
This chapter is going to throw light on the advocacy process that followed the Snowden revelations. It will explore what kinds of mechanisms and modes of social action have been used by human rights advocates to pressure the USA to comply with the human right to privacy. The spiral model differentiates four such modes: coercion (use of force or legal enforcement), changing incentives (sanctions and rewards), persuasion (by discourse) and capacity building.

The main contributors to the international human rights regime should be explored: liberal states, IOs, and (I)NGOs. As a matter of course, not all advocates can be scrutinized here; instead, I focus on a few of them. When I look at the liberal states, I will focus on the states that advocated the right to privacy the strongest. Regarding the IOs, the behavior of the three most important actors will be analyzed: First of all, the UN is the organization that has made the biggest contribution to the establishment of human rights in the international system. Hereafter, the EU as well as the CoE will be scrutinized. As mentioned in the third chapter, they have both been relevant actors in the establishment of the right to privacy. Last but not least, NGOs should be highlighted. AI is one of the biggest international human rights organizations and, therefore, a good example to use to explore the advocacy process at the international NGO level. Although the behavior of all actors will be scrutinized separately, their activities are interdependent as a matter of course (Nyst/Falchetta 2017: 109).
5.1. Liberal states

The strongest commitment to privacy has been made by Brazil and Germany (Nyst/Falchetta 2017: 105). Together, both initiated a UN resolution on the right to privacy in the digital age.

Brazil's president Dilma Rousseff canceled a September 2013 visit to the USA and instead delivered a speech at the UN, which was the most direct response of a state leader in public. Rousseff noted:

The right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country. [...] In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. [...] We expressed to the Government of the United States our disapproval, and demanded explanations, apologies and guarantees that such procedures will never be repeated. [...] Brazil, Mr. President, will redouble its efforts to adopt legislation, technologies and mechanisms to protect us from the illegal interception of communications and data. My Government will do everything within its reach to defend the human rights of all Brazilians and to protect the fruits borne from the ingenuity of our workers and our companies. The problem, however, goes beyond a bilateral relationship. It affects the international community itself and demands a response from it. Information and telecommunication technologies cannot be the new battlefield between States. Time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war [...]. For this reason, Brazil will present proposals for the establishment of a civilian multilateral framework for the governance and use of the Internet and to ensure the effective protection of data that travels through the web. [...] Harnessing the full potential of the Internet requires, therefore, responsible regulation, which ensures at the same time freedom of expression, security and respect for human rights. (Rouseff 2013: 158 f.)

Rousseff argued on the basis of human rights. Brazil has acted on their notice and adopted new legislation to strengthen privacy protections for their own citizens. In 2014, Rousseff signed a Civil Rights Framework for the Internet into law that requires the government to decide if an Internet provider is acting fairly and protecting consumer’s privacy. Among other things, Rousseff promoted legislation forcing global Internet providers to store the customer data of the Brazilians inside Brazil. In February 2014, Brazil and the EU decided to build their own undersea cable between Portugal and the Brazilian coast. Additionally, Brazil hosted a global multi-stakeholder meeting, NETmundial, where
participants discussed the future of Internet governance (Fidler 2015 a: 157; Wright & Kreissl 2015: 25 f., 29; Sales 2015).

In Germany, concerns about mass surveillance of the communication of Germans were also huge. They caused an increased effort to strengthen the right to privacy at the international level, which found expression in the support of a UN resolution. But also at the bilateral level, Germany delivered consequences. The German government terminated an intelligence treaty with the USA from the Cold War era. Furthermore, Germany tried to negotiate a so-called no-spy agreement with the USA and minimized the cooperation of German and US intelligence agencies. The government did not renew the contract with the US telephone company Verizon because of security concerns (Fidler 2015 a: 160; Connolly 2015).

Nevertheless, German Chancellor Angela Merkel did not push publicly for stronger protection of privacy rights. She tried to minimize the incident and reminded the Germans of the important role of the USA in post-War German history. After it became public that the NSA had intruded on her own privacy by monitoring her phone, however, she proved to be more concerned in public74 (Wright & Kreissl 2015: 30). Her strongest public reaction was: “Spying on friends – that does not work” (Roth & Gathmann 2013).

In 2014, the German Parliament, the Bundestag, launched an investigative committee on the NSA affair. The result was a research report published in June 2017, stating that the USA did not conduct mass surveillance, because their activities had not been executed without probable cause (the parliamentary opposition dissented from this assessment) (Deutscher Bundestag 2017: 1214ff.; Biermann 2017 b). The main findings of the investigative committee had been the collaboration of the German intelligence agencies, mainly the Bundesnachrichtendienst, with intelligence agencies of the Five-Eyes member states (Biermann 2017 a). As some scholars hold (Peters 2017: 168 f.), these surveillance activities of German (and other European) intelligence agencies – as they were brought to light by the committee

74 Besides that, the Bundestag as well as a few other Parliaments in the world (Canada, United Kingdom) launched inquiries. In all countries the committees faced the refusal to cooperate by foreign and domestic officials and, partly, their own governments (Gill 2015: 84; Gebauer et al. 2013).
– probably violated the European Convention on Human Rights by “concluding bilateral agreements with the United States, by tolerating US activities, and by engaging in surveillance programs themselves” (Peters 2017: 169).

Because of the intermingled relationship of the Bundestag and the German government, which is typical of parliamentary democracies, the success of this committee largely depended on the parliamentary opposition (Miller 2017: 72 f.). Nevertheless, it seems that the parliamentary opposition succumbed in the debate about the consequences of the findings of the inquiry: In October 2017 the Bundestag adopted a new intelligence law establishing new oversight mechanisms but also – according to critics – largely legalizing the wrongdoing of the German intelligence agencies (Biermann 2017 c; Heißler 2017).

Besides Germany, other European states were concerned as well. France’s Minister of Foreign Affairs, Laurent Fabius, noted that this kind of espionage would be not acceptable. The reaction of the United Kingdom was relatively muted. The Information Commissioner stated that the conduct of the USA might contradict European data protection law (Wright & Kreissl 2015: 9 f.).

There were plenty of other states complaining about the NSA surveillance measures, not only liberal states with rule-consistent behavior. However, this does not automatically result in a commitment to privacy. One example is a statement of the Chinese National Ministry of Defense demanding that the USA to stop surveillance activities.

For a long time, the relevant agencies of the United States have relied on its advanced technology and infrastructure to carry out large-scale, organized cybertheft, bugging and monitoring against foreign politicians, businesses and individuals. These facts are known to all. The hypocrisy and double standards of the United States regarding Internet security issues have been abundantly obvious from WikiLeaks to the Snowden affair. The Chinese military is a serious victim of this kind of US conduct. [...] China demands that the United States [...] immediately stop such activity. (Chinese National Ministry of Defense 2014: 165)

It is remarkable that the Chinese Ministry of Defense complained about US surveillance practices without even mentioning the word privacy. There is talk of Internet security instead. This makes sense when it comes to the prioritization: Cybertheft as well as spying on politicians is first mentioned. Only afterward, the mass surveillance on individu-
als is expressed. Although many states are concerned about the US surveillance practice, one can assume that a big part of international complaints is driven by the strategic interests of those states (against US interests of cyber security matters) instead of a true commitment to the human right to privacy (Fidler 2015a: 164).

All in all, the reaction of liberal states was considerably weak. This is due to both lacking of political will and missing or inappropriate tools to punish the norm violation by the USA. First of all, two of four modes of social action are not available to liberal states or inappropriate in use. Since the USA is a consolidated democracy and, thus, is not lacking limited statehood, capacity building is not appropriate. Furthermore, it would be questionable what kind of capacities should be enhanced, as the definition of privacy and how to protect this human right are highly controversial even between European states. Coercion is also not a possible tool to use. The use of military force would be inappropriate, because mass surveillance is not a classical military attack. On the other hand, there are no supranational legal institutions (e.g., like the International Criminal Court) available that would be responsible for punishing the violation of the right to privacy within the means of law.

Therefore, the only modes of social action, which are possible, are persuasion and changing the incentives for the violating state. However, no state imposed sanctions against the USA or used other measures to influence the utility calculation of the USA in a positive or negative way. Although many states reacted with domestic consequences (terminating contracts with US companies and intelligence agencies or adopting laws to enhance domestic privacy regulation), these measures did not so much aim for influencing the utility calculations of the USA as at minimizing the US power base regarding the Internet. The planned installation of an undersea fiber optic cable between Portugal and Brazil is a good example of it. This action does not aim to change US behavior but their possibilities of mass surveillance.

75 The effort of states to prevent communications from travelling through the USA could lead to a so-called balkanization, which means a regionalization of the Internet. As some scholars hold (e.g., Gill 2015: 79 f.), this development is unlikely because of the high social and economic costs.
To make matters worse, domestic consequences are not necessarily a pure commitment to privacy. For example, albeit the new Internet law in Brazil was adopted with the intention to protect the privacy of Brazilian Internet users, Sales (2015) observes that the Snowden revelations were used by the Brazilian government to increase state control over the Internet. This action does not constitute a confession to privacy as such, because a lot of authoritarian countries, like China or Iran, also have huge control over the Internet (Krieger 2014: 346) and do not use this power to enhance privacy protection. The new German intelligence law is another example. Hence, one has to await further developments and the usage of the new state competences by Brazilian security and intelligence authorities until one can fully judge the Brazilian and German commitment to privacy. On the whole, the domestic measures taken by liberal states cannot be seen as primarily targeted to changing the incentives for rule-consistent behavior.

However, theoretically stronger actions by liberal states could have been taken in order to advocate privacy. There are two reasons why this did not occur. First, there is a lack of concepts and rules for privacy as well as for behavior in cyberspace. There is no clear concept of privacy and no clear measures to successfully fight terrorism. Thus, it would be difficult to determine in which case possible sanctions should be lifted (Kietz 2013: 6), and that impedes coordinated and united actions of liberal states against the USA. Furthermore, a big part of the revealed mass surveillance practices (particularly the PRISM program) are not far away from what other countries do: They are also in control of their domestic communication system and demand that telephone and internet providers to develop their collection techniques in a way that is accessible for the government and to deliver information in cases of national security threats (Krieger 2014: 345). However, they do not store it and access this source only for targeted surveillance practices. Last but not least, there is no regime for the governance of cyberspace. For a big part, the states’ behavior in cyberspace is driven by anarchism until today (Gill 2015: 78).

Second, almost all liberal states cooperate with USA intelligence services. With the existence of the SIGINT alliance Five Eyes, Australia, Canada, New Zealand and the UK are automatically norm violators as well. Beyond that, other liberal states’ intelligence services – e.g., of
France and Germany – also have close relationships with the NSA (Smale 2015). The main problem is that this cooperation is not on equal footing. No Western intelligence service exists that does not rely on the NSA. Hence, a big power asymmetry drives the relationship between the NSA and other liberal states’ intelligence services. To make matters worse, all states are in competition with each other for the best relationship to the NSA (Kietz 2013: 6 f.; Krieger 2014: 345 f.). Hence, the credibility of possible advocacy activities of liberal states is weakened enormously. That influences both the use of sanctions and discursive measures.

Persuasive and discursive measures are not fully available to liberal states’ network either. Although the statements of liberal state leaders – particularly those from Rousseff – are the first step of persuasive measure by declaring the US behavior as norm violating and countering the mass surveillance practices with arguments (the universality of human rights), no long-term process of discussion has set in. This is due to the very heterogeneous understanding of privacy. To enter a long-term discussion with the norm violator USA, the community of advocating liberal states would need a definition of privacy that is shared by all of the actors. Moreover, the aforementioned weak credibility, which is caused by the norm violation of many liberal states, undermines possible persuasive measures. Unsurprisingly, Rousseff called for a multi-stakeholder approach to resolve the problem. It is, by the way, remarkable that most of the criticism of liberal states covered the surveillance of foreigners instead of criticizing the violation of privacy rights of American citizens in the same way.

All things considered, the liberal states have failed to set in motion any mode of social action in a comprehensive way. Although it has turned out that they prefer the mode of persuasion and discourse to react to the norm violation of the USA, they are not able to use this method effectively. For this reason, it seems that they rely on IOs to solve this problem because IOs seem more capable of doing so.
5.2. **International Organizations**

As aforementioned, the liberal states put much effort in activating IOs – particularly the UN – to react to the norm violation by the USA. Nevertheless, IOs are also by themselves strong advocates of human rights laws. In this section, the reaction of three IOs will be addressed: the UN, the EU, and the CoE.

### 5.2.1. **United Nations**

The only mode of social action that is possible at the UN-level is the one of persuasion and discourse. For coercive measures or the raising of sanctions, a resolution of the UN Security Council would be necessary. Because the USA holds a right of veto in this body, it is not possible for the UN member states to use coercive measures against the USA without their consent. Discursive measures, hence, are the only way for the UN to go.

In December 2013, the UN General Assembly (2013) adopted resolution 68/167 initiated by Brazil and Germany. The resolution recognized the right to privacy as set out in the UDHR and the ICCPR and

1. Reaffirms the right to privacy [...] and the right to the protection of the law against such interference [...];
2. Recognizes the global and open nature of the Internet [...];
3. Affirms that the same rights that people have offline must also be protected online, including the right to privacy;
4. Calls upon States: (a) To respect and protect the right to privacy, including in the context of digital communication; (b) To take measures to put an end to violations of those rights [...]; (c) To review their procedures [...] including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law [...]. (United Nations General Assembly 2013)
Furthermore, the resolution asked the UN High Commissioner for Human Rights to provide a report on the protection of the right to privacy in relation to the surveillance practices of states. Half a year later, in June 2014, this report – which is called the “yardstick against surveillance” (Nyst/Falchetta 2017: 108) by privacy activists – was issued. In his report, the Commissioner clearly argues that the current surveillance practices by some states violate the right to privacy. Albeit the report agrees to the argument that electronic surveillance can be a “necessary and effective measure for legitimate law enforcement or intelligent purposes,” it stresses that “compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto” (United Nations Human Rights Council 2014 a: 6). Thereby, the report objects to the mass surveillance practices conducted by the USA and their allies, similar to the UN resolution. But the report goes further by actively contradicting arguments that are made to justify mass surveillance practices.

[... ] it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as ‘metadata’ may give an insight into an individual’s behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. [...] It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy [...]. (United Nations Human Rights Council 2014 a: 6 f.)

Moreover, the report objects to the argument often made by non-complying states that the conducted interferences of communications were in conformity with domestic law. “[... ] interference that is permissible under national law may nonetheless be ‘unlawful’ if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights” (United Nations Human Rights Council 2014 a: 7). In view of the contribution of such surveillance programs to national security purposes the report states that the “degree of interference must, however, be assessed against the necessity of the measure to
achieve that aim and the actual benefit it yields towards such a purpose” (United Nations Human Rights Council 2014a: 8). This would imply “that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State’s own constitutional regime and international human rights law” (United Nations Human Rights Council 2014a: 10).

Last but not least, the UN High Commissioner on Human Rights criticises the argument that extraterritorial surveillance were automatically lawful, which also led to intelligence cooperation and the circumvention of domestic law by countries spying on each other’s citizens.

The Human Rights Committee, in its general comment No. 31, affirmed that States parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. This extends to persons within their ‘authority.’
The Human Rights Committee has been guided by the principle, as expressed even in its earliest jurisprudence, that a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking ‘at home.’ [...] A State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other.
It follows that digital surveillance therefore may engage a State’s human rights obligations if that surveillance involves the State’s exercise of power or effective control in relation to digital communications infrastructure […]. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. (United Nations Human Rights Council 2014a: 10ff.)

In March 2014, the HRC raised objections concerning the mass surveillance practices of the USA. In a country report on the USA, the HRC invites the state to “[t]ake all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17” (UN HRC 2014b: 10). The report shows particular concern about the
weak possibilities of protection and remedy in cases of abuse of surveillance power. Although the USA did not ratify the procedure for individual complaints contained in the Optional Protocol, they ratified the IPCCER and so agreed to comply with it (United Nations Human Rights Council 2014 b; Pöschl 2015: 439 f.).

But this was not the only response by the UN to the Snowden revelations. It was recognized that the problem was also about the definition of privacy. Thus, a long-running process of discussion has been started. The members of the HRC agreed in March 2015 to establish a UN Special Rapporteur on Privacy (SRP). In August 2015, Joseph Cannataci was appointed as the UN’s first SRP. He delivered his first annual report in March 2016 (United Nations Human Rights Council 2016: 3).76

The report serves mainly as a description of the mandate and how the SRP sees his task. According to the report, “the focus of the SRP shall be on informational privacy” (United Nations Human Rights Council 2016: 10). Of particular interest is the following statement, because it contradicts the argument of balancing security and liberty:

[I]t becomes clear that it is not only privacy that impacts the flows of information in society but also other rights like freedom of expression and freedom of access to publicly-held information. All of these rights are im-

76 Before this, mass surveillance practices and the right to privacy were also addressed by a report of the Special Rapporteur on countering terrorism in 2014. It states that certain states violate international human rights law with their intelligence conduct: “State’s obligations under article 17 of the International Covenant on Civil and Political Rights include the obligation to respect the privacy and security of digital communications. This implies in principle that individuals have the right to share information and ideas with one another without interference by the State, secure in the knowledge that their communication will reach and be read by the intended recipients alone. Measures that interfere with this right must be authorized by domestic law that is accessible and precise and that conforms with the requirements of the Covenant. They must also pursue a legitimate aim and meet the test of necessity and proportionality. […] the technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. […] there is an urgent need for States using this technology to revise and update national legislation to ensure consistency with international human rights law” (UN General Assembly 2014: 22).
portant and commitment to one right should not detract from the importance and protection of another right. Taking rights in conjunction wherever possible is healthier than taking rights in opposition to each other. Thus, properly speaking, it is not helpful to talk of ‘privacy vs. security’ but rather of ‘privacy and security’ since both privacy and security are desiderata … and both can be taken to be enabling rights rather than ends in themselves. Security is an enabling right for the overarching right to life while privacy may also be viewed as an enabling right in the overall complex web of information flows in society which are fundamentally important to the value of autonomy and the ability of the individual to identify and choose between options in an informed manner as he or she develops his or her own personality throughout life. (United Nations Human Rights Council 2016: 10)

That statement reveals the actual task of this discussion process: to address the basic argument of the proponents of mass surveillance and to challenge this point of view with a better argument – following the discourse theory of Habermas. This process of discussion will go on for the next few years. At the time of writing, the outcome can hardly be anticipated.

In August 2016, the second report of the SRP was published. The paper gives a description of the work progress. According to the report, the upcoming reports should highlight the right to privacy in five different focuses of activity called Thematic Action Streams: a better understanding of privacy; security and surveillance; big data and open data; health data; personal data held by cooperation (United Nations General Assembly 2016). With this report, the fields of discussion for the next years are defined.

Right down the line, the tactics of persuasion and discourse are the only ones used by the UN to face the violation of the human right to privacy. However, the UN uses this mode, based on the logic of appropriateness, in a very comprehensive way contrary to the single actions of many liberal states. This process of discussion follows three steps: In the first, the UN upholds the norm of privacy with a resolution to show that the behavior of the USA is not compliant with this norm. Second, they countered the arguments of the proponents of mass surveillance, who hold that the intelligence procedures of the USA and their allies are lawful and, hence, in accordance with the norm of privacy. And third, the UN launched a long-term discussion process aiming to challenge the underlying norm of mass surveillance as such.
This does not mean that the UN would try to *destroy* this norm with counterarguments. Rather, the interpretation of the norm of security should no longer encounter the norm of privacy, so both can coexist.

Anyway, one has to keep in mind that besides the UN efforts since 2013 there is neither a new international law on privacy nor a new interpretation of the right to privacy (Peters 2017: 148 f.). Instead, the UN highly neglected the right to privacy, especially between 1989 and 2009 (Nyst/Falchetta 2017: 105).

### 5.2.2. European Union

According to Elmar Brok, the chairman of the Foreign Affairs Committee at the EP, the mass surveillance practices of the USA caused an “enormous loss of trust” (2013, cited in Wright & Kreisl 2015: 11 f.). But from the three adequate modes of social action in this case (coercion, incentives, persuasion), only discursive measures were used to push the USA to a state of rule-consistent behavior. The EP proved to be the “most active European institution on the issues implicated by the NSA-Affair” (Schneider 2017: 557) in comparison to the Council and the Commission.

Although the EU could have raised sanctions against the USA, this was not possible because of the involvement of a considerable number of member states in mass surveillance practices. The Snowden revelations brought to light that not only the intelligence community *Five Eyes* exists, but other forms of cooperation like the *Nine Eyes* and the *14 Eyes* as well. These alliances are more limited forms of cooperation than the *Five Eyes*, a group of which the United Kingdom is a member. The club of the *Nine Eyes* includes the members of the *Five Eyes* as well as Denmark, France, the Netherlands and, as a non-EU member state, Norway. The group of the *14 Eyes* consists of the *Nine Eyes* and Belgium, Germany, Italy, Spain and Sweden (Shane 2013). Because of these linkages to the NSA, the credibility of the EU member states to take measures to enforce the right to privacy is weak. Hence, it is unsurprising that the EP gave the strongest response to the NSA scandal and not the Council.
In July 2013, the EP adopted a Resolution on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ privacy that expressed

1. [...] serious concern over PRISM and other such programmes, since, should the information available up to now be confirmed, they may entail a serious violation of the fundamental right of EU citizens and residents to privacy and data protection. [...] 
13. Stresses that in democratic and open states based on the rule of law, citizens have a right to know about serious violations of their fundamental rights and to denounce them, including those involving their own government; stresses the need for procedures allowing whistleblowers to unveil serious violations of fundamental rights and the need to provide such people with the necessary protection, including at international level [...].

(European Parliament 2013)

Furthermore, the resolution requests that the USA provide all necessary information about surveillance practices and that they answer a letter by Commissioner Reding, sent only a few days after the first Snowden revelations to US Attorney General Holder, which demanded explanations from the US side. The Commission, moreover, should make sure that the standards of EU data protection would not be undermined in the negotiations about the Transatlantic Trade and Investment Partnership (TTIP). The resolution also calls on the Commission to review the Save Harbor agreement (European Parliament 2013).

On a final note, the EP instructed the Committee on Civil Liberties, Justice and Home Affairs (LIBE) to conduct an inquiry into today’s surveillance practices and possible legal reforms. Committee members traveled to Washington and discussed with various officials and experts the US surveillance practices and held more than a dozen hearings in Brussels. At the end of this process, the EP adopted the LIBE report together with a resolution that expressed the main results of the report and demanded actions on behalf of these findings. Both the report and the resolution were passed in March 2014 and adopted by a large majority (Wright & Kreissl 2015: 12; European Parliament 2014).

In the resolution the EP considers the existence of far-reaching surveillance programs that were set in place by some states, pointing especially to the USA’s PRISM program. They called the EU member states to revise their intelligence policy and existent oversight measures
to comply with the right to privacy. But contrary to the first resolution, the EP did not only determine that a norm was violated, it also contradicted the arguments brought forward by supporters of mass surveillance practices. It

5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society [...]  
10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens [...]. (European Parliament 2014)

By this, the EP contradicts the national security norm that justified surveillance practices. But does the EP’s resolution also attack this norm in the same way as it was done by the UN? As it can be considered in the following quotation, the EP does not question the metaphor of the balance between security and privacy. Instead, the members of parliament stick to the point and call for states to strike the right balance between these norms. Nevertheless, they contradict the norm of security in the way that the EP denies that it is the only norm that applies to the practice of surveillance practices. The resolution

6. Recalls the EU’s firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection; [...]  
12. Sees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects’ fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law; [...]  
16. Strongly rejects the notion that all issues related to mass surveillance programmes are purely a matter of national security and therefore the sole competence of Member States; reiterates that Member States must fully respect EU law and the ECHR while acting to ensure their national security [...]. (European Parliament 2014)
But the EP did not only apply discursive measures to challenge the US’ behavior, the resolution also demands “strong political undertakings from the new Commission which will be designated after the May 2014 European elections,” (EP 2014) particularly regarding the adoption of a renewed data protection regime and the changes of the US Safe Harbor agreement.

The Safe Harbor agreement came to operation in 2000. With it, the Commission certified that the US data protection regime was congruent with the EU data protection laws. On the other hand, US companies that process data of EU citizens had to self-certify annually (in cooperation with the US Department of Commerce) that they abide by these rules (Wright & Kreissl 2015: 16). In light of the US surveillance practices, the EP demanded the suspension of this agreement from the Commission, because the members of parliament viewed the agreement as insufficient to protect the EU citizens’ rights. The resolution notices that the Commission failed to act, although the same demand was made in the 2013 EPs resolution (EP 2014). Nevertheless, in the very end it was not the Commission but the European Court of Justice that brought down the Safe Harbor agreement in 2015 (Gibbs 2015).

Therefore, the Commission and US officials started negotiations about a new agreement that fits the EU law. In February 2016, the so-called EU-US privacy shield was launched. Basically, this shield consists of an annual written guarantee of the USA that their intelligence agencies have no indiscriminate access to the EU citizens data (Scott 2016). Although a working group in which every member state is represented criticized the privacy shield in April (Gibbs 2016), the privacy shield was published in the official gazette in August 2016. Only six weeks later, an Irish civil society organization took legal action against this privacy law at the European Court of Justice (Rudl 2016). Only a few days after taking office in January 2017, the 45th President of the United States, Donald Trump, issued an executive order that minimized the privacy rights of non-US citizens. At the time of writing, it is still unclear what consequences this will have for the validity of the privacy shield (Rebinger 2017).

With regard to the new Data Protection Regulation, changes were made after the Snowden revelations. One year before the NSA scandal, the USA successfully lobbied away a paragraph that demanded not to
recognize any kind of judgment or decision of a court or an administration authority that requires disclosing personal data of a EU citizen. That would mean that the EU would not accept FISC warrants. But after the Snowden revelations, the entire paragraph was replaced word for word (Wright & Kreissl 2015: 16). When the new regulation was officially adopted in April 2016, however, the aforementioned paragraph was not included (EU 2016). Nevertheless, in Article 36.2a it says that the Commission should decide about the adequacy of a third country’s data protection standard with regard to the “rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data” (EU 2016).

After the revelation of the Snowden documents, some EU policy makers attempted to put the negotiations concerning the TTIP on hold (Wright & Kreissl 2015: 24).

Besides this, there was also a broader process of discussion that was launched. In early December 2015, the European Data Protection Supervisor (EDPS) established an Ethics Advisory Group that should start a broader discussion on EU level and globally about “how to ensure the integrity of our values while embracing the benefits of new technologies” (European Data Protection Supervisor 2016) and to explore “the relationships between human rights, technology, markets and business models in the 21st century from an ethical perspective, with particular attention to the implications for the rights to privacy and data protection in the digital environment” (European Data Protection Supervisor n.d.). The discussion should involve civil society actors as well as scientists and politicians.

In comparison to the EP, the Commission’s and Council’s reactions were considerably weak. The Commission, for example, did not initiate negotiations about a new privacy regime between the USA and the EU. Instead, the Council of Justice of the European Union overturned the Safe Harbor agreement in the Schrems case (Schneider 2017: 540ff., 562). Also the European Council has been very reluctant in its response to the Snowden revelations (Schneider 2017: 562).

Summarizing the EU responses, one can observe that persuasive measures made up the largest part of it. The EU response followed to a
certain degree the UN response: After discerning the norm violations, arguments against the violating behavior were made and – in the last step – a broader discussion process was initiated to discuss the relationship between privacy and modern techniques. Even attempts to negotiate new data protection arrangements with the USA have to be considered as persuasive measures. After all, the USA have to agree to such new agreements. Nonetheless, if the US continues to deny EU citizens sufficient data protection, the EU could sanction this with a refusal of a new Safe Harbor agreement. But because of the importance of a free flow of data between both the US and EU territories, it seems unlikely that this will happen.

5.2.3. Council of Europe

As early as 2008, the Commissioner of Human Rights of the CoE (CHR) noticed in his Issue Paper on Protecting the Right to Privacy in the Fight Against Terrorism: “We are rapidly becoming a ‘Surveillance Society.’ […] Freedom is being given up without gaining security” (13). Thus, it comes as no surprise that the Snowden revelations caused an ongoing response by the CHR. In further Issue Papers, he continued to challenge the security norm by arguing that the reasoning of national security was not an acceptable tool to minimize the validity of human rights (Commissioner of Human Rights 2015: 21ff.; Commissioner of Human Rights 2014: 107ff.). Moreover, using articles published in newspapers, the CHR reminded readers of the values of the European convention of human rights and expressed that untargeted mass surveillance could undermine the trust of citizens in the state and democratic values. He calls for the limitation of surveillance practices by law and a strong oversight of intelligence services (Muižnieks 2015; Muižnieks 2013). But did the Council of Ministers and the Parliamentary Assembly echo the efforts of the CHR?

The Snowden revelations definitely raised an awareness of the challenges to the right to privacy by technical developments. The CoE set in an Ad Hoc Committee on Data Protection (CAHDATA), which has the task to review and renew the Convention 108 on Data Protection, which played a major role in the development of data protection
at the international level (Council of Europe n.d.b). At time of writing, results are still to be expected. Nevertheless, this was not the only response given by the CoE.

Only a few days after the first revelations in the *Guardian*, the Council of Ministers adopted a declaration acknowledging the threat of mass surveillance to the right to privacy, the right to free expression as well as to free media and reminding all member states that law enforcement activities have to comply with the CoE’s human rights standards (Council of Europe 2013a). A few months later, in November 2013, a second declaration was adopted by the member state’s ministers for media and information society, which calls for safeguards against electronic mass surveillance. The declaration considers the destruction of democracy as possible and condemns the unlawful monitoring of communications (Council of Europe 2013b).

The Parliamentary Assembly also adopted a resolution on mass surveillance in April 2015. It states that mass surveillance endangers human rights and calls for surveillance activities that are targeted and based on a court warrant and encourages national parliaments to carry out inquiries into the NSA affair (Council of Europe 2015a). Additionally, it is notable that the resolution states “that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials” (Council of Europe 2015a). Another resolution, which was adopted in June 2015, called for a better protection of whistleblowers and asked the USA to let Snowden return to his home country and to give up the investigation against him for reasons of public interest (Council of Europe 2015b).

In April 2016, the Council of Ministers adopted a recommendation encouraging states to evaluate their level of Internet freedom and Internet human rights standard periodically and share their findings with the CoE (Council of Europe 2016a). To tackle the issue of human rights, rule of law and democracy in an online environment in the long run, the Council also adopted a New Internet Governance strategy in 2016 to launch a broad process of discussion. This includes specific steps and activities that should be accomplished by 2019. Among other things, a platform should be established where governments and Inter-
net companies can launch a process of discussion about human rights online. In general, new standards regarding the behavior of Internet intermediaries should be established. To reach this target, the CoE wants to include governments, companies, civil society actors and academia in this discussion. As one of the key stakeholders, the UN-led Internet Governance Forum is mentioned. Particularly with regard to mass surveillance and the right to privacy, the Internet Governance strategy provides the international promotion of the CoE Convention 108 and triennial reports on the state of data protection in the member states on the basis of the renewed Convention 108 (Council of Europe 2016b).

In total, the responses of the CoE were only persuasive ones. This comes as no surprise, because the USA is not a member of the CoE. Hence, the coercive measure to sue the USA at the European Court of Human Rights was not available – contrarily to European accomplices of the USA. The persuasive measures were directed at both the USA and the member states of the CoE. This makes sense considering the fact that at least 25 European security services or their governments, respectively, have cooperated with the USA in mass surveillance practices (Commissioner of Human Rights 2015: 20). Thus, in the first place, the reaction was not directed purely against the USA. Instead, member states were reminded that privacy is a precious human right. The internal persuasive measures, however, were recognized by the USA because of their observer status at the CoE (Commissioner of Human Rights n.d.c).

All in all, the persuasive measures of the CoE have the same structure as the responses of the UN and the EU. After objecting to the practices of the US and their allies, the norm that justified these measures was challenged with counterarguments (here: democratic values and research that shows that mass surveillance is not helpful to fight terrorism) leading to a broad multi-stakeholder discussion process about the right to privacy and other human rights in the digital age. As

---

77 E.g., Big Brother Watch et al. vs. United Kingdom. Generally, the United Kingdom is – as one of the closest partners of the USA in SIGINT – under peculiar scrutiny of the CHR, as a memorandum on surveillance in the UK shows (Commissioner of Human Rights 2016).
the next part of this chapter exhibits, the response of the (I)NGOs is similar to this.

5.3. (International) Non-Governmental Organizations: Amnesty International

The Snowden revelations caused a response by many international and domestic NGOs. Mainly, they used two modes of social actions to enhance the human right to privacy: coercion and persuasion. Even before the Snowden revelations many (I)NGOs advocated the right to privacy. The most far-reaching point of these activities was the development of the Necessary and Proportionate Principles, a soft law standard that should help to apply human rights to the technical world (Nyst/Falchetta 2017: 107). Nevertheless, also for the (I)NGOs the Snowden revelations can be seen as a starting point for a new phase of enhanced activity regarding the advocacy of the right to privacy.

The (I)NGOs informed the public about the norm violation with brochures and through an Internet presence. With it, they tried to cause awareness of this norm violation and create a public climate that is hostile to the government’s norm violation. Thereby, they created pressure that could force the state to change its behavior. Protests were raised in Washington, D.C., and elsewhere in the world (Newell 2013), and even new NGOs originated through the Snowden revelations (Restore the Fourth 2015). However, aside from that, the NGOs also used the mode of legal enforcement to make the USA comply with human rights standards – at least to the extent that it was still possible. As already mentioned in chapter four, the FAA cut the possibility of suing by exempting companies that acted on behalf of the government from being prosecuted. Many charges were brought against the surveillance activities conducted by the USA (American Civil Liberties Union n.d.; Electronic Frontier Foundation n.d.c); however, one was the most well-known one: ACLU vs. Clapper. The ACLU brought the claim against the mass collection of phone records of Americans to court only six days after the first revelations by the Guardian. The complaint argued that the NSA’s surveillance program PSP violated the privacy rights of Americans protected by the Fourth Amendment. In May 2015, the
Court of Appeals for the Second Circuit declared the program illegal (American Civil Liberties Union 2015). This case is considered to be the first successful outcome against the US surveillance activities.

As a matter of course, not all activities of all international and national NGOs can be considered in this chapter. But one organization should be scrutinized further: Amnesty International. One advantage of the investigation of AI is that it is one of the biggest human rights organizations on the globe and that the advocacy actions with regard to the right to privacy can be seen in comparison to advocacy processes of other human rights. In the following, the reactions of AI to the Snowden revelations will be analyzed.

Not only since the Snowden revelations was AI aware of the possible threat that the American law provided to human rights by granting huge possibilities of legal spying. Only a few months before the NSA affair had gone viral, the Supreme Court decided in Clapper vs. Amnesty International that AI was not allowed to challenge the existing surveillance laws allowing the security branch to intercept international communications of US persons because they cannot prove that they had been spied on (Liptak 2013). Hence, it is not remarkable that the organization strengthened their efforts to fight mass surveillance.

One of the first actions taken by AI was to support bodies of the international human rights regime with information. For example, AI provided a written statement to the UN HRC to discuss US behavior (Amnesty International 2013).

Whereas privacy rights and surveillance issues have not played a role in the public campaigning of AI until 2013, this changed after the Snowden revelations. In March 2015, AI launched the campaign #Unfollowme, which was directed mainly at the surveillance practices of the USA but also of the UK and other governments – making it the main global AI campaign against mass surveillance. With it, the INGO not only argues that the mass surveillance practices of states are intruding in the private sphere massively, they also supported this argument with a global poll. 15,000 people in 13 countries were surveyed on behalf of AI about the interception, storage and analysis of Internet user data. The poll found a majority in all countries against the huge capabilities of governments to conduct mass surveillance (Amnesty International 2015a). Moreover, the campaign encompassed a petition to...
President Barack Obama, urging him to end mass surveillance practices that violate the privacy right of Americans and people around the globe; and to amend Executive Order 12333 that serves – among other things – as legitimation of the spying activities (Amnesty International n.d.a). In June 2015, the Board Members of AI USA wrote a letter to President Obama to communicate their concerns about US mass surveillance activities and to express that AI as an international human rights organization relies on secure and confidential communications with employees and victims of human rights violations. The letter also demands the amendment of Executive Order 12333, similar to the petition (Amnesty International 2015 b).

Nevertheless, the campaign was mainly initiated to raise attention to the issue of mass surveillance and, thus, to enhance public awareness of the issue. This was done by interviews with whistleblowers like Edward Snowden or by publishing information about what countries are involved in the NSA scandal and which country is sharing data with US authorities (Beaumont 2015 a; Amnesty International n.d.b). This awareness was also strengthened by a report about the importance of encryption in March 2016. It is Amnesty’s first official position on the importance of encryption to human rights.

However, this campaign is different from other AI campaigns. One month after #Unfollowme was launched, AI stated that many comments had reached the organization, saying that surveillance was necessary and that one who had nothing to hide had nothing to fear – a response unthinkable to happen with regard to human right violations like torture or freedom of expression. These reactions showed AI how strong the security norm had proliferated even within societies. AI reacted by explaining in detail why such a point of view was not congruent with human rights (Beaumont 2015 b).

AI also cooperated with other human rights organizations and advocators of privacy rights. The organization joined campaigns like Reset the net (Amnesty International et al. n.d.) and helped develop software against surveillance activities of governments (Amnesty International 2014). Furthermore, together with Privacy International it published a brochure two years after the NSA affair had broken out to summarize the revelations and the main responses to it (Amnesty International & Privacy International 2015).
However, the right to privacy is not promoted in the same way as other human rights in cases of violation. The analysis of the annual reports since 2013 draws a picture of how diverse the right to privacy is and that it does not only apply to the surveillance issue.

In all annual reports of AI, mass surveillance is not mentioned in the section that deals with human right violations of the USA. Also with regard to other countries, the right to privacy is only a minor issue. Whereas in the latest annual report (Amnesty International 2016) concerns about a limitation of the right to privacy in European countries were expressed and UN efforts to enhance this human right are welcomed in the regional overview about Europe and Central Asia, the right to privacy was mentioned with regard to the state of human rights in single countries for different reasons. Brazil was lauded due to their efforts to enhance privacy; Australia, New Zealand and the UK were criticized for the surveillance activities of their intelligence services. Also new surveillance laws as well as the state of Internet privacy in countries like China, India, Korea, the Netherlands and others, were condemned. This does not always happen in relation to the mass surveillance practices but also with regard to the freedom of expression. Looking to other countries, like Iran, Morocco and South Africa, the right to privacy was mentioned in relation to the free choice of sexual practices and habits (Amnesty International 2016a; Amnesty International 2015c).

It is noteworthy that privacy is mentioned in several different capacities: in combination with sexual habits, freedom of expression and security issues. A human right that is as diverse as the right to privacy is more difficult to advocate. This does not mean that AI did not advocate the right to privacy, for example this statement by Salil Shetty (cited in Amnesty International 2016b), the AI’s Secretary General, shows that privacy was mentioned when the latest annual report was launched:

The misguided reaction of many governments to national security threats has been the crushing of civil society, the right to privacy and the right to free speech; and outright attempts to make human rights dirty words, packaging them in opposition to national security, law and order and ‘national values.’
Nevertheless, the problem of correctly addressing the surveillance topic is existent. Although the US section of AI approaches the issue under the broad topic of Security and Human Rights, the right to privacy is addressed in two subchapters: Freedom of expression and mass surveillance. Whereas the racial profiling of mass surveillance activities and especially the violation of privacy of Muslim citizens is addressed in the freedom of expression category, the mass surveillance chapter deals with the intrusion into the privacy of citizens and non-citizens in general (Amnesty International n.d.c).

In addition, the intensity of advocacy of the right to privacy is also lower than the advocacy efforts of other human rights. One example of this is the Amnesty Journal, a periodical that is published every two months by the German section of AI, which covers topics of human rights violations and successes in the fight for human rights. From the time of the Snowden revelations until the end of May 2016, only a handful of articles were published that match the search terms Überwachung (surveillance), NSA or Snowden. In comparison to other human rights violations, the surveillance topic is underrepresented. Torture, one of the classical violations of human rights norms, is much more present in the journal: The term Folter (torture) leads to almost 100 articles in the same period (Amnesty International n.d.d). There are also no brochures about privacy or surveillance issues available on the German web page of AI (Amnesty International n.d.e).

In summary it can be said that the advocacy process of the right to privacy is different from the advocacy processes of other human rights. First of all, the topic of mass surveillance is quite new to AI. It took almost two years to launch the first global AI campaign on mass surveillance. Nevertheless, there are also other reasons that may explain the underrepresentation of the surveillance topic in the actions by AI. With a view to the annual reports and the Internet presence of AI regarding the presentation of the right to privacy and the violation of it through mass surveillance, it becomes obvious that privacy is a term that does not only touch many areas of life but also many human rights. Although the term privacy is mainly connected with the fight against mass surveillance, privacy is also at stake when it comes to freedom of expression and sexual self-determination. Last but not least, one main problem is the low visibility of privacy violations, as already
mentioned in chapter three. This became apparent when many people voiced opposition to the campaign of AI against mass surveillance. Furthermore, the violation of privacy rights is hardly customizable – a tool very often used by AI to call attention to human rights violations.

In total, two modes of social action were used to prevail upon the USA to comply with the privacy norm: legal force and coercion. Nevertheless, the example of AI showed that it is not a simple task to campaign for the right to privacy. As aforementioned, several aspects can weaken the persuasive response of human rights organizations. Modes of coercion were also restricted, but civil liberties organizations used what was left of legal remedies to react to the human rights violation.

By having analyzed the actions of privacy advocates, it became apparent that the international advocacy network was activated by the Snowden revelations. But is there a discursive opportunity to change the behavior of the USA? Polls show that in the months after the Snowden revelations the attitude to privacy rights changed in the USA. Whereas a few days after the first revelations people considered the NSA surveillance measures as acceptable, a few months later people said that the measures intrude their privacy rights and, thus, opposed the NSA activities, although people would still opt for security instead of privacy in case of doubt (Wright & Kreissl 2015: 20 f.). A symbol of a shifting value for privacy can be observed in increasing encryption activities worldwide (Wright & Kreissl 2015: 34 f.). This is an indication that a discursive opportunity in favor of the privacy advocacy network exists – contrary to previous cases of enclosures of surveillance activities of the US. Nevertheless, because of the weakness of the advocacy process, it can be doubted if the USA will reach the rule-consistent behavior stage in the near future, as the next chapter shows by scrutinizing the US reaction.