# Echoes of History: Understanding German Data Protection

Alvar C.H. Freude and Trixy Freude

## The Basics

The discussion surrounding surveillance and the collection of personal data—whether by the private or public sector—and the debate over the authority of the intelligence services have never been more relevant in Germany. The debate has become more complex and contentious as a result of the disclosures about U.S. surveillance by whistleblower Edward Snowden and the growing threat of terrorist attacks worldwide. Some politicians are using this heightened awareness to call for and sometimes push through tougher security laws, while others have rallied against what they perceive to be too much government surveillance. In the midst of this jockeying, pragmatic solutions offered by moderate players have often gone unnoticed. Although there are a variety of opinions on the subject, non-Germans are usually surprised by the strength of the opposition to surveillance measures in the country.

Germans place a great deal of importance on privacy and data protection. Fear of the private sector and, even more so, government abuse of personal data is widespread. That said, German laws grant citizens a great deal of protection. Storage of personal data, for example, is prohibited, with some exceptions—unless the affected individual has consented to the storage.

Data protection is not explicitly enshrined in Germany's constitution, also known as the Basic Law, but it does enjoy protection by virtue of what is known as the "census ruling" by Germany's highest court. In this 1983 landmark case, the court decided that citizens have a basic right to self-determination over their personal data. The decision was in response to a census that became the subject of numerous constitutional complaints of violations of respondents' civil rights. Following the decision, the federal government was compelled to separate personal data from the census questionnaires and ensure greater anonymity for survey-takers. Due to opposition, the census was delayed until 1987, and scaled back considerably.[1] In the ensuing years, suspicion of surveillance has remained strong.

## Privacy in Context

The private sphere is particularly protected and is a human right that should be restricted only under specific circumstances. Although the idea of privacy dates back to antiquity, our current understanding of the term is a product of the modern age. Historically, privacy has frequently been infringed upon depending on the type of government, such as fascism, or circumstances like war or terrorism.

World War II, the darkest chapter in Germany's history, left a deep mark on its citizens. As a result, Germans feel strongly about data protection—specifically, protection of the citizen against abuse of his or her data—and protection of privacy. The Federal Constitutional Court (FCC), Germany's equivalent of the Supreme Court, has derived a right to data protection from a section of the constitution pertaining to personal freedoms, which will be discussed later in this article. In turn, specific laws such as the Federal Data Protection Act, as well as the Criminal Code, the Civil Code, the Telecommunications Act and the Telemedia Act, govern how various kinds of data may be handled.

This approach is materially different from how data protection is handled elsewhere. In the United States, for example, some specific regulations exist regarding issues such as the privacy of children on the internet. However, there is no comprehensive body of U.S. laws like the German Federal Data Protection Act. Nevertheless, privacy is a right worthy of protection around the world, even if it is not explicitly stipulated in a nation's constitution.

Legal efforts relating to privacy are aimed at creating a space where every individual can behave freely. This is spelled out in Articles 10 and 13 of the Basic Law, which deal with privacy of correspondence, posts and telecommunications as well as the inviolability of the home. There are, however, exceptions for law enforcement authorities and intelligence services. For example, audio surveillance of private premises—known in casual parlance as *Großer Lauschangriff*, or large-scale eavesdropping—is permitted in certain cases and only as an extreme measure of law enforcement. The introduction of this instrument was so controversial that one of its major opponents, Minister of Justice Sabine Leutheusser-Schnarrenberger, resigned when her party voted to support it.[2] The former minister brought a constitutional complaint against the legislation, which was partially successful.[3]

Data protection legislation in the European Union and particularly in Germany is extensive. The protection covers all data pertaining to the personal or material circumstances of the individual. The buying and selling of data as practiced in some countries—where extensive information about individuals, such as their shopping habits, can be purchased from data merchants—is inconceivable in Germany. Although data merchants do exist there, they are subject to strict regulation.

## Surveillance, Control and Intelligence Services in Nazi Germany and the GDR

There are historical explanations for the distrust and revulsion Germans feel toward state surveillance, which help explain the widespread belief that privacy merits special protection. During its reign from 1933 to 1945, the Nazi regime used numerous instruments to monitor the public, control behavior and use citizens to monitor their neighbors, colleagues and friends. National Socialism dictated public and private life; all spheres of society and the state had to submit to the *Gleichschaltung*—the policy of achieving rigid and total coordination and uniformity. Total uniformity meant the elimination of democratic structures in favor of the *Führerprinzip*, or the leader principle, which allowed the leader's authority to go unchecked and exist above the law.[4]

The Third Reich also systematically abused private data: It maintained a so-called index of Jews that listed the identity of all Jews dating back to their grandparents' generation. In addition, it relied on data collected during the Weimar Republic (1918–1933), including records of homosexuals. Nazi Germany's persecution of Jews and homosexuals proved that no matter the intent of the data-collecting entity, the collection of so much personal information about individuals could be dangerous in and of itself.

The state used the Gestapo, its secret police, and numerous party organizations to exercise control, but it could not penetrate every facet of its peoples' private lives. The Gestapo relied on the more or less willing collaboration of the people. And it got it in the form of denouncers, who sought rewards for spying on and incriminating anyone who opposed the state ideology. However, fear of or loyalty to the system was not the only reason people informed against each other. Often it was "the attempt by the weaker ones to assert themselves against the stronger ones."[5] Citizens took advantage of the government's system to hurt their personal enemies.

The German Democratic Republic (GDR), also known as East Germany, was founded in 1949 after the postwar partition of Germany. Though it had a constitution in which personal freedom and the inviolability of the home were enshrined, it functioned as a socialist dictatorship.[6] Individual rights were regularly violated by the Ministry for State Security, also known as the Stasi.

The Stasi searched private premises, installed hidden tapping devices, questioned neighbors and combed the personal mail of "suspicious persons," usually opponents of the regime. Surveillance, control and intimidation were commonplace. Logs known as "house books" showed just how deeply the state intruded into the privacy of its citizens. Beginning in the mid-1960s, every house was required to keep a record with details about each resident, including place of birth and profession. Likewise, information about any visitors had to be entered in these books. The Stasi also created files on hundreds of thousands of citizens. In particular, outside influences were considered dangerous and suspicious. Mail from West Germany was typically screened, as were letters sent from the residents of the GDR to West German relatives. Against this historical backdrop, state surveillance of the citizenry evokes a deep-seated uneasiness among Germans even today. Many feel that measures that are barely acceptable in a democracy could easily be abused in the event of a change in government, as has happened in the past.

When Germans bring up the U.S. National Security Agency (NSA) and its controversial surveillance and data collection practices, they often compare it to the Stasi. How many files did the Stasi hoard, how many filing cabinets were needed? How many cabinets would be needed to store the volume of data that the NSA collects? The comparison trivializes the extensive personal files collected on citizens of the GDR, but it shows how fiercely Germans feel about the intelligence services collecting their data.

## The Current Landscape

There is broad consensus among German politicians that data protection is important in and of itself. Still, there are stark differences between the parties' approaches to the issue. These differences are particularly evident on issues like the rights companies should have in data processing, as well as how law enforcement and intelligence services should be regulated. Members of the conservative sister parties, the Christian Democratic Union (CDU) and the Christian Social Union (CSU), including Chancellor Angela Merkel, are more inclined to call for lower standards of data protection and highlight the opportunities that big data applications have to offer. Their center-left coalition partner, the Social Democratic Party (SPD) places a greater emphasis on data protection. Opposition parties, particularly the Greens and the Left, support data protection even more staunchly. Many in those parties believe that data protection is in jeopardy. In recent years the Free Democratic Party (FDP) has not held any seats in the Bundestag, but it remains vocal on civil rights issues.

Merkel often holds back for a long time before taking a public position on complex and controversial political issues like data protection. She allows the debate to evolve and then assumes the lead late in the discussion. This could be observed in her response to the Snowden revelations: For a long time, she said nothing. Only after it was disclosed that the NSA had monitored her cellphone did she comment publicly: "Spying on friends—that's totally unacceptable."[7] At the ninth National IT Summit in 2015, a meeting of the federal government and business community, Merkel spoke about data protection and demanded that big data applications not be impeded by data protection.[8] However, she still refrains from taking clear public positions on many data issues and lets her ministers and party cohorts do the talking.

At the same time, positions also diverge among the individual ministries. For example, the Federal Ministry of Justice and Consumer Protection established a working group for the National IT Summit, which aims to strengthen data protection. Within this forum, several focus groups have taken on different challenges. The Consumer Sovereignty and Transparency Focus Group is developing simple and clear privacy statements, while the Privacy by Design/Data Protection through Technology Focus Group is working on recommendations for privacy-friendly product design. Members of the group include representatives of private industry, civil society, the scientific community and the ministry.

The differences among political players are particularly evident in the discussion surrounding the Snowden disclosures. While many conservatives view Snowden as a traitor and would like to have the same options for data storage in Germany as exist in the United States, the Left and Greens criticize the activities of intelligence services—in Germany and abroad—and want the most stringent regulations possible. The Social Democrats are torn between their commitment to the governing coalition and their own domestic policymakers on the one hand and support for basic rights on the other.

Ultimately, the only option for privacy and civil rights advocates is to resort to the Federal Constitutional Court and the European Court of Justice. For example, in a 2008 judgment on a law regarding online searches and government Trojan Horse software, which allows law enforcement to monitor online communications of suspected criminals, the FCC introduced a "fundamental right to the guarantee of confidentiality and integrity of information technology systems,"[9] and in 2010 the court overturned the law on data retention. Four years later, the European Court of Justice declared the underlying EU data retention directive invalid on the ground that it violates fundamental rights.[10]

## German Data Protection Laws and the Federal Data Protection Act

By the late 1960s, increased automation in electronic data processing spurred calls to regulate the processing of personal data. In 1970, the world's first data protection act was adopted in the German state of Hessen; in 1974, the state of Rhineland-Palatinate followed; and in 1977, the Federal Data Protection Act was passed. The legislation was meant to protect personal data "against abuse in their storage, transmission, modification and deletion (data processing)."[11]

As mentioned earlier, debate about the census in the 1980s was particularly contentious. With its 1983 census ruling, the FCC introduced a basic right to "self-determination over personal data," according to which every individual has control over the processing of his or her data. However, as with all fundamental rights, this must be weighed against other rights, such as the freedom of expression.

The central message of the judgment can be summed up as follows (emphasis added):

> A societal order and a legal order enabling it in which citizens are no longer able to know who knows what about them, when and in what context would be irreconcilable with the right to self-determination over one's own personal data. **Anyone who is unsure whether deviant behavior is being recorded at any time and permanently stored, used or passed on as information will try to remain inconspicuous in such conduct. […] This would harm not only the individual's opportunities for self-development but also the common good because self-determination is a basic condition of a free democratic community that is based on the ability of its citizens to act and collaborate.** Consequently, the free development of personality under the modern conditions of data processing presupposes protection of

> the individual against the unlimited collection, storage, use and passing on of his personal data. This protection is thus encompassed by the basic right of Article 2 (1) [free development of personality] in conjunction with Article 1 (1) of the Basic Law [human dignity]. In this respect, the basic right guarantees the **power of the individual, in principle, himself to decide on the disclosure and use of his personal data.**[12]

To this day, the judgment remains groundbreaking and continues to influence legislation. The same also applies to the Federal Data Protection Act, which implements the EU Data Protection Directive in its latest form. The law has been frequently revised over the course of time and is based on six basic principles:

- **Ban subject to permission:** The collection, storage and use of personal data is in principle prohibited unless permitted by a legal provision or the affected individual's consent.
- **Direct collection:** Data may be collected only from the affected individual himself. The law does provide for exceptions, for example, if such collection would be too complicated or if another law permits the collection.
- **Data economy:** Data is not to be kept too long and must be deleted after an appropriate period.
- **Data minimization:** As little data as possible is to be collected and processed.
- **Purpose limitation:** Data processing is permitted only for a specific, previously defined purpose unless the affected individual consents to another arrangement.
- **Transparency:** The affected individual must know that data is being collected, what type of data it is, why it is being recorded and how long it will be stored.
- **Necessity:** The collection of the data must be necessary; it is only permitted if no other means are available.

## The European Data Protection Directive

The European Union has several legislative means. There are directives, which set the framework and must be translated into national law by the legislators. There are also regulations, which are applicable to all member states.

The European Union's Data Protection Directive of 1995 describes the minimum standards for data protection and the processing of personal information, but it is implemented differently in each EU state. Ireland, for example, though subject to the directive, has weaker data protection laws and exerts less government oversight than many other EU states. This makes it attractive for international companies to base their offices there. That will change, however, with the new General Data Protection Regulation, which will take effect in all European Union member states, including Ireland, in May 2018.

## The New European General Data Protection Regulation

The General Data Protection Regulation will ensure a uniform framework throughout the EU. Still, in special sectors, such as data protection in the employment sector, so-called "escape clauses" remain, permitting member states to write their own rules. Despite some gaps, the regulation will ensure that the same standards apply throughout the European Union. Citizens will be affected by the changes to varying degrees depending on the current data protection landscape in their country. In Germany, relatively little will change, as the level of data protection is already high. Many provisions already existed under the Federal Data Protection Act. There will also be some new provisions, such as the marketplace principle. It states that all companies operating in the EU, even those that have their headquarters in a country outside the EU, must comply with local standards when processing personal data of European citizens.

Privacy advocates and civil society organizations see the Privacy Shield as only a minor improvement over Safe Harbor

Another new provision is the right to data portability. It requires social network providers, such as Facebook, to give their users the option to transfer their data—including, for example, posts, photos or lists of friends—to another provider. Another new feature is the right to be forgotten. Under this provision, users can demand, subject to certain conditions, that their personal data be deleted from internet services such as search engines. Moreover, in the future, companies will face stiffer penalties if they violate data protection requirements, which could add up to 4 percent of their worldwide turnover.

The negotiations on the implementation of the General Data Protection Regulation lasted several years. It took broad political discussions before the European Commission, the European Council and the European Parliament were able to reach the current compromise. For example, the question of how to deal with big data applications was a hard-fought issue.

## Safe Harbor and the Privacy Shield

In order to bridge differences between European and American data protection laws and to facilitate trans-Atlantic business, the European Commission recognized the Safe Harbor principles in 2000. These principles allowed for the transfer of data of EU citizens to the United States when certain rules were observed. However, the European Court of Justice invalidated this decision in 2015, arguing that once data was transmitted, it could no longer be controlled and American authorities effectively had unfettered access.[13]

In its critique of the Safe Harbor principles, the court said, "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."[14] With that ruling, the most important legal basis for transmitting personal data to the United States ceased to exist.

Soon thereafter, negotiations began to establish a new agreement. Starting in July 2016, the Privacy Shield replaced the invalidated Safe Harbor principles. The Privacy Shield has come under heavy criticism because, like Safe Harbor, it is not a law, but merely a European Commission "adequacy decision" that proposes revisions. Privacy advocates and civil society organizations see the Privacy Shield as only a minor improvement over Safe Harbor.[15] One improvement is the requirement that U.S. companies store EU citizens' data only for as long as it takes to meet the purpose for which the data is collected. But American authorities will continue to have access to the data under U.S. law, leading many critics to surmise that complaints will be filed and the European Court of Justice will rule against the Privacy Shield.

## Intelligence Services in Germany: Powers and Oversight

Given the historical context described earlier, Germans have a complicated relationship with intelligence services in general and their national services in particular. Here, a distinction must be made between domestic and foreign intelligence services.

The Federal Office for the Protection of the Constitution and the 16 state offices for the Protection of the Constitution are domestic intelligence services. Their task is to collect and analyze information about anti-constitutional and extremist activities, as well as to combat foreign espionage. The Office for the Protection of the Constitution has grabbed headlines in recent years due to various scandals, particularly in connection with a series of murders and other attacks committed between 1999 and 2011 by the far-right terror organization National Socialist Underground (NSU). Important documents were shredded, files were lost and dossiers were not processed appropriately. The domestic intelligence agencies were unable to solve the NSU attacks or the murders, let alone investigate them as extremist crimes. Authorities were unaware of the very existence of the group. Instead, the Office for the Protection of the Constitution sometimes suspected that the victims themselves belonged to criminal organizations. Numerous inquiry committees were established in both the German Bundestag and the state parliaments as a result of the failures of the Office for the Protection of the Constitution and the police.

Critics such as legal scholar Wolfgang Gast have argued that the domestic intelligence agencies monitor the leftist scene especially rigorously, but look the other way when it comes to right-wing extremism. Gast observed, "Domestic intelligence agents have always been engaged far more intensively and actively in monitoring presumed or actual machinations of the leftist scene than terror from the right."[16]

> "What sense does oversight make, when the overseers rely solely on mere statements by those who are supposed to be overseen?"

The Federal Intelligence Service (Bundesnachrichtendienst, BND) is the German foreign intelligence service. It collects information outside Germany about terrorism, organized crime, illicit financial flows, drug and weapons trafficking and "sensitive" regions such as Afghanistan and Pakistan. The BND partially coordinates with the NSA and has come under public criticism for passing data to the agency. In 2014, the German Bundestag established an inquiry committee to examine, among other things, this cooperation and determine the extent to which and the reasons why foreign intelligence services are spying in Germany. However, the investigation has proven difficult because witnesses from intelligence circles are reluctant to provide information and the federal government does not grant many people permission to testify.[17]

The Federal Armed Forces Counterintelligence Office is the smallest, but also the most secretive, of the German intelligence services. As the counterintelligence service of the Bundeswehr, the German armed forces, it performs roughly the same tasks as the Office for the Protection of the

Constitution for members of the armed forces. Its responsibilities include counterespionage and security clearance checks of soldiers.

The Bundestag oversees and monitors the intelligence services through the Parliamentary Control Panel, made up of members of parliament who are bound by an oath of confidentiality. The federal government is obligated to thoroughly inform this top-secret panel about the activities of the intelligence services. However, since membership in the body is only one of the MPs' many tasks, few have the time to study the issues in-depth and scrutinize all the information. Journalist Daniel Leisegang noted, "The Parliamentary Control Panel appears to be a toothless tiger, for ultimately the overseers have to rely primarily on the information of government officials and the services, the veracity of which they can only confirm to a limited degree. For this reason, in the past they usually did not learn of legal breaches or failures on the part of the intelligence services until it was reported in the media."[18]

Wolfgang Nešković, a former judge of the Federal Court of Justice, was a member of the Parliamentary Control Panel until 2013. He has criticized the oversight practice of the panel, saying: "What sense does oversight make, when the overseers rely solely on mere statements by those who are supposed to be overseen? That's comparable to a fare ticket check, where the conductor does not have travelers present their tickets but rather contents himself with their assurances that they have one."[19]

It is not (open) courts, but the G10 Commission of the Bundestag or—in the case of the state intelligence services—the G10 Commission of the relevant state parliament that decides whether surveillance activities of the intelligence services are permissible. The G10 Commission meets secretly and is made up of members who are independent and selected by the parliaments.

## Government versus Private Surveillance

The discrepancy between citizens' desires and citizens' actions in relation to data protection has frequently given cause for discussion. Advocates of government surveillance argue that while Germans heavily criticize monitoring by the intelligence services, they also willingly disclose their data on Facebook and other sites. However, this criticism is not a strong one. First of all, online users are not a homogenous group. Many consciously boycott social networks. Second, there is an important distinction to be made: On most networks, the user decides what personal information to disclose. In the case of government surveillance, the user has no influence; people cannot opt out, or can do so only with difficulty. They cannot contest and often do not even know what data is being collected and stored and why.

Still, some German politicians generally hold the view that citizens should criticize Facebook more and government surveillance less. Civil rights advocates criticize both, and they are fighting back through creative means. In Germany and 18 other countries, the Big Brother Award (BBA) is conferred annually to companies, projects or politicians identified as "data leeches." Interior ministers have won in the past, many earning the Lifetime Award, the prize for lifetime achievement.

For some, it may sound strange that technology-savvy people, such as members of the Europe's largest hacker association, the Chaos Computer Club (CCC) condemn government and private sector data collection. Frank Rieger, a CCC spokesman, puts it this way: "Frequently, the people who earn the most money act as though it were almost a law of nature, that the loss of privacy is an inevitable consequence of the use of computers and networks. They don't, however, like to publicly discuss the profit motive behind that view."[20]

## A Final Word

Germany has a very different understanding of data protection than many other countries, such as the United States. People fear that their data, whether stored with private companies or the government, can be easily abused, now or in the future. The increasing popularity of right-wing populist and extremist parties shows that, even in firmly established democracies, there is a risk that leadership will change. Citizens fear not only that their data could be directly abused, but also that, in the event of a change in government, the intelligence services could abuse their role.

Meanwhile, EU politicians continue to debate individual regulations about the powers of the security agencies and intelligence services. However, groundbreaking progress has not come from the political sphere. Rather, courts have decided these important issues, including the census ruling, data retention judgment, Trojan Horse software and within Europe, the European Court judgment on Safe Harbor. This explains why any attempts to weaken German and European data protection laws through political influence are destined to fail. The FCC and the European Court of Justice have already made clear that they derive the right to data protection and self-determination over personal data directly from the inalienable fundamental rights of the individual.

### ABOUT THE AUTHORS

Alvar Freude is an internet activist and works as a freelance software developer and database expert. Between 2010 and 2013 he was an expert witness for the Bundestag Commission on Internet and Digital Society.

Trixy Freude is a freelance journalist with a specialization in social media. Additionally, she is the proprietor of an information design business and consults on web usability.

**ABOUT NEWPOLITIK**

Newpolitik provides in-depth analysis of German foreign and domestic policy issues for policymakers beyond Berlin.

## Citations


1 See also Sylvio Dahl, “Die Predigt wurde nicht verstanden,” *Die Zeit,* issue no. 49, Nov. 27, 1987.

2 Martin Ferber, “Leutheusser-Schnarrenberger: Im ständigen Clinch mit der Union,” *Augsburger Allgemeine,* Aug. 3, 2013, *http://www.augsburger-allgemeine.de/politik/Leutheusser-Schnarrenberger-Im-staendigen-Clinch-mit-der-Union-id26487811.html*.

3 Federal Constitutional Court Decision 109, 279 - 391, Judgement of the First Senate of March 3, 2004*,* ref. no. 1 BvR 2378/98.

4 Michael Grüttner, *Brandstifter und Biedermänner,* (Stuttgart: Klett-Cotta, 2015).

5 Karl-Heinz Reuband, “Denunziation im Dritten Reich. Die Bedeutung von Systemunterstützung und Gelegenheitsstrukturen,” *Historical Social Research,* vol. 26, no. 2/3, 219-234, 2001.

6 Werner Rossade, *Gesellschaft und Kultur in der Endzeit des Realsozialismus* (Berlin: Drucker & Humblot, 1997).

7 Christian Tretbar, Ruth Ciesinger, Lutz Haverkamp, “Merkel: Ausspähen unter Freunden geht gar nicht,” *Der Tagesspiegel,* Oct. 24, 2013, *http://www.tagesspiegel.de/politik/nachrichtenticker-zum-nsa-skandal-merkel-ausspaehen-unter-freunden-geht-gar-nicht/8978818.html.*

8 Stefan Krempl, “Merkel auf dem IT-Gipfel: Datenschutz darf Big Data nicht verhindern,” *heise online,* retrieved on July 11, 2016, *http://www.heise.de/newsticker/meldung/Merkel-auf-dem-IT-Gipfel-Datenschutz-darf-Big-Data-nicht-verhindern-2980126.html.*

9 Federal Constitutional Court Judgment - 1 BvR 370/07, 1 BvR 595/07, Federal Constitutional Court Decision 120, 274, Feb. 27, 2008.

10 European Court of Justice, Judgment in Case C-362/14, Oct. 6, 2015.

11 Section 1 (1) of the Federal Data Protection Act, 1977).

12 Section 1 (1) of the Federal Data Protection Act, 1977).

13 European Court of Justice, Judgment in Case C-362/14, Oct. 6, 2015, Maximillian Schrems v Data Protection.

14 Court of Justice of the European Union, The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid, *PRESS RELEASE No 117/15.*

15 Ingo Dachwitz, “Privacy Shield: Neue Grundlage für transatlantischen Datenverkehr gilt jetzt – noch,” *Netzpolitik.org,* July 12, 2016, *https://netzpolitik.org//2016/privacy-shield-neue-grundlage-fuer-transatlantischen-datenverkehr-gilt-jetzt-noch/*.

16 Wolfgang Gast, “Rechts blind, links blöd,” *Cicero,* March 9, 2012, *http://archiv.cicero.de/berliner-republik/rechts-blind-links-bloed/48562/.*

17 See also Kai Bierman, “Der Geheimhalter,” *ZEIT ONLINE*, Nov. 2, 2015, *http://www.zeit.de/politik/deutschland/2016-07/nsa-bnd-spionage-gutachten-datenschutz.*

18 Daniel Leisegang, “Geheimdienste außer Kontrolle: Wer überwacht eigentlich die Überwacher?” *Bundeszentrale für politische Bildung,* 2013, *https://www.bpb.de/dialog/netzdebatte/169068/geheimdienste-ausser-kontrolle-wer-ueberwacht-eigentlich-die-ueberwacher.*

19 Wolfgang Nešković, “PR statt Aufklärung,” *Frankfurter Allgemeine Zeitung,* Aug. 10, 2013, *http://www.faz.net/aktuell/politik/geheimdienstkontrolle-pr-statt-aufklaerung-12496027.html.*

20 Frank Rieger, “Von Daten und Macht,” *Aus Politik und Zeitgeschichte,* vol. 63, 15–16/2013, April 8, 2013, Transparenz und Privatsphäre, p. 4.