the world’s problem. [...] Today, terrorists take advantage of greater openness and the explosion of information and weapons technology. The new technologies of terror and their increasing availability, along with the increasing mobility of terrorists, raise chilling prospects of vulnerability to chemical, biological and other kinds of attacks, bringing each of us into the category of possible victim. This is a threat to all humankind. (United Nations General Assembly 1998: 10)

Several terror attacks had cemented the replacement of the communist threat by the terrorist threat: the bombings at the World Trade Center (1993) and in Oklahoma City (1995) as well as the Tokyo nerve gas attack (1995) and the bombing of two US embassies in Africa (1998). Through these attacks the security norm proliferated and made US politicians as well as the US public agree to a fighting-against-terrorism approach, including advocating more spying operations on Americans, although the total amount of terrorist attacks in the USA as well as worldwide decreased.\(^{48}\) But the US as the sole standing superpower

\(^{48}\) Terrorist incidents in the whole world were fewer in the 1990s than in the 1980s. Indeed, it is questionable why terrorist attacks became the main threat of the US in recent history, especially regarding the numbers of US persons who have actually been killed by terror attacks. Statistically, more Americans die of bee stings or allergic reactions to peanuts than of terrorism (Greenberg 2010: 161; Chesterman 2011: 2).
feared that they might become more vulnerable to terrorist attacks, because they remained the prime target for terrorists (Greenberg 2010: 151ff.).

One example occurred in the year 1997. At that time, only two terrorist incidences had occurred in the USA – both small letter bombs. Nevertheless, the FBI stated in the annual terrorism report that the USA would face terror threats in the near future (Greenberg 2010: 161). This threat was combined with the apocalyptic fear of the use of weapons of mass destruction by terrorists. In a report of the same year, the Department of Defense explains:

As the new millennium approaches, the United States faces a heightened prospect that regional aggressors, third-rate armies, terrorist cells, and even religious cults will wield disproportionate power by using – or even threatening to use – nuclear, biological, or chemical weapons against our troops in the field and our people at home. (Cited in Greenberg 2010: 155)

Another development that was considered a threat was the increasing use of personal computers in the 1980s and the 1990s as well as their connection through the World Wide Web49, which had been invented in 1994 (Lyon 2015: 49). To handle all this new technology, the FBI demanded the power to monitor web traffic as well as access to hard drives. By executive fiat Clinton allowed such snooping. In 1998, the FBI launched a new surveillance system called Carnivore. With it, the FBI could spy on e-mails. The system was directly implemented in the system of the Internet Service Providers (ISP) and could search e-mails for certain key words. In addition, it was possible for the FBI to demand that all data be registered to an individual from ISPs. Furthermore, the FBI began monitoring Web browsing, relying on clickstream data. These data became available to law enforcement and were not restricted by law (Greenberg 2010: 166 f.).

In addition to that, people started to use cell phones. In 1985, about 200,000 Americans used this new way of telecommunication, five years later already four million used it (Harris 2010: 72). The FBI – like other US intelligence agencies – simply feared to lose the possibili-

---

49 Because of the Internet structure, most of the information travels through US territory. For information about the history of the Internet and its technical structure, I recommend Bunz (2009) and Sprenger (2015).
ty of wiretapping, because communication had changed from the ana-
log to the digital way. They pushed Congress for authorization. In 1994, the Communication Assistance for Law Enforcement Act (CALEA) was adopted. It allowed the FBI to dictate to the phone companies how to create their system’s technology. FBI officials wanted them to design their systems in a way that would make them accessible for spying activities. But the negotiations between the FBI and the phone companies failed to reach an agreement on what should be collected because of fierce protests of the telecommunication companies. Hence, a Federal Communications Commission was set in place to judge what is appropriate. The commission ruled in the FBI’s favor and also allowed the federal agents to monitor cellular phones and track their location (Greenberg 2010: 168; Schaar 2013: 122). The legal argument of the phone companies had been that the FBI’s demands were unreasonable, because they would enhance the FBI to get much more information than with usual wiretaps. Others questioned the demands by the FBI, because in 1994 FBI agents conducted only 1,154 wiretaps nationwide, mostly for drug investigation (Harris 2010: 79).

The FBI was also continued to mention that – facing a high terrorist threat – encryption technologies enabling criminals to block police and intelligence monitoring needed to be prohibited. Some scholars hold that this debate was created by the government merely to gain more surveillance capacities, referring to the very low degree of this problem. In 1999, the FBI was encountered to encryption only 53 times (Greenberg 2010: 168). Nonetheless, President Clinton issued a presidential directive in 1993 under which the NSA developed a so-called Clipper chip that would be installed in every US phone (a kind of back door for law enforcement and national security purposes). The chip should eavesdrop every phone conversation that was done with such phones (Harris 2010: 75). When the Clipper program became public through a New York Times article in April 1995, business representatives strongly opposed the idea. They claimed that this would hin-

---

50 Laws demanding telephone companies to create their networks in a manner that makes surveillance possible also exist in many other countries in the world, e.g., in Argentina, Australia, Austria, Belgium, Brazil, Canada, Estonia, France, Germany, India, Israel, Malaysia, the Netherlands, New Zealand, Russia, South Africa, Sweden and the United Kingdom (Brown 2013: 206ff.).
der foreign customers to buy US products and that company secrets could be revealed by government officials. In the end, the program was dropped (Diffie 2007: 7ff.).

But the intelligence agencies did not only fear the new techniques, they also used them. One of the first departments that used computers to search for information and for profile building was the Army Intelligences Information Dominance Center (IDC) in Virginia. Originally, this unit was created to track cyber attackers of military systems. The analysts developed possibilities to track such people in the cyberspace (Harris 2010: 98). “Their analytic methods relied heavily on information technology ‘tools,’ specially designed computer programs that processed vast amounts of electronic data and revealed connections among people, places, and activities that the human eye and mind often missed” (Harris 2010: 99). But they quickly realized that these technologies could also be used to track ordinary people thanks to personal information that was delivered by phone metadata and by the open source information on the Internet. At the beginning often neglected, the opportunities of this intelligence unit became present to generals, senior government officials and to some members of Congress (Harris 2010: 99 f.).

Very soon analysts recognized that they had hit a legal wall. While analyzing thousands of web pages, analysts unavoidably collected data on US citizens incidentally (Harris 2010: 111). Nevertheless, in December 1999, the Army’s Special Operations Command took notice of the IDC. They needed new techniques to track an upcoming terrorist group, named al-Qaeda. One year before al-Qaeda terrorist had launched attacks on US embassies in Kenya and Tanzania. The Special Operations unit was tasked to map out and dismantle this terror organization. They wanted to study this network like a foreign army and for this they needed active intelligence that showed them where to hit. Hence, the IDC was chosen to help with this task (Harris 2010: 116 f.).

The IDC found many footprints of al-Qaeda around the world, in Europe, North Africa, the Middle East and the Far East – even within the USA. Most of the intelligence agencies were not aware of this huge spread, although most of the IDC’s information came from open sources. From now on, the IDC should take the lead in mapping al-Qaeda. The operation was named Able Danger (Harris 2010: 120ff.).
But IDC practices had also alarmed government lawyers. Already in 1999, the House Intelligence Committee took notice of the IDC and were concerned about what would happen in case of disclosure (Harris 2010: 113). Here we can observe that actors were indeed aware of the privacy advocates and, therefore, of the existing norm of privacy. Although the lawyers had huge concerns about the program, the IDC continued to work, because this was valuable to Able Danger’s aim to attack al-Qaeda efficiently. But Rear Admiral Michael Lohr, legal counsel to the chairman of the Joint Chiefs of Staff, early in 2000 noticed that the IDC would “pull together into a single database a wealth of privacy protected US citizens information, in a more sweeping and exhaustive manner than was previously contemplated” (cited in Harris 2010: 124). He observed that the Army must think carefully about how to deal with such a capacity and that this decision should involve the senior level of the Defense Department (Harris 2010: 113ff.).

This would happen in February 2000. Tony Gentry, the top lawyer for the Intelligence and Security Command, ordered the chief analyst of IDC to delete all data relating to US citizens during a 90-day period. All information was deleted51 (Harris 2010: 130 f.).

In this case, one can consider a process that follows the spiral model – pushing the norm-violating actor, IDC, from step four to the

51 The growing interest of US intelligence services and the US Army in the rising Internet structure can be observed in several cases. In 1998, the NSA opened a department for cyberattacks, called the Office of Tailored Access Operations (TAO). It aims to get access to foreign networks through viruses or even through physical break-ins (so-called off-net operations). Since the 1970s the US conduct such operations, but the foundation of the TAO was the first step toward a professionalization of such attacks (Ruhmann 2014: 41).

Thereby, the USA followed a global trend. In the 1990s, many countries discovered the possibilities of the cyber space for military and intelligence purposes against foreign countries. States around the world started to develop cyber doctrines: North Korea (in 1998), China (in 1999), Japan (in 2005), and the United Kingdom (in 2009) were among the first. Although the USA has been a pioneer in the practice of cyber attacks against opponents, the first comprehensive US cyber strategy was published in 2011 (Winterfeld & Andress 2013: 31ff.). Nevertheless, the USA has the dubious honor to be the first country that officially announced the first cyber war in history. In March 2016, US minister of defense, Ash Carter, published the first declaration of cyber war. Addressee was the Islamic State. This procedure was seen as the approach to establish the first rules for cyber wars through customary law for want of an international agreement (Kurz 2016).
rule-consistent behavior of step five. But the advocates are not INGOs or liberal states, but inside advocacy actors. A similar program, called Thin Thread, was invented by the NSA, but its use was prohibited in 1999 because of privacy concerns (Electronic Frontier Foundation n.d.b).

At the same time, in the late 1990s, phone companies like AT&T developed so-called Packet Scopes. These made it possible to create a mirror image of all contents of fiber optic cables and to measure and analyze the data that passed through the cables. All the data were stored in a data warehouse of AT&T as long as necessary for record keeping. The companies needed this for record keeping, but at the same time they were concerned about the privacy of their customers. Hence, only the headers of the packets, which showed the address information, were intercepted, not the content. The Packet Scopes were fully installed by 1997. From 2001 on, these measures were also used by the NSA (Bamford 2009: 180 f.).

Besides that, claims for more possibilities of surveillance were raised in the policy arena, because, according to the FBI, many terrorist groups had adopted a leaderless, fragmented structure. To prepare for this, the FBI changed its internal structure to enhance its predictive capabilities (Greenberg 2010: 160). Clinton justified this structural change in March 1999 in a public speech addressing the terrorist threat at that time:

The only cause for alarm would be to sit by and do nothing to prepare for a problem we know we could be presented with. Nothing would make me happier than to have people look back 20 years from now and say, ’President Clinton overreacted to that, he was overly cautious.’ The only way they will say this is if we are overly cautious, if we’re prepared, if we can keep bad things from happening. (Cited in Greenberg 2010: 162)

In his words, we can see a new security norm rising: prevention. Although the de facto terrorist threat was declining, Clinton justified the government’s measures as necessary in order to be prepared for threats that could eventually happen in the future. This pre-emptive approach was the one taken by many Western countries after the 9/11 terror attacks. Nevertheless, during the year 2000 most of the US policymakers viewed the government’s anti-terrorism efforts as inadequate and as an overreaction (Greenberg 2010: 156 f.).
In the 1980s and 1990s, concerns about serious terrorist threats grew enormously. This led to a proliferation of the norm of security and the preventive approach to security. Nonetheless, and although the security norm led to massive spending by intelligence agencies and to new efforts of surveillance by broadening the term terrorist, the norm of privacy was present and was not weakened by legislative acts, with the exemption of CALEA. Even when intelligence agencies tried to use metadata for the first time, they could only do so in accordance with the norm of privacy. An advocacy process was activated in the mid of the 1990s when the government sought to install a software to decrypt phones. In the end, this was successful. Advocacy processes of governmental authorities could also be observed in the case of the IDC practices, although the spiral model originally does not include them as advocates.

On the eve of the 9/11 attacks, the norm of privacy was even upheld by President George W. Bush, who stated in an interview on October 6, 2000: “I believe privacy is a fundamental right, and that every American should have absolute control over his or her personal information. Now, with the advent of the Internet, personal privacy is increasingly at risk. I am committed to protecting personal privacy for every American […]” (cited in On the Issue n.d.).

Despite this, intelligence services were concerned about the new technologies. In December 2000, the NSA stated in a report about the challenges of the 21st century that the increasing volumes of routing data made it more difficult to gain intelligence information. To perform their mission efficiently, the NSA would need to “live on the network” (cited in Electronic Frontier Foundation n.d.b). Thus, they already asked telephone companies to install eavesdropping equipment on their facilities in early 2001. However, the telephone companies refused this request (Bamford 2009: 178).

### 4.4. After 9/11

The terror attacks in New York and Washington on 11 September 2001 paved the way for strengthening surveillance activities conducted by
intelligence agencies – especially in the domestic realm (Nyst/Falchetta 2017: 106).

President George W. Bush argued that the fight against Islamic groups was a global war, labeling it as the war on terror: “America and our friends and allies join with all those who want peace and security in the world and we stand together to win the war against terrorism” (2001, cited in Foerstel 2008: 25). This differs essentially from the former approaches that saw terrorism as a matter of domestic law enforcement instead of an issue that needs to be combated with military means (Wesselberg 2010: 71). This point of view did not only cause the invasions into Afghanistan and Iraq but also an extension of domestic mass surveillance⁵² (Greenberg 2010: 183).

The security norm proliferated enormously. This can be observed while looking at Vice President Dick Cheney’s response to 9/11. In a decree to the CIA two month after the attacks, he advocated the security norm by introducing the one percent doctrine saying that all low-probability threats should be treated as a certainty (Greenberg 2010: 184). This kind of thinking implemented new surveillance measures. Even in public the view was expressed by experts that the Church Committee had weakened the intelligence agencies and that this contributed to the terror attacks (Ashby 2008: 57).

President Bush also agreed to the strengthening of intelligence capabilities in order to implement a new approach to security threats: pre-emption. As Bush stated after the 9/11 attacks,

> new threats also require new thinking. [...] If we wait for threats to fully materialize, we will have waited too long. [...] We must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge. [...] Our security will require the best intelligence, to reveal threats hidden in caves and growing in laboratories. (The White House 2002)

Even before 9/11 the shift from a post-crime to a pre-crime society is visible. The trend towards a pre-emptive society – “the rational for broad criminal offences and civil orders that aim to control individuals

---

⁵² Indeed, similar to previous terror attacks, the 9/11 attacks could have been prevented if information obtained by the intelligence sector would have been pieced together in the right way (Harris 2010: 150). Some scholars (e.g., Cole 2003) hold that with the war on terror a new McCarthyism was launched.
before they are able to wreck harm upon the community” (Lynch et al. 2010: 5) – was becoming apparent before 9/11 as part of the broader trend to minimize future risks. This trend consolidated and expanded in the course of the post-9/11 world (Mills 2015: 203). But for a comprehensive pre-emptive security approach it is necessary to predict the future. Therefore, intelligence became increasingly important. This has entailed the continuing blurring of borders between the functions of police, military, and intelligence agencies and to a larger extent of surveillance authority53 (McCulloch & Pickering 2010: 13ff.).

On October 26, 2001, Bush signed the USA Patriot Act. In his comment at the signing ceremony he balanced security and privacy issues:

Today, we take an essential step in defeating terrorism, while protecting the constitutional rights of all Americans. With my signature, this law will give intelligence and law enforcement officials important new tools to fight a present danger. […] Surveillance of communications is another essential tool to pursue and stop terrorists. The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones. As of today, we’ll be able to better meet the technological challenges posed by this proliferation of communications technology. Investigations are often slowed by limits on the reach of federal search warrants. (The White House 2001, cited in Foerstel 2008: 46 f.).

The Patriot Act was the direct legal response to the terror attacks that had occurred more than one month ago. In Section 802, domestic terrorism is now defined as activities involving “acts dangerous to human life that are a violation of the criminal law of the United States or of any State” (United States Government Publishing Office 2001: 376) and that are intended “to intimidate or coerce a civilian population” (United States Government Publishing Office 2001: 376) or “to influence the policy of a government by intimidation or coercion” (United

53 This development of blurring the distinction between the functions of intelligence, police and military began already in the 1980s. While the Church Committee reports still drew a clear line between laws governing domestic (and regulated) law enforcement and foreign (unregulated) national security issues, this distinction was weakened by the Reagan administration for the first time in the war on drugs. By enacting the 1989 Defense Authorization Act, the Defense Department was able to apply US command to watch the drug scene (Diffie & Landau 2007: 137 f.).
States Government Publishing Office 2001: 376). This very vague definition gives a great deal of leeway for law enforcement and intelligence agencies to conduct domestic surveillance. Originally, this definition included more than 40 federal crimes comprising computer hacking and malicious mischief. But this plan of the Department of Justice was thwarted by the Senate (Foerstel 2008: 69).

Furthermore, the Patriot Act expanded the use of so-called National Security Letters (NSL).\(^\text{54}\) NSLs are used as a subpoena coming from the administration. Any FBI field officer without authorization by a prosecutor or judge can issue them to a third party, such as telephone companies, Internet providers and financial institutions. NSLs are mainly used for gaining access to electronic communications and the person’s proceedings in cyberspace. They can “reveal how and where a person earns a living; how he spends his money; how much he gambles, borrows or pawns; who telephones or e-mails him at home or at work” (Foerstel 2008: 76). The Patriot Act broadened the scope of entities and the scope of parties that are subject to NSLs. This included “eliminating the relevance standard and the need to show specific and articulable facts; expanding the scope of investigations beyond foreign counterintelligence to also include international terrorism or espionage” (Greenlee 2008: 189). A NSL, moreover, is automatically a gag order, which means that the receiver of a NSL, who has to hand over information about a target, is not allowed to make this request public (Foerstel 2008: 76ff.). Again, terrorist threats were used to argue in favor of

\(^{54}\) Originally, the Right to Financial Privacy Act of 1978 introduced NSLs regarding to the requests of bank records by federal agents. The law was the reaction to a judgment of the Supreme Court in United States vs. Miller. The Supreme Court held in 1976 that there was “no legitimate expectation of privacy concerning transactional information kept in bank records, and therefore, subpoenas issued by government authorities for such information created no intrusion upon customer Fourth Amendments rights” (Greenlee 2008: 186 f.). Therefore, Congress extended the privacy rights to bank records. Nevertheless, the members sought to balance the right to privacy and the need for law enforcement agencies to obtain such information. They allowed, thus, the access to this information due to a NSL stating that the data holder was an agent of a foreign power. Already in this first version, the NSL was combined with a gag order prohibiting the addressee to inform the target of the subpoena. In 1986, the use of NSLs was extended to telephone company subscriber information and toll bill records by adopting the Electronic Communications Privacy Act (Greenlee 2008: 186 f.).
an extension of NSL use, as a statement by Attorney General Ashcroft shows: “For us to begin to limit the ability to use this law enforcement tool I think would expose the American people to jeopardy because we would have less capacity to enforce the law and keep people safe” (cited in Foerstel 2008: 73).

Section 215 of the Patriot Act amended the FISA Act and allows FBI agents to obtain a search warrant from FISA courts for any tangible thing without attesting a probable cause of an illegal act. Agents only have to claim that the demanded information might be important for investigating international terrorism or intelligence activities. As Senator Feingold held in the debate on the Patriot Act, “under this provision, the Government can […] collect information on anyone – perhaps someone who has worked with, or lived next door to, […] or whose phone number was called by the target of an investigation” (2001, cited in Foerstel 2008: 62). Additionally, gag orders can be issued. Furthermore, roving wiretaps were allowed in Section 206, according to a FISA court warrant. This means that law enforcement officials can follow a person or continue to wiretap this target even when the target changes telephones or communication devices (Foerstel 2008: 52).

The Bush administration’s plan was to rewrite the body of law regulating government surveillance. Nonetheless, most of the measures introduced by the Patriot Act had been demanded by intelligence and law enforcement agencies for many years and were not directly related to terrorism issues (Foerstel 2008: 30). Objections had no chance to be heard. Both Republicans and Democrats in Congress “knew that any opposition would be seen as weakness by the American electorate” (Foerstel 2008: 30). This shows that advocacy processes can be stifled by the predominant political climate.

This does not mean that there was no opposition to the Patriot Act at all. Indeed, there was a movement of resistance, which was headed by the ACLU. Soon after the attacks, they published the manifesto In Defense of Freedom at a Time of Crisis, calling politicians “to ensure that actions by our government uphold the principles of a democratic society, accountable government and international law, and that all decisions are taken in a manner consistent with the Constitution” (American Civil Liberties Union 2001). More than 150 groups supported the
manifesto, including AI, Privacy International and EPIC. Nevertheless, the act of advocacy was ignored in the post-9/11 hysteria; the ACLU’s press conference, where the manifesto was presented to the public, was sparsely attended (Foerstel 2008: 31). The prevailing sentiment that terrorist attacks could be adverted by enhanced surveillance powers prevented that this act of advocacy was heard.

The spiral model again fails to explain this turn. It provides no opportunity for something to hamper the advocacy process. Of course, it includes the possibility of low social vulnerability that prevents an actor’s advancement to the rank of rule-consistent behavior. But, according to the spiral model a weakening of the social vulnerability by the influence of a competing norm is not possible when a state has already reached the rule-consistent behavior status. But this is what was happening here: The occurrence of a terror attack on US soil weakened the social vulnerability of the USA to the efforts of the transnational advocacy network because the security norm trumped privacy concerns (at least temporarily).

As a matter of course, intelligence and law enforcement agencies immediately started to use their new powers. One of the profiteers was the FBI, which tripled the amount of investigations within a year and quadrupled the requests to eavesdrop on suspected terrorists. On the same day, President Bush signed the Patriot Act, the FBI’s Office of the General Counsel sent a memo to all divisions which was almost enthusiastic about the newly gained possibilities of surveillance. The Patriot Act inhibited counterintelligence investigations on US persons that are solely based on activities enjoying protection of the First Amendment of the US Constitution, which was highly appreciated by FBI officials:

Congress inserted this to indicate that the technique will not be used against US persons who are merely exercising constitutionally protected rights. However, it is highly unlikely, if not entirely impossible, for an investigation to be authorized [...] that is ‘solely’ based on protected activities. In other words, all investigations of U.S. persons will likely involve some allegation or possibility of illegal activity [...] which is not protected by the First Amendment. (Cited in Foerstel 2008: 42)

In May 2002, a new guideline by Attorney General Ashcroft allowed FBI agents to investigate in public spaces. That meant that FBI agents started to monitor chat rooms, bulletin boards and websites without...
any indication of criminal wrongdoings by the suspects. So-called fishing expeditions are conducted to find radical statements and to open further investigations in the case that such statements are found. This extension of surveillance practices was justified with the necessity to prevent another 9/11, although information leading to the 9/11 terror attacks was found in advance but was not analyzed in the right way (Greenberg 2010: 189). Ashcroft claimed that FBI agents had to become better “in detecting terrorist activities to the full extent permitted by the law with an eye toward early intervention and prosecution of acts of terrorism before they occur [to put] prevention above all else” (cited in Theoharis 2011: 149). The new guidelines prompted critical comments in the media, but the majority of the public and Congress accepted this new approach (Theoharis 2011: 149; Greenberg 2010: 190) – the main difference to the 1970s. This consensus strengthened the security norm.

In 2006, it became public that the FBI used cell phones as tracking devises and eavesdropping tools. Even in 2004, it became public that intelligence agencies were able to activate the microphone of a phone, irrespective if it is on or off. It was expected that this new technique called roving bug would be mainly used to spy on UN and foreign government officials (Wheeler 2004). Nevertheless, in 2003 the FBI also started to use this measure to spy on a New Yorker mafioso. This was revealed in 2006, when a US District Court ruled that this practice was legal under contemporary wiretapping law (McCullagh 2006). No advocacy process was activated.\(^{55}\)

It is obvious that the advocacy process did not work after 9/11. In a way, members of Congress anticipated that they could not act on behalf of the privacy norm directly after 9/11, because of the weak US social vulnerability of that time, but that this would be possible later on. That is why they equipped the most intrusive sections of the Patriot Act with a sunset provision. After four years, they would lose legal force. Hence, in 2005 debates started in Congress about the reautho-

\(^{55}\) Five years after 9/11, the FBI acknowledged that it did not identify one single al-Qaeda cell within the USA (Greenberg 2010: 205). In addition, in a 2009 report the FBI stated that only five per cent of the leads were credible enough to start further investigations. Between 2005 and 2006, only 19 of 150 FBI international terrorism referrals were charged by the Justice Department (Theoharis 2011: 153 f.).
rization of the relevant sections, resulting in the USA Patriot Improvement and Reauthorization Act of 2005, which was signed in March 2006.

During the political discussions of the Reauthorization Act, some politicians articulated concerns about too much surveillance power, but the Congress did not follow their arguments, although the debate was lengthy and contentious this time (Foerstel 2008: 193). Nevertheless, the majority of Congress members was convinced of the terror threat argument. As Senator Bill Frist put it: “The Patriot Act expires […], but the terrorist threat does not” (2005, cited in Foerstel 2008: 180). And deputy Attorney General James Comey said that “especially with some of these tools, if you sunset them again we will never be able to get people to completely believe that the world has changed” (2005, cited in Foerstel 2008: 196).

In the very end, only minor changes were made. The biggest change was made in regard to NSLs. For the first time provisions were put in place for a judicial overview of NSL requests (Greenlee 2008: 194). Regarding Section 215 and NSLs, Congress obtained the right to demand an annual report containing the total number of applications56 (Foerstel 2008: 187ff.). But the number of sunsets decreased. From 16 sunset provisions only two remained in place, also because Republicans were following the Bush administration’s desire to keep all authorities out of the Patriot Act. One of the contested provisions was the sunset division for Section 21557 (Foerstel 2008: 197).

Besides the legal response to 9/11, illegal responses occurred as well. Originally, to obtain a FISC search warrant, surveillance had to be targeted. But the government, as well as intelligence agencies, wanted to engage in newer approaches of data mining – the opposite of a

---

56 President Bush did not accept these requirements and rejected them in a signing statement. He reasoned that he could withhold this information as the leader of the executive branch. Nonetheless, there has been a Justice Department Inspector General report in 2007, recording massive abuses of NSLs by the FBI (Conyers 2009: 167).

57 This normalization of extraordinary measures is a trend that can be observed in many countries in the 21st century (McGarry & Williams 2010: 131ff.). Derogations from certain human rights are allowed according to the ICCPR in cases of public emergency. Only the right to life and the right not to be subjected to torture are indispensable (Chesterman 2011: 44 ff.).
targeted effort (Mills 2015: 203). In January 2002, the Defense Department’s Defense Advanced Research Project Agency (DARPA) was founded in a new department called the Information Awareness Office (IAO). The main target was to develop new tools for anticipating terror attacks and to provide warnings. One of the tools the IAO developed to reach this goal was the Total Information Awareness (TIA) program. TIA aimed to combine all the amount of personal information (of US persons and foreigners) that is accessible to all US intelligence services to identify certain structures of behavior and conduct. To put it simply, it was a tool for analyzing big data with regard to certain behavior patterns. As Tony Tether, head of DARPA, opined before a House Committee, “[…] the TIA program is designed as an experimental, multi-agency prototype network that participating agencies can use to better share, analyze, understand and make decisions based on whatever data to which they currently have legal access” (2003, cited in Lee 2015: 142). This would help to predict terror attacks, as an official IAO document states (Lee 2015: 143). Albeit private companies had developed such a program before 9/11, it was the first time that the US government was willing to employ such programs to analyze personal information regarding security issues (Lee 2015: 136ff.). In the 1990s, an approach to create a similar database, called Thin Thread, failed because of privacy concerns. But the inside advocacy process did not work completely. Rather one tried to combine both norms.

The notion that the TIA program heavily affected the privacy rights of US citizens and foreigners was clear for the idea generators. That is why the development of privacy protection technologies was one of the top priorities of the TIA. The Genesis Privacy Protection Program was developed to match this goal. While TIA and intelligence analysts should have free access to the metadata of phone calls or financial transactions, Genesis would deny access to the real name of a target without a court approval. Any access to identifying information

---

58 Harris (2010: 151 f.) shows that the war against terror was not the only purpose of this program. Already in its infancy, senior officials were aware of the potential of such a program to ease the decision-making in other fields, especially in the field of foreign policy. Furthermore, people thought about the inclusion of biometric data, such as fingerprints and image scans to TIA, which are not fitting in with the definition of surveillance in this paper.

https://doi.org/10.5771/9783628867505-39

Generiert durch IP '54.70.40.11', am 28.09.2020, 10:05:34.

Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.
would be denied in the first step by Genesis (Harris 2010: 153; Lee 2015: 136ff). General John Poindexter, chief of the IAO and main idea generator of the TIA program, highlighted the privacy issue in his resignation letter in August 2003: “We did not want to make a tradeoff between security and privacy. It would be no good to solve the security problem and give up the privacy and civil liberties that make our country great” (cited in Lee 2015: 147).

The resignation of Poindexter was necessary, because the plans for TIA became public in November 2002 through a New York Times article and faced enormous resistance in the aftermath (Lee 2015: 138 f.). The public pressure was so big that Congress stopped TIA in September 2003 by cutting off funding (Lee 2015: 138ff.). But in 2008 the Wall Street Journal unveiled that the TIA program was incorporated in a secret NSA program conducting surveillance on the international communication of Americans, the Terrorist Surveillance Program (TSP) (Lee 2015: 152).

On October 4, 2001, the Bush administration secretly started a program of warrantless wiretapping for foreign intelligence purposes. The TSP intercepted the communications of US citizens when one party of a conversation was outside the US without a FISA court obligation. The NSA conducted this eavesdropping under the codename STELLARWIND. The President as well as the Attorney General himself reauthorized the program every 45 days. The administration’s lawyers justified this program with unchecked legal authority of the President in times of war. According to them, “the President […] may initiate preventive war without authorization from Congress” (Adler 2008: 99). The deputy Attorney General John Yoo and the legal counsel of Vice President Cheney David Addington were the generators of this justification (Conyers 2009: 146 f.). This is again a main difference to the 1930s to 1970s period, when the surveillance activities were clearly illegal. At least this is argued by the President. While presidents and Attorney Generals sometimes enhanced or even ordered these illegal activities, they generally accepted these norms, because they did not

---

59 This was the first time since the 1970s that the NSA conducted domestic surveillance in a broader sense. Before, on US soil they concentrated largely on the surveillance of foreign embassies and missions as well as other missions with a FISC order (Montgomery 2008: 133 f.).
try to make new legal approaches to surveillance issues. This changed with the new approach.

A vital change in the behavior and attitude of NSA officials became noticeable immediately after 9/11. As a former NSA-employee put it: “The prior approach focused on complying with the Foreign Intelligence Surveillance Act. The post-September 11 approach was that NSA could circumvent federal statutes and the Constitution as long as there was some visceral connection to looking for terrorists” (cited in Electronic Frontier Foundation n.d.b). Only a few days after the attacks, the NSA drew on the Thin Thread plans to perform contact chaining on metadata.60 When President Bush signed his order, NSA officials strongly misunderstood it. Indeed, they believed that this order also gave authorization to collect Internet and telephone content and metadata solely of domestic US communications.61 Consequently, they started to do it. From mid-October on, the NSA approached telecommunication and Internet companies to work with the NSA on this secret program. Many companies agreed voluntarily.62 During the next two years, the NSA started to build secret rooms in the facilities of telecommunication companies to get access to all communications passing through the USA. By the end of 2003, agents of the FBI and CIA joined the program to improve the collaboration between the intelligence agencies (Electronic Frontier Foundation n.d.b).

The Attorney General certified the PSP without assessing the legality of the program, although some administration’s lawyers objected the plan. But this does not mean that Yoo and Addington were not aware of the breaking of a norm. When the NSA’s inspector general, who was informed about the program one year after it had been launched, sought access to the memoranda that served as legal foundation of the surveillance program, Addington rebuffed his request. After Yoo had resigned, the concerns about this program increased in the

---

60 The Justice Department had prohibited Thin Thread in December 1999, finding that the examination of metadata is considered as electronic surveillance under the FISA (EFF n.d.b).

61 It remains unclear since when the President was informed that in fact also metadata of domestic calls and Internet usage had been collected.

62 In June 2003, one approached company requested the legal basis for this program in a letter to the Attorney General. Three months later, the Attorney General responded that the demands of the NSA were lawful (EFF n.d.).
Justice Department as well. When the President was confronted with the imminent resignation of the level of command of the Justice Department and the FBI, he indulged (Conyers 2009: 148 f.; Electronic Frontier Foundation n.d.b):

In March 2004, the concerns of Justice Department officials became obvious. Deputy attorney James Comey was an opponent of the NSAs activities. One day before Attorney General Ashcroft was hospitalized at a time when one of the regular authorizations was becoming due, Comey told him that the PSP might be illegal. One day later, Comey was the acting Attorney General and denied to sign another 45-day extension of the program. Therefore, White House staff members raced to the hospital to pressure Ashcroft to authorize the bill – which he refused to do. Thus, the White House decided to extend the program without the approval of the Justice Department. This confrontational course caused enormous headwind: Comey as well as several top Department of Justice officials and FBI officials planned to resign. Hence, Bush rescinded the order, and the NSA stopped the mass surveillance program. In the following, FISC was briefed about the program and, after that, in June 2004, gave the first authorization to collect metadata 63 (Conyers 2009: 150; Electronic Frontier Foundation n.d.b).

In December 2005, the New York Times disclosed the official part of the program 64 after one year of investigation: “[...] the intelligence agency [NSA] has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants” (Risen & Lichtblau 2005).

63 In May 2006, the FISC broadened the scope of Section 215 of the Patriot Act, claiming that the term *business records* was defined as the entirety of a telephone company’s database. With it, the court accepted dragnet surveillance by the NSA. This caused President Bush in February 2007 to no longer sign authorizations for the NSA program because the FISC allowed to continue the program indefinitely (Gellmann 2013; EFF n.d.b).

64 Only the collection of metadata of Americans’ conversations with foreigners was revealed – hence, the official PSP. Nevertheless, the newspaper reported also about rumors that in some cases the NSA would also capture phone calls of purely domestic nature. That the NSA collects all American’s phone calls was revealed by the USA Today in May 2006 based on insider reports. Nevertheless, this could not be proved right until the Snowden revelations (EFF n.d.b).
President Bush confirmed the existence of the program and defended the program, describing it as a “vital tool in our war against terrorists” (cited in Theoharis 2011: 159). Snowden revealed later that the program also included the collection of metadata for about every phone call and Internet activity of Americans. Furthermore, Bush referenced the permission of Congress, authorizing military operations in the war against terror (Theoharis 2011: 159).

In the aftermath, an advocacy process was activated. The procedures as well as their legal justification attracted the attention of the Justice Department’s Office of Professional Responsibility (OPR), which launched an investigation into the President’s Surveillance Program (PSP) beginning in 2004 to examine if these rulings had violated the ethical and professional standards of legal profession. In 2009, they published the report stating that especially in the case of Yoo’s juridical practice misconduct had occurred. They concluded that “situations of great stress, danger, and fear do not relieve departmental attorney of their duty to provide thorough objective, and candid legal advice, even if that advice is not what their client wants to hear” (cited in Theoharis 2011: 152). The OPR report recommended to refer this case to the bar association for disciplinary actions\(^65\) (Theoharis 2011: 152).

In addition, many lawsuits were opened against the Bush administration and the telecommunication companies, like AT&T, which were said to have assisted the US government.\(^66\) Many lawmakers and civil liberties groups called for immediate action like Congressional inquiries. Legal scholars and former government officials sent a letter to congressional leaders to express their concerns, thereby especially challenging the legal justification of the President (Montgomery 2008: 124ff.).

Despite this, the advocacy process did not succeed. Although the TSP had caused a lot of public criticism, Congress did not follow up on these concerns. Instead, the members of Congress did not cut the NSA

\(^{65}\) President Bush heavily opposed the OPR investigation. Among other things, he denied security clearances to the investigating attorneys to hamper the inquest (Montgomery 2008: 143 f.).

\(^{66}\) One of these lawsuits was Amnesty International vs. Clapper, filed in 2008. In February 2013, the Supreme Court ruled that the plaintiffs could not prove that they had been monitored by the NSA (EFF n.d.).
budget (like was done with the TIA program) and they confirmed General Hayden to head the NSA in 2006, who in the same year had stated before Congress: “This [the TSP] is not about intercepting communications between people in the United States. This is hot pursuit of communications entering or leaving America […]. This is focused. It’s targeted. It’s very carefully done. You shouldn’t worry” (2006, cited in Lee 2015: 152).

Besides, Congress enacted the Protect America Act (PAA) and the FISA Amendments Act (FAA) in 2007 and 2008, respectively. The PAA for the first time allowed the surveillance of foreign-to-foreign communication on American soil if there were reasons to believe that the target was outside the USA. Because more than 80 percent of the world’s communication is processed through technical infrastructure on US soil, a FISC approval was required for every foreign target. Although the NSA had not followed this rule since the early 2000s, this rule was officially adopted through the PAA. Furthermore, conversations of US persons with people overseas were exempt from FISC approvals. Hence, the Attorney General and the director of intelligence had to approve the international surveillance operations without attesting that a person was an agent of a foreign power; the FISC only reviewed their decisions. Because the PAA’s duration was limited to six months, the FAA was adopted confirming these new measures. Additionally, the FAA excluded all cooperating telecommunication companies from criminal prosecution (Blum 2009: 295ff.; Theoharis 2011: 160 f.).

Although the Democrats held the majority in both houses in Congress – they are the party that made a major contribution to the accomplishment of the enactment of FISA in the late 1970s – many of them voted in favor of the proposed bills coming from the White House. They rationalized this decision in public by saying they acted in the name of national security (Montgomery 2008: 152). This led to the FAA, FBI and NSA getting for the first time in history the legal authority to monitor the communications of Americans with persons outside the US (Montgomery 2008: 151).

This reluctance of Congress to oppose the TSP is a subsequent acknowledgement of the Bush administration’s procedure. Blum (2009) holds that
although one can criticize the Bush administration for acting unilaterally and bypassing Congress and FISA, the underlying reasons for the TSP appear genuine and sound. If not, Congress could have taken more aggressive steps to reign in the program once it was revealed instead of passing legislation that retroactively condoned the warrantless surveillance. (296)

Indeed, the loose reaction of Congress this time is the main difference from the situation in the 1970s, and it highlights “how an obsession over security led it to cede wide latitude to the White House and the intelligence agencies, purportedly to safeguard the nation from potential threats” (Theoharis 2011: 163).

In January 2009, Barack Obama took office. Three years later, the Obama administration stopped the collection of domestic Internet metadata for operational and resource reasons (Greenwald & Ackermann 2013). A few years later, on June 5, 2013, the Guardian disclosed that an April 2013 FISC order forced the American telecommunication company Verizon to hand over to the NSA on a daily basis all metadata regarding international and purely domestic phone calls for the duration of three months (Greenwald 2013 a). Just a few days later, the Wall Street Journal unveiled that such enactments were also given to metadata of other American phone companies and Internet providers (Gorman et al. 2013). Further information showed that such enactments were given on a regular basis for years and were reauthorized by the FISC shortly before they expired (Lee 2015: 162; Schaar 2013: 123). Although rumors about such activities of the NSA already existed, government officials denied their truthfulness before the Snowden revelations. In a March 2013 Senate hearing, the Director of National Intelligence, James Clapper, responded when asked whether the question whether the NSA collected data on millions of Amer-

---

67 One may ask if the monitoring of phone call’s metadata can be considered as a questionable form of surveillance, because this kind of surveillance does not touch the full content of a phone call (it is not monitored what is said). But this point of view would neglect the huge possibilities of metadata for surveillance. The main advantage is that metadata are much easier to analyze, process and link than the content of conversations. Furthermore, while content can be encrypted, this is almost impossible with metadata. When metadata are collected over a longer period, they can tell a lot about social relationships, preferences and actual living conditions of an individual (Meister 2013: 229ff.). Some experts (Moechel 2013: 242) hold that with the metadata of a mobile phone much more things can be learned about an individual than with old-school eavesdropping measures.
cans: “Not wittingly. There are cases where they could inadvertently, perhaps, collect, but not wittingly” (cited in Greenberg 2013). NSA director Keith Alexander also testified before Congress in March 2012 that an article claiming that the NSA was conducting mass surveillance on Americans was not true. He denied these practices on several other occasions (Cate 2015: 30). This shows that the NSA never intended for this program to become public and that they were aware of the norm of privacy.

The Snowden revelations showed this collection was done under the code name STELLARWIND. Unlike its predecessor Thin Thread, it does not include any privacy protection algorithms (Mills 2015: 204). Later it was disclosed that the metadata of American e-mails were also stored until 2011. Both the bulk phone and the email metadata collection began in late 2001. In 2011, the collection of e-mail metadata was discontinued due to resource reasons, but the bulk phone data collection went on. In cases where the phone metadata of a target should be considered, this is done in two degrees of separation (two hops) (Greenwald 2013 b). Hence, the PSP never really ceased to exist.

It has become clear, from the first warrantless surveillance approach by Roosevelt to the surveillance program authorized by George W. Bush, that national security issues have been the major justification of warrantless eavesdropping.

Since 9/11, our concept of national security includes protecting domestic locations within the United States. The motivation of national security and the availability of new technology have enabled the surveillance environment in which we find ourselves today, but there has always been a motivation for national security and a thirst to use the new technology of the time. (Mills 2015: 219 f.)

Furthermore, the Snowden revelations also revealed a global mass surveillance approach, which is going to be elucidated in the following. It shows the blurring of the domestic and international spheres with regard to surveillance activities.
4.5. Foreign Surveillance

An article in the *Washington Post* revealed at the beginning of June 2013 the surveillance program PRISM. PRISM allows the NSA and FBI to collect personal data from American Internet companies – not only metadata but also content. This data includes “emails, chats, videos, photos, stored data, voice-over-IP, file transfer, video conferencing, logins, and online social networking details” (Lee 2015: 162). PRISM was raised “from the ashes of President George W. Bush’s secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority” (Gellman & Poitras 2013). Congress gave this new authority by adopting the PAA and FAA. Companies voluntarily collaborating with the NSA were free from prosecution. Furthermore, PRISM was justified, with the new FISA section 702 allowing electronic surveillance in the USA, as long as no US citizens are intentionally monitored. NSLs were used to obtain the information from companies (Mill 2015: 209ff.). Nevertheless, the privacy protection technology provided by TIA was not included in the TSP by the NSA. The data have been gained indirectly from company servers68 (Kietz & Thimm 2013: 1f.; Lee 2015: 162). The distinction between domestic and foreign is not existent in the PRISM approach; additionally, data from American citizens (domestic communications) are collected. Although the program officially has to comply with Executive Order 12333, in practice this is not the case (Wright & Kreissl 2015: 14).

Further surveillance programs were disclosed: MUSCULAR has extracted data in bulk from Google and Yahoo! servers overseas without the agreement of the companies. Copying and analyzing the data of the servers have been done without the knowledge of the companies. In addition to that, in joint programs the NSA and the British GCHQ worked together to get access to undersea fiber optic cables around the

68 PRISM started in 2007 with collecting data from Microsoft, followed by Yahoo! (2008), Google and Facebook (both 2009), YouTube (2010), Skype and AOL (2011) and Apple (2012) (Lee 2015: 162). The access is an indirect one because the NSA has no direct access to the company servers. Instead, the data are copied to NSA servers where they are analyzed (Moechel 2013: 241).
world. By using intercept probes and physical taps, the intelligence services collect everything that is sent through the fiber optic cables, including phone calls, e-mail messages, Internet history and social network contents. Metadata of this personal data collection are stored for up to one month, the content for three days. With so-called selectors, the intelligence agencies are capable of searching through this data pool and store information on targets69 (Mills 2015: 210ff.).

The reason why this information is not stored for a longer period is due to the very large storage locations that would be needed for this purpose. As a result, the NSA built a new data center that went online in 2013 and was fully operational in May 2014. This is used to store all intercepted data (Lee 2015: 158ff.).

Furthermore, the Snowden documents revealed that the NSA used covert implants to get access to computers, smartphones, network servers, firewalls and routers. The malware is able to take over a computers microphone and camera in order to take pictures and record conversations and to collect login details and passwords. While the NSA usually accesses the target machines through the Internet the agency is also able to collect data from machines never connected to the Internet by installing taps (Cate 2015: 32 ff.).

All in all, the NSA scandal unveiled three dimensions of surveillance: First, the interception of data in transit that is processed by so-called upstream programs. Second, the access to stored data, as it is done with the PRISM program. This is done in one of three ways: a NSL/FISA warrant, a private agreement between the government and the company; or by hacking into the systems (Mills 2015: 218). A third layer is the installation of spyware on personal devices like computers or smartphones (Lyon 2015: 18ff.). As a result, the distinction between mass and targeted surveillance has blurred. “If data are sought on a mass basis […] with a view to identifying who might be a ‘person of interest,’ the point at which ‘mass’ becomes ‘targeted’ surveillance is fuzzy at best” (Lyon 2015: 22). This goes so far that intelligence agencies insisted after the Snowden disclosures that the mere mass capture of data without later intervention could not be defined as surveillance (Lyon 2015: 41 f.). Another two spheres that are blurred are the dis-

69 Mills (2015: 210ff.) provides a list of all revealed surveillance programs in 2013.
tinction between state surveillance and surveillance conducted by companies, since the US intelligence agencies have direct access to the data collected by US companies (Lyon 2015: 29).

This infrastructure comes very close to a global mass surveillance of as many individuals as possible. Today, the NSA intercepts two million types of communication per hour (Lee 2015: 159). This is not the first time that such an approach of global mass surveillance is conducted. There is one predecessor: a program called ECHELON.

ECHELON was also capable of performing a total surveillance approach of virtually all kinds of technical communication. The program, set up in 1971 and operationalized by the NSA under permission of the intelligence alliance *Five Eyes*70, was “worlds away from the popular conception of the old wiretap” (Goos et al. 2015: 57) by intercepting all communications that were processed over satellite and captured all messages that were relevant for national security. First rumors about this program already existed in the late 1980s when whistleblowers and journalists reported about it. This made the EP’s Science and Technology Options Assessment committee scrutinize and report about ECHELON in 1999, leading to an EP report in July 2001 that officially revealed the program. The report was concerned about the ECHELON program and stated, “any interception of communications represents serious interference with an individual’s exercise of the right to privacy” (EP 2001). Nevertheless, the advocacy network could not push the USA and its Five Eyes allies to respect the privacy norm. The reason for this was a considerable shift in public perception: The 9/11 attacks, committed only two months after the EP’s report was published, made the public focus on security instead of privacy issues. Albeit the actual target of ECHELON was the interception of the Soviet Union’s communication and their satellite states, the program continued after the end of the Cold War – also to conduct business espionage against the Europeans (Bedan 2007: 435 f.). Documents revealed by Snowden showed that the program is still active today, although most of the

---

70 The partnership in SIGINT between the USA, the UK, Australia, Canada and New Zealand is known as *Five Eyes* and emerged in 1947. The initiating agreement, named UKUSA Agreement, was actually an agreement between the UK and the US, but as the UK colonies became independent, they joined the coalition (Bedan 2007: 435).
The NSA development of new approaches of surveillance in the 1990s was due to the fact that more and more communications were transmitted by fiber optic cables and not via satellite. Fiber optic cables transmit signals much faster than microwaves, which was important in the face of the development of the Internet and rising communications via Voice over Internet Protocol (VoIP). The global network of fiber optic cables had one crucial point: the so-called switches, “central nodes and key crossroads where millions of communications come together before being distributed to other parts of the country. […] Like border crossings, they are the points of entry for all international cable communications” (Bamford 2009: 176 f.). More than half a dozen switches had been installed on both US coasts, processing 80 percent of all international communications (Bamford 2009: 175ff.). This led to the development of the PRISM program.

But is the surveillance of foreigners on foreign soil a breach of the norm of privacy? Indeed, US law does not prohibit foreign surveillance. Until the 1970’s, foreign intelligence operations were not regulated. And even after investigations of the Church Committee following the Watergate scandal and the adoption of the FISA Act, no privacy protection mechanisms had been installed for intercepting communication of two foreigners on foreign soil (Johnson 2016: 231ff.). “This decision was not a mistake. Rather it was a deliberate policy choice, and the norm for foreign intelligence programs worldwide” (Johnson 2016: 234)\(^\text{71}\). The same is true with view respect to international law. Because of the widespread practice of espionage, “there are no specific international law norms that prohibit or regulate espionage” (Peters 2017: 163)\(^\text{72}\).

\(^71\) The question remains, if the concepts of territoriality and nationality are still useful tools to guide intelligence practices in times of Internet traffic traveling the whole globe before reaching its destination (Johnson 2016: 235ff.).

\(^72\) Nevertheless, there are other treaties and principles of international law that have been violated by the USA. According to Peters (2017: 164ff.), the USA “breached the law of diplomacy by conducting surveillance activities at and through embassies” (167) and they violated the principle of Westphalian sovereignty.
But do the non-prohibition of espionage in the international realm and the missing domestic rules on foreign intelligence automatically deny the right to privacy of non-citizens on foreign soil? Since the NSA Affair, legal scholars have been debating this question. With regard to the US constitution, some scholars (Miller 2017) conclude that it provides no rules “that can be said to clearly and definitely resolve the question of its application to foreigners or beyond Americas territorial jurisdiction” (92), others (Walen 2017) argue that there is no case law on constitutional rights clearly prohibiting the extension of such rights to nonresident aliens (NRA). “[…] in the in the wake of Boumediene v. Bush, the jurisprudence has moved in favor of extending constitutional protections to NRAs” (Walen 2017: 283).

Whereas the scope of the constitution’s application is still a matter of debate, the evidence seems much more clear in view of international law. The ICCPR, which formulates the right to privacy (and especially to informational privacy (Vöeneky 2017: 500)) in Article 17, has extraterritorial validity, because all singers declare to guarantee this right to subjects to its jurisdiction (Vöeneky 2017: 501 f.; Peters 2017: 151ff.). “[…] one has to conclude that a state’s jurisdiction is implicated even if a state merely exercises factual power on the territory of a nonstate or third party. Factual power is exercised in the conduct of espionage on the territory of another state” (Vöeneky 2017: 501 f.). Hence, if a state wants to restrict or limit the right to privacy of foreigners on foreign soil, this must be – according to the ICCPR – proportionate and in order to reach a legitimate aim (Vöeneky 2017: 502; Peters 2017: 153ff.). In addition to this, “the ICCPR protects persons against discrimination” (Peters 2017: 162), which is why the USA owes every person – US citizen or not – equal protection of the international right to privacy (Peters 2017: 162 ff.).

This interpretation of international law is not new. Already in 1988, the UN Human Rights Committee clarified that any kind of electronic surveillance and wiretapping of conversations violates international law (Peters 2017: 148).

The question remains if the US foreign surveillance activities are legitimate and proportionate – and, hence, comply with standards of international law. Especially since 9/11, the USA feel threatened by terrorists. But “a shocking insight is that many of the surveillance meth-
ods implicated by the NSA programs […] are not very effective at exposing the plans of terrorists” (Peters 2017: 162), which results in a “deep and significant intrusion on the right to communications privacy” (Peters 2017: 162), generating little benefit (Peters 2017: 162). Therefore, the foreign surveillance activities of the USA exposed by Edward Snowden can be considered as a norm violating behavior.

As shown up to this point, “security [has become] a key driver of greater surveillance” (Lyon 2015: 31), not only since 9/11. How this relates to the spiral model will be scrutinized in the next section.

4.6. The USA and a Comprehensive Spiral Model

Is the spiral model a useful tool to explain the degradation of a human rights norm? By illuminating the history of mass surveillance, it became clear that the five steps of the spiral model are not sufficient to explain the norm regression in the USA.

The regress of a human rights norm does not happen in the same way it emerges. While the spiral model is capable of covering the secret violation of a norm by government authorities (the step from rule-consistent behavior to the prescriptive status), the five categories of the spiral model do not fit to explain further norm regressions, because the next step (from the prescriptive status to the status of tactical concessions) would include the withdrawal of international treaties and national law that includes the human rights norm. On the contrary, it seems that the withdrawal from law might be a very advanced step of norm regression. The history of the struggle between the norm of privacy and the norm of security in the USA shows that the spiral model is not capable of explaining the developments.

Furthermore, the spiral model is not capable of explaining why the advocacy processes are not successful in every case. This was most obvious after 9/11: International advocacy groups joined domestic NGOs to prevent the renunciation of human rights norms. According to the spiral model, this can only be explained with the lower social vulnerability of the norm violating state. However, the general political climate seems to influence the effectiveness of the advocacy process as well.
Nevertheless, a certain structure can be observed that summarizes the developments in the USA, which can be theorized in a second spiral. To get a comprehensive model of how states are prevailed to comply with a norm and how this development is inverted, such a second spiral seems necessary. By reference to the case study presented in this chapter a spiral \( B \) can be proposed. The different stages are not selective but fluent, as it is the case with the original spiral model. A certain framework can be deduced from the development of mass surveillance in the USA; it consists of five steps – similar to spiral \( A \) of the spiral model and, therefore, compatible.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Abolishment</td>
<td>The norm is rejected and discarded</td>
</tr>
<tr>
<td>2) Concessions</td>
<td>The state reluctantly concedes to the norm</td>
</tr>
<tr>
<td>3) Equilibrium</td>
<td>The state finds a balance between the norm and its interests</td>
</tr>
<tr>
<td>4) Circumvention</td>
<td>The state finds a way to act in opposition to the norm</td>
</tr>
<tr>
<td>5) Rule-consistent behavior</td>
<td>The state complies with the norm</td>
</tr>
</tbody>
</table>

Diagram:

Fig. 1) The Comprehensive Spiral Model

5) **Rule-consistent behavior:** This phase is equivalent to step five of the original spiral model. A state has ratified international treaties, accepting the human rights norm, and acts on behalf of this norm. Furthermore, the state has included this norm in domestic jurisdiction and acts on behalf of this norm without questioning it.

Since the USA began to violate the privacy norm from the moment of its juridical implementation, the country has literally never reached this status. Only for a very short time after the Church Committee hearings this status can be assumed.

4) **Circumvention:** Some state authorities or politicians start to act in a way that contradicts a human rights norm. Their behavior is led by a counter norm that objects the human rights norm. Nevertheless, a majority of the public as well as a majority in the political arena does not support this counter norm. Attempts to implement the counter norm in domestic or international jurisdiction fail. Nevertheless, the actors advocate the counter norm in public and a first diffusion of the
counter norm sets in. Because persons and authorities acting on behalf of the counter norm are aware of the prevailing political climate, they try to conceal their acts. By doing this, they show awareness of the prevailing human rights norm: They hide their actions to circumvent the human rights norm, because they fear future prosecution and because they know their actions are not accepted. This behavior continues until the very last step of spiral B. The more the counter norm spreads, the more actors acting on behalf of this norm feel vindicated and continue their secret acts or extend them. Not until the human rights norm is dead, unrestricted behavior on behalf of the counter norm is possible. Furthermore, the violation of the human rights norm does not necessarily have to become public. Inside advocacy actors, i.e., actors inherent to the state level, like supervising boards, civil servants (e.g., lawyers) or individual politicians, can prevail the norm violating procedures and ensure that these measures are stopped.

In reference to the history of mass surveillance in the USA, this phase can be observed from the early years of Roosevelt until the early 1950s and from the Reagan administration until the 1990s. Roosevelt’s justification of surveillance for the defense of the nation developed in the Truman era into a comprehensive approach to national security, but the security norm did not challenge the privacy norm considerably. And although surveillance measures were extended in the Reagan years because of security concerns, the security norm was inasmuch not a considerable part of public discourse, because the privacy norm was not challenged publicly. Both periods show an existence of the counter norm of security and politicians and authorities acting on behalf of this norm. Although terms like subversive and terrorist were shaped and broadened over time to justify the departure from the human right to privacy in the name of national security, Congress did not pass any laws that reduced the validity of the human right to privacy. The attempts by Roosevelt, Hoover and Celler to push Congress to adopt such laws failed. Instead, they had to hide their actions, which did not comply with the privacy norm. But nevertheless, albeit a counter norm was present the majority of the public and state actors were not convinced to cut privacy rights in favor of gaining security.
3) Equilibrium: This phase is characterized by finding a compromise between both the human rights norm and the counter norm. The counter norm continues to spread and resonates significantly. Nevertheless, both norms are now more or less equally acknowledged and represented in public and in the political arena. This can lead to the enactment of laws or treaties that try to combine the requirements of the two norms. Another possibility to reach equilibrium is to suspend the human rights norm temporarily. This shows that the counter norm is only accepted in a specific situation – e.g., in case of an emergency. This does not have to be against international law. In case of the privacy norm, a temporary suspension of this human right is acceptable and legal in special situations.

Generally, the human rights norm is not rejected. In this phase, it is less likely that internal advocacy actors initiate advocacy processes, because actions on behalf of the counter norm are to a certain extent legal, and many more people on the state level are advocating the counter norm, in this case: the norm of security. Hence, it is less likely that inside advocacy actors initiate spiral A. Additionally, the successful initiation of the spiral is not granted, because the social vulnerability of a state often decreases with the adoption of a contradicting norm.

This phase can be observed in the case study from the 1950s (the adoption of the Omnibus Crime Control and Safe Streets Act) until the early 1970s, when an advocacy process initiated by the press and NGOs led to a sea change in the intelligence policy of the USA and pushed the state to a rule-consistent behavior, and from the mid 1980s until 2007.

With the Coplon case, the security norm spread significantly in the apparatus of state. The discussions in Congress in the 1950s about the legalization of wiretapping are an example of the noticeable resonance of the security norm in the public space. This was followed by the adoption of the Omnibus Crime Control and Safe Streets Act in 1968. In retrospect, the Act was a very naïve try to combine both norms: It was a commitment to the right to privacy and – by allowing wiretapping for reasons of national security – a commitment to the norm of security.

In the 1980s, the USA again entered the stage of equilibrium. Although the Huston plan was almost a step towards the stage of conces-
sion, it was not implemented for fear of an advocacy process. In the Clinton era, the security norm resonated in public in the form of an advocacy process (by the government) in favor of a preventive security state. The adoption of the CALEA is an expression of it. Other initiatives, like the Clapper program, failed. However, the events of 9/11 pushed the security norm enormously. But the Patriot Act was not a general renunciation of the right to privacy. Many senators and representatives were aware that they only wanted to limit the right to privacy and other civil and human rights temporarily to respond to the terrorist threat effectively. That is why many provisions curtailing privacy were equipped with sunset provisions. Furthermore, although the counter norm diffuses at the state officials’ level, there still exists a considerable amount of officials upholding the human rights norm. This is symbolized by the dispute between the Bush/Yoo camp and the Comey camp in 2004.

An attempt to combine both norms was not only made by jurisdiction but also by the intelligence agencies. The development of TIA is an example of the development of a surveillance system that complies with the privacy norm. After the stoppage of the IDC through inside advocacy actors, TIA was developed as a system that tries to combine both norms, but it did not survive the activation of the spiral model in the aftermath of the disclosure by a newspaper article.

Even public statements showed the equal awareness of both norms. In the signing ceremony of the Patriot Act, Bush noticed that this act would defend both security and civil liberties of Americans.

2) Concession: By entering this phase, advocates of the counter norm have gained mastery. Concessions are made to them by the implementation of the counter norm in legislation at the expanse of the human rights norm. The laws and treaties providing the basis for the human rights norm are restricted – but not completely canceled. For certain situations or individuals the human right is not valid any more. The social vulnerability of a state further decreases. State authorities are increasingly acting on behalf of the counter norm. In public discourse, the counter norm is generally accepted.

The USA reached this phase with the adoption the PAA in 2007 and of the FAA one year later. The revelations from the end of 2005 did not led to rule-consistent behavior. Instead, PAA and FAA restricted
the right to privacy as being valid only for the domestic communications of Americans. Intelligence agencies began to work on behalf of these new laws. Furthermore, phone companies could not be sued for any actions violating the privacy norm. The acceptance of secret surveillance activities on Americans by the FISC can also be classified at this stage (although it happened already in 2004), because it shows that arguments in favor of the counter norm (in this case, by the NSA) influences decisions of judges and actions of human rights oversight mechanism (!) enormously (in this case, of the FISC court).

1) Abolishment: In this phase the human rights norm is dead. Treaties or laws advocating this norm are abandoned. State officials officially deny the validity of the human rights norm, and state authorities stop acting on behalf of the human rights norm completely. No illegal and secret actions on behalf of the counter norm are necessary anymore, because the human rights norm is overcome.

This phase was developed in theory and without evidence of the case study on the USA. Nevertheless, this would be a logical consequence of this development. At least theoretically, the Snowden revelations could cause the USA to enter this phase – similar to the development in 2007, when revelations did not lead to a behavior that is more rule-consistent. In the public discussion, it is theoretically possible that the privacy norm is further weakened by normative arguments on behalf of the security norm and that the existence of the surveillance programs unveiled by Snowden are accepted in the end. How likely this is going to happen, will be explored in the next chapter.

All in all, this second spiral can explain the development of a state from complying with human rights to differing from this norm. Nevertheless, it is merely a first attempt to theorize this evolution. This second spiral has to be verified by further case studies, as a matter of course. Of peculiar interest would be the question whether this model also applies to strong norms like the prohibition of torture.

It is questionable if this model can be used to explain the international condition of a human rights norm. The programs ECHELON and PRISM, conducted by a multilateral intelligence cooperation network led by the USA, can merely be considered as a first attempt to circumvent the norm of privacy (spiral B, step 4, ‘circumvention’). The diffusion of the security norm at the international level did (at the time
of writing) not influence existing international human right treaties with regard to weakening the norm of privacy. Prima facie, this seems to be in line with the findings of McKeown (2009: 11) whereupon a norm is first encountered in the domestic arena, and afterwards this development reaches the international level. But there are also counterarguments to that: The norm security has widely spread in the last decade at international level, which would actually demand to classify the condition of a norm as weaker than the stage of circumvention. Nevertheless, because the spiral model was developed to explain domestic policy changes, problems to explain the norm regression in the international sphere are not surprising.

Furthermore, the proposed framework fails to explain the interdependencies of state actors and advocacy networks that are fundamental to the original version of the spiral model. It is beyond the scope of this paper to illuminate the advocacy actors in every single phase; instead, the state behavior was central to this case study. This has to be done by further research. Merely one conclusion can be drawn with regard to this: The level of non-compliance influences the mechanisms of social actions, particularly coercion and persuasion. First, the higher the degree of non-compliance, the harder it is for domestic and international advocacy groups to enforce human right norms legally. Once the domestic law is changed, it is more difficult for advocacy groups to enforce a human right in court. Second, with the increasing acceptance and influence of a counter norm to the policy of a state, it gets harder to convince a state to comply with a human rights norm. Mostly, this goes hand in hand with the diffusion of the counter norm in the public.

The original spiral model has to be expanded by one more facet. As the case study shows, there are some examples where the transnational network is activated but failed to push the state to a rule-consistent behavior. The original spiral model does not provide an explanation for this. As the case study showed, it is very often the political climate that prevents a successful iteration of the spiral. To include this possibility in the spiral model, it is necessary to add one more scope condition: the discursive opportunity. Whether an advocacy process is successful or not, is dependent on the existence of a window of discur-
The original spiral model merely contains the scope condition of social vulnerability. However, it is not only the social vulnerability of the state but also of the society and public that decides about the success of an advocacy process. The question if spiral A can be activated, if the advocators are able to pressure a state to a rule-consistent behavior will be dependent on the prevailing discourse in the public domain. A temporary change in discourse in favor of the human rights norm triggered by revelations or public discussions about new laws (tipping point) is necessary to guarantee the success of spiral A. Thereby, the comprehensive spiral model can explain that norm-violating procedures survive their disclosures in cases where such a discursive opportunity is not existent (a main point of criticism to the spiral model by McKeown (2009: 10)).

At every stage of norm regress, discursive windows of opportunities (like exposures of norm violations) can emerge and be used to activate the spiral A. This is symbolized in the chart by the intact arrows. However, if the advocacy network is not successful in pressuring the violating state to the prescriptive status, the norm regress is not stopped and can continue. This is symbolized by a line between the steps of tactical concession and prescriptive status. If the prescriptive status is reached, two possibilities exist: the further development of rule-consistent behavior as well as the immediate challenge of a norm by counter norm entrepreneurs, which would directly lead to a stage of

---

73 The theory of discursive opportunity has its roots in the concept of political opportunity. This concept wants to highlight that the success of social movements is not only dependent on the actors and actions of social movement groups but also of the political framework and circumstances in which the movement acts. In other words, a political opportunity refers to “aspects of the political system that affect the possibilities that challenging groups have to mobilize effectively” (Giugni 2009: 361). Charles Tilly (1978) made the most important contribution to make this approach circularize in research literature, because he was the first to come forward with a comprehensive approach. Nevertheless, this approach was criticized enormously for its vagueness; it was in danger “of becoming a sponge that soaks up virtually every aspect of the social movement environment” (Gamson & Meyer 1996: 275). In response to this critique, scholars started to further specify the concept. One result was the development of the discursive opportunity approach. It purports that there is “a discursive side relating to the public visibility and resonance as well as the political legitimacy of certain actors, identities, and claims” (Giugni 2009: 364). This is meant when I refer to discursive opportunity here.
circumvention. These two possibilities are symbolized by the broken arrows in the chart.

Whereas this chapter has focused on how the development of non-compliance with a human rights norm is possible, the next chapter will explore the actions of the advocacy network after the Snowden revelations and, hence, will focus on the second research question. Following the comprehensive spiral model, the revelations give the opportunity to activate spiral A. The next section will show if this happened.