Chapter 4
Transatlantic Privacies—Lessons from the NSA-Affair

Russell A. Miller

Introduction

One of the most significant—and overlooked—lessons of the NSA-Affair, which Edward Snowden triggered with his massive disclosures about American intelligence operations, is that a vast chasm exists between American and German perspectives on privacy. This has been a favorite theme of well-known comparative law scholars such as Yang (1966), Walsh (1976), Barnett (1999), Bignami (2007), Lachmayer (2014), and Krotoszynski (2014). In fact, the different American and German reactions to Edward Snowden's leaks demonstrate that there is hardly another issue about which transatlantic attitudes diverge so sharply. Americans do not understand Germans' outrage over the collection of seemingly meaningless and mostly innocent information that, when deployed creatively, has pragmatic value for promoting security and commercial innovation. At the same time, Germans do not understand Americans' seeming indifference toward the profound personal privacy implicated by access to highly-revealing telecommunications and Internet data. The so-called "NSA-Affair"—as it is referred to in Germany—once again proves that there are "significant privacy conflicts between the United States and the countries of Western Europe—conflicts that reflect unmistakable differences in sensibilities about what ought to be kept private" (Whitman 2004).

Transatlantic disagreement over the social, political, and legal meaning of privacy calls into question the widespread conviction that privacy is a shared and fundamental Western value, not to mention the view that privacy is a universal norm. That is a confounding conclusion for any discussion about managing our digital and data-centric future.

This chapter is an extensively edited and revised version of the author's contributions to the book *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Miller ed., 2017).

R. A. Miller (✉)
Washington and Lee University School of Law, Lexington, USA
e-mail: MillerRA@wlu.edu

D. Feldner (ed.), *Redesigning Organizations*,
https://doi.org/10.1007/978-3-030-27957-8_4

The critical insight I intend to advance with my contribution to this expansive collection grappling with the issues of data privacy and digital security is this: Privacy, especially when expressed as a norm within a domestic legal framework, necessarily reflects a society's culture (Altman 1977; Richter and Albrecht 2013). Our different legal notions of privacy are rooted in different histories, different social forces, different political traditions and institutions, different legal cultures, and different economic conditions and orientations. On these terms, there is no privacy. There are only privacies (Nissenbaum 2009).

First, I will document the dramatically different reactions to the NSA-Affair in the United States and Germany. This substantiates my fundamental claim that America and Germany have different views about privacy. Second, I will describe some of the social and political factors that unavoidably influence the two countries' very different legal understandings of privacy.

Different Reactions to the NSA-Affair

I have used the phrase "NSA-Affair" to refer to the political and legal turmoil—both domestic and international—loosed by Edward Snowden's disclosures. And that is precisely how Germans view the NSA operations exposed by Snowden: the NSA's activities were scandalous, unethical and illegal. But the developments swirling around Snowden's revelations are not seen in singularly appalling terms by most Americans. It is telling, for example, that Snowden's revelations have not widely earned the label "NSA-gate" or "Snowden-gate" in the popular American coverage of the story. That would have been in keeping with the tiresome American practice of borrowing the suffix "-gate" from the Nixon-era "Watergate scandal" to create a catchy label for every contemporary controversy worthy of Americans' attention. But Americans apparently view Snowden's revelations as less problematic than under-inflated footballs ("Deflategate") and "wardrobe malfunctions" during the Super Bowl halftime show ("Nipplegate").

Besides the very different ways in which Americans and Germans speak about the NSA-Affair, other anecdotes point to the radically different responses to Snowden's revelations in the two countries. Germans have sought to recognize Snowden as an advocate for freedom, bestowing honorary degrees or other awards of distinction on him, or by naming plazas and streets after the former NSA contractor. The Academic Senate of the Free University of Berlin granted Snowden an "honorary membership" in appreciation for his "exceptional commitment to transparency, justice and freedom" (ASTA FU 2014). Just blocks from Dresden's marvelously restored baroque Frauenkirche, a private landowner has named a plaza in Dresden's Neustadt district "Edward Snowden Platz" (Noack 2015). There have been few such gestures of veneration in the United States, where Snowden still faces a federal criminal indictment that could result in a lengthy prison sentence—if the American authorities can get

their hands on him. Perhaps worse than the government's strong condemnation, it seems that the American public quickly lost interest in Snowden. One commentator wondered if Snowden's revelations have grown stale or have "proven to be inaccessible or not titillating enough for the American public" (Chandler 2015).

There can be little doubt about Americans' and Germans' dramatically different responses to Snowden and the NSA intelligence-gathering operations he disclosed. Germans are inclined to see Snowden as a hero who cast light on highly intrusive and unnecessary surveillance programs. Americans are inclined to see Snowden as a well-intentioned criminal who jeopardized valuable anti-terrorism programs. A large majority of Germans (61%) approved of Snowden's actions, even if they were illegal. Sixty percent see him as a "hero" and not as a "criminal" (Spiegel 2013). PEW Research (2013), on the other hand, registered an increase in the percentage of Americans who believe the government should pursue a criminal case against Snowden (Motel 2014). On the basis of a survey conducted in the days immediately following the media's initial extensive coverage of Snowden's disclosures, PEW reported that a narrow majority of Americans (56%) found the NSA's intelligence-gathering operations to be acceptable (Cohen 2013). In June 2013—at the height of the sensational coverage of Snowden's leaks—a majority of Americans (53%) believed that the NSA's programs helped prevent terrorist attacks (PEW 2013).

American and German differences with respect to personal information privacy and intelligence-gathering—and the resulting different reactions to Snowden's revelations—are not just reflected in labels and anecdotes. Social science research and survey data confirm the differences.

Research that draws on the characteristics of national culture described by G. Hofstede (1980, 1991) assigns the United States and Germany to different (albeit adjacent) clusters of national culture, identified respectively as the "Anglo" and the "Germanic Europe" cultural groups (CCL 2014). Building from these claims, many authors in the area of Information Science argue that they have "identified a relationship between national culture and attitude to information privacy" (Cockcroft 2007). Concerns about personal information privacy are stronger, the research suggests, in societies characterized by higher levels of power equality, higher levels of communitarianism, and higher levels of uncertainty avoidance (Bellman et al. 2004). In one study, Germans were found to be twice as likely as Americans to be concerned about personal information privacy (IBM 1999). Social and Information scientists seem willing to attribute this result to a German national culture that is—at least relative to America—more egalitarian, more communitarian and more averse to uncertainty.

The 2014 "Privacy Index" produced by the German Internet and technology consultancy EMC (see also Rosenbush 2014), and a parallel survey produced by the Boston Consulting Group (Rose et al. 2014), substantiate the claim that Americans and Germans have different expectations with respect to personal information privacy. The former report found, for example, that Germans are much less willing than Americans—by almost 20 percentage points—to trade some privacy for greater convenience (EMC 2014). Underscoring their general aversion to trading privacy for convenience—even in the commercial or consumer context—EMC's "Privacy Index" reported that Germans were more likely than Americans to believe that the

law should prohibit businesses from buying and selling data without an individual's consent. While 92% of Germans thought that businesses should be legally barred from selling consumer information without consent, only 88% of Americans felt the same way. The latter report shows that, across a broad range of categories, Germans are significantly more likely than Americans to consider data to be "moderately" or "extremely" private (Rose et al. 2014), including: social network information (14% higher); information about media usage and preferences (10% higher); dialed-phone-number history (9% higher); exact location data (6% higher); and surfing history (5% higher).

The significant American and German differences regarding personal information privacy are also evident in the work of scholars and commentators.

German privacy scholars, for example, are inclined to see technology almost exclusively as an ominous threat. They devote large parts of their work to documenting the new and ever-deeper ways technology is intruding upon our privacy. In 2009, Peter Schaar, the former Federal Commissioner for Data Protection and Information Freedom (*Bundesbeauftragter für Datenschutz und Informationsfreiheit*) published a representative manifesto entitled *Das Ende der Privatsphäre* (*The End of Privacy*). His alarm taps into Germans' awareness of the fact that IBM punch card technology was used in the Nazis' 1938 census, which helped the *Reich* develop the demographic profiles it needed to implement the Holocaust.

Computing technology, Schaar warns, can lead to an all-encompassing surveillance state of the kind Orwell imagined. The first fifty pages of Schaar's book constitute a careful accounting of the many ways in which Orwell's vision is now being realized. Schaar concludes, for example, that the Internet "has a shadowy side". He warns against the state's collection of data about our normal activities and the grave risks for data protection that result from our deepening "*Vernetzung*" (increasing use of the Internet). The most threatening possibility, Schaar notes, comes from the role technology is coming to play in the health care sector, including digital and networked records-keeping and data-driven or biometric research and treatment. Christine Hohmann-Dennhardt, in a 2006 essay published during her service as a Justice at the Federal Constitutional Court, also lamented the way in which technology seems to have rendered privacy an "antiquated description of an idyllic condition that belongs to the past". The year before he joined the Federal Constitutional Court as the reporting justice for matters concerned with, inter alia, personal liberty and data-protection, Wolfgang Hoffmann-Reim wrote about the "new risks" resulting from "new technologies", a development he compared to an arms race (1998). In 2014, Spiro Simitis, one of Germany's best-known experts in the field of data protection, took a similar approach, expressing particular concern about the ways in which technology is helping businesses track—perhaps even manipulate—consumers' shopping activities (Simitis 2005). If they do so at all, these German scholars only reluctantly acknowledge the ways that the same technologies have improved our lives.

The general skepticism towards technology in German privacy scholarship is accompanied by a contrasting pastoral, quasi-spiritual conceptualization of privacy. Wolfgang Schmale and Marie-Theres Tinnefeld represent the most extreme version

of this posture. In their 2014 book, *Privatheit im digitalen Zeitalter* (*Privacy in the Digital-Age*), they draw on the *Bible*'s "Garden of Eden" as a metaphor for privacy, because it points to the deeply-rooted cultural significance we place on the need for a protected retreat in which we can think and compose ourselves in full acceptance of nature and our bodies. The tangible garden, Schmale and Tinnefeld believe, should allow us to understand the abstract notion of data protection in more concrete terms. Sadly, they miss the chance to point out that it is in no small part the technology of a company called "Apple" that has chased us from privacy's paradise—or that the Garden of Eden may have been the most comprehensively surveilled place in human history (thanks to God's worrisome monitoring of the actions taken by Adam and Eve). In any case, Schmale and Tinnefeld see the European Union, with its culture and tradition of rights, as the "paradise" in which privacy can be restored. Hohmann-Dennhardt, taking a more secular turn, compared privacy to Rousseau's garden, in which one lives in simple harmony with nature. Simitis also understands data protection as part of an effort to fashion a utopian paradise. Schaar sees something of the sacred in privacy. He approvingly quotes Philippe Quéua, the former Director of the UNESCO's Division on Information and Society, who called privacy the "foundation of human dignity and the sacred nature of the human person". It is this quasi-spiritual approach to privacy that helps make sense of Schmale's and Tinnefeld's appeal for data and information aestheticism.

Daniel Solove, America's leading privacy scholar, sees things differently. First, Solove takes a more balanced approach to technology. He acknowledges that technology raises concerns about privacy. But Solove leaves space for an alternative view of these developments by acknowledging that "not everyone is concerned". He is less willing than the German privacy scholars to see technology in exclusively menacing terms. On the one hand, he characterizes many of the problems facing privacy as traditional or historical concerns, including risks to communications privacy (going back to the eras of letters, telegraphs, and telephones), risks resulting from information collection and surveillance (going back to ancient Jewish law and the original "peeping Tom" in the middle-ages), and risks resulting from information processing and aggregation (going back to the accelerating use of computers in the 1960s). These are old problems that are not exclusively linked to advances in technology. Nor is technology, for Solove, exclusively a threat. He is able to acknowledge the benefits of modern technology, even in areas (such as consumer data aggregation) that Schaar vilifies. "Identification is connecting information to individuals", Solove explains. While accepting that "identification" creates special problems, Solove recognizes that it also provides many benefits. Solove obviously cares a great deal about privacy. But he does not succumb to German scholars' Neo-Luddism.

Solove's most significant contribution to the theory of privacy is precisely his rejection of the broad and abstract approach adopted by German privacy scholars. Solove proposes a pragmatic, context-specific understanding of privacy. His is a "pluralistic" and not a "unitary" theory. Most conceptions of privacy suffer, Solove explains, because they are too broad. This is true of Louis Brandeis' and Samuel Warren's famous conclusion that privacy is the "right to be let alone". It is true of the notion that privacy involves a right to limit others access to the self, which

Solove sees as "too broad and vague". It is also true of the idea that privacy involves the right to control one's personal information. This approach is too broad, Solove explains, "because there is a significant amount of information identifiable to us that we do not deem as private". According to Solove, each of these general theories of privacy (and others I have not mentioned here) suffers from being "too vague" or "too broad". To solve this problem—which plagues the German approach to privacy—Solove proposes treating "privacy" as an "umbrella term that refers to a wide and disparate group of related things". Those "things", Solove urges, must be assessed pragmatically in their specific contexts. He quotes Serge Gutwirth, who observed that "Privacy … is defined by its context and only obtains its true meaning within social relationships". With this admonition in mind, Solove proposes differentiated concepts of privacy for distinct circumstances, including private relations in the family, privacy relating to one's body and sex, privacy associated with the home and privacy connected with communications.

America and Germany have different cultural expectations of personal information privacy. The question remains: how are these cultural differences reflected in the two countries' legal regimes for privacy?

Different Transatlantic Privacies

The different conceptions of privacy in America and Germany are shaped by and reflected in discordant regulatory regimes for the protection of privacy, especially in the context of the state's surveillance and intelligence-gathering activities. Our different notions of privacy are the consequence of different histories, different social and cultural forces, different political traditions and institutions, different legal cultures and different constitutional regimes. I will highlight only a few of these differentiating factors, including different American and German histories regarding privacy and intelligence-gathering; the two countries' different political cultures, which lead policy makers in the two systems to strike different balances with respect to the protection of privacy and the threat posed by terrorism; and the ways in which their different constitutional regimes operationalize different legal conceptions of privacy.

Different Histories

A common explanation for Americans' and Germans' different responses to the NSA-Affair is that their reactions reflect the disparate experiences they have made with respect to terrorism and their countries' use of personal surveillance. On both points, America and Germany have very different histories.

On the one hand, while the American government has long had an excessive interest in collecting information about its citizens, Americans have not had to confront brutal and invidious totalitarian dictatorships, such as those that used personal information to terrorize all Germans between 1933 and 1945 and East Germans between 1949 and 1990. On the other hand, the contemporary American acceptance of government intelligence gathering reflects the still-recent trauma of the 11 September 2001 terrorist attacks in the United States. Germany has its own history with terrorism. And Germany is a target of the current brand of Islamist terrorism (Deutsche Welle 2015; VICE 2016). Yet, the terror of the German Autumn is now several generations old, and the country—unlike its European neighbors in Spain, England, and France—has so far avoided large-scale Islamist terror attacks. The experience Germans had (and have been socialized to remember in subsequent generations) with Nazi and East German authoritarian surveillance and control helps to explain why German law places such a high priority on personal information privacy as a fundamental liberty protection (Gujer 2010). Germans have deep and profound historical reasons to prioritize privacy and no recent terrorist trauma that would suggest the need to sacrifice privacy in the name of security.

America's spies, domestic and foreign, have not been angels. But comparisons with the Gestapo and Stasi are fallacious. The FBI has played a role in curtailing personal freedoms. The CIA has killed and sown the seeds of bloody discord around the world. But it cannot be said that the American intelligence community was a central cog in one of history's largest and most gruesome genocides, or that it implemented one of history's most thorough, invasive and sinister regimes of surveillance and social control. It is an unfortunate fate, but those are distinctly German histories. The intrusions on privacy with which the American public has been confronted—including the programs revealed by Snowden—are a pale reflection of the domestic terror German governments have (relatively recently) inflicted on their citizens with the help of secret, state-sanctioned surveillance and intelligence gathering.

But it is not only the different quality (or quantity) of intelligence abuses that distinguishes the American and German histories. The consequences of the abuses, once exposed, also differ in significant ways. Americans have come to understand that intelligence abuses inevitably come to light and can be met with democratic responses inside the state's institutions and structures. This is the enduring lesson of the Church Committee (Miller 2008). It has also been true in the post-9/11 era. The scandal involving the Terrorist Surveillance Program prompted President George W. Bush to discontinue the NSA initiative and to place future surveillance programs under the authority of the Foreign Intelligence Surveillance Act and the Foreign Intelligence Surveillance Court (NYT 2007). Snowden's revelations have generated significant reform, including President Obama's Policy Directive 28 and the USA Freedom Act (The White House 2014). By contrast, the only outcome of the extreme intelligence abuses Germans endured in the 20th century (under the Nazis and in East Germany) was the complete dissolution of the respective states. External forces were needed in both cases—with respect to the German Reich and the German Democratic Republic—to overcome the political cultures that had fostered and facilitated massive surveillance regimes. Unlike the Americans, the Germans have not experienced

the corrective possibility of an existing democratic system confronting their worst intelligence abuses.

Different Political Cultures

A country's response (legal or otherwise) to the threat of terrorism is affected by many factors. It is the most straightforward republican calculation, but one factor is the degree to which the political class is required to be attuned and accountable to popular sentiments, such as fear of terrorism. The American and German political systems calibrate this dynamic differently. According to typologies originally mapped by comparative political scientists such as Lijphart (1999), American politics are seen as more majoritarian while German politics are seen as more consensual (Dickovick and Eastwood 2013). Democracies classified as majoritarian are characterized by high levels of subsystem autonomy and intense competition for majoritarian support among elites (Lijphart 1969). Consensual democracies are characterized by limited subsystem autonomy and deliberate efforts on the part of elites to take actions that counteract the potentially destabilizing impulses of shifting majorities. Confirming Germany's classification as a consensual democracy, Ralf Dahrendorf famously described German politics as "government by elite cartel" (1967). Elsewhere, Lijphart has used the concepts "mass political culture" and "elite political culture" to describe these distinct democratic approaches (1971).

A number of features in the two systems confirm these labels. America is a heterogeneous society with strong subsystem autonomy. Politics in the United States harnesses these forces through multi-level and nearly constant competition in the formation of governing majorities and for the framing of policy. The majoritarian and accountability elements of the systems are institutionally secured through biennial, direct elections for Congress and the (seeming) direct election of the president (U.S. Const. art. II, § 2–3; Dahl 2003). The autonomy of subsystems can be seen in the relative lack of party discipline and the mélange of civil society advocates, activists and lobbyists (Beutler 2014). Germany is a more homogenous society with weaker subsystem autonomy. Elites in Germany have seized on these factors to fashion and maintain a governing consensus. In its most benign form, this has served as a curative to the highly-fractious and unstable politics of the Weimar era (Schwarz 2010). Germany's consensus politics are facilitated by a number of structures, including the so-called *Parteienstaat* (which almost exclusively privileges the traditional political parties in the democratic process); proportional, party-based election of half the parliamentarians; and the proportional-parliamentary election of the chancellor (Kommers and Miller 2012). Grand coalitions featuring the largest center-right parties (CDU-CSU) and the largest center-left party (SPD) are a prominent example of Germany's consensus politics (Lijphart 1969). Three of the last four governments have been formed through grand coalitions of this type.

The distinct political cultures, and the institutions that reinforce them, produce different conditions with respect to the control and oversight of intelligence

services—and, by extension, the two societies' understanding of privacy. The strict separation of powers in America's Madisonian system, for example, permits Congress to play a significant role in overseeing the executive's intelligence-gathering operations. This can be reinforced by frequent partisan splits between the presidency and the Congressional majority. Again, this was the lesson of the Church Committee. Especially in the wake of the 11 September 2001 terrorist attacks, an inter-branch and bipartisan security consensus formed in America that undermined the possibility that checks and balances would be an adequate brake on the government's intelligence-gathering activities. Still, Congress found extremely rare common ground to enact the USA Freedom Act in 2015, a move that one commentator described as a signal "that the days when Congress gave maximal deference to the executive branch might finally be over" (Lemieux 2015). The success of this reform was also a product of America's strong subsystem autonomy, which helps to explain the emergence and political success of the "Tea Party" movement (Beutler 2014). The Tea Party movement has, in part, been animated by libertarian concerns about government overreach, including on issues of intelligence gathering and security (Clement 2013). The 2012 Senate Intelligence Committee's historic "Study of the Central Intelligence Agency's Detention and Interrogation Program" may be a more inspiring example of the possibility in the American system for inter-branch oversight. The *Bundestag's* intermingled relationship with the chancellor and her cabinet—typical of the parliamentary model—leaves the German parliament with a smaller role in controlling the executive's intelligence-gathering function. The success of the *Bundestag*'s Investigative Committee on the NSA-Affair, for example, will largely depend on the engagement of the parliamentary opposition, which held only four of the Committee's sixteen seats. With these structural differences in mind, it is not surprising that the American judiciary has shown more restraint than the German judiciary in its review of privacy and intelligence-gathering cases.

Different Constitutional Laws of Privacy

An examination of the two countries' constitutional systems reveals dramatic differences with respect to privacy. These regimes are distinguished, in part, by their different constitutional texts and a resulting, very different jurisprudence of privacy.

If constitutional text is the beginning of constitutional analysis, then American and German constitutional law start from very different places with respect to the issue of personal information privacy. It is an old trick, for example, to note that the U.S. Constitution never uses the term "privacy" while the German constitution does. Article 10 of the Basic Law provides that "the *privacy* of correspondence, posts and telecommunications shall be inviolable". More than its mere invocation of the term "privacy", Article 10 is significant because it establishes a concrete constitutional protection for the exact activities involved in the NSA-Affair. With its modern outlook, Article 10 also seems to better anticipate the contemporary forms of electronic communication—such as email and smartphone usage—that are central to

reimagining privacy for our digital age (Fetzer and Yoo 2013). Naturally, America's 18th century text is more awkwardly suited to that project.

Of course, constitutional law is not bound to the narrowest construction of the charter's text. Slightly broader readings of both constitutions reveal a number of liberty protections that serve the same interests as those we imagine to be involved in privacy (de Vries 2013). Without using the term "privacy", the Fourth Amendment to the U.S. Constitution nevertheless protects Americans from unreasonable searches and seizures "in their persons, houses, papers, and effects". This has been extended to include some of the forms of communication covered by Article 10 of the German Basic Law (Fetzer and Yoo 2013). Both constitutions also protect against government intrusions into the home (U.S. Const. amends. III, IV, Basic Law art. 13).

The Basic Law, however, prominently includes text that identifies and protects liberty interests and values that can be more easily read to be constituent elements of privacy. Articles 2 and 1 of the Basic Law, for example, are clear and very expressive commitments to personal freedom and human dignity. The human condition to which these protections aspire—including the relationship to state power—obviously involves an inviolable intimate sphere (Kommers and Miller 2012). America's Due Process Clause has been put to similar use, but without the same clarity and expressive force (Stephens 2015). Similarly, the Eighth Amendment to the U.S. Constitution, which prohibits "cruel and unusual punishments", asserts a dignified (privacy-respecting) image of the human condition, but does so chiefly in the limited circumstances of the state's penal function.

On the basis of their distinct constitutional texts and traditions, the American and German courts have developed dissimilar jurisprudences on the issues of personal information privacy. German law resorts to a general concept of privacy derived from Articles 2 and 1 of the Basic Law. American law recognizes discrete privacy interests to which it extends distinct legal protections. The privacy interests implicated by the NSA-Affair, for example, are chiefly a concern of the Fourth Amendment to the U.S. Constitution.

A number of recent cases decided by the Constitutional Court have recognized a right to personal information privacy in surveillance or data-collection scenarios on the basis of the Court's pioneering jurisprudence that conceived a right to "informational self-determination". The right was first articulated in the 1983 *Census Act Case* (65 BVerfGE 1, 1982). The Constitutional Court demanded that the parliament amend the federal census statute to ensure that there would be no abuses in the collection, storage, use and transfer of the personal data gathered during the census. The Constitutional Court demonstrated remarkable foresight—with respect to technology, data collection and the potential for the chilling effects of surveillance—when articulating the basis for the new right.

The Constitutional Court derived the right to informational self-determination from the general personality and dignity protections secured by Articles 2 and 1 of the Basic Law. That constitutional doctrine has provided a foundation for a general concept of privacy that finds relevance in a number of settings. The easy application of this general privacy interest in circumstances as various as transsexual rights and

information privacy is a consequence of the German legal culture's preference for abstract concepts.

The right to informational self-determination has taken on increasing relevance as Germany pursued its own counter-terrorism measures in the wake of the 11 September 2001 attacks in the United States. Perhaps the most dramatic example of the Constitutional Court's promotion of privacy in the context of those policies was the *Online-Durchsuchungen Entscheidung* (*Online Computer Surveillance Case*), which was decided in 2008 (120 BVerfGE 274). The Court issued a landmark ruling in defense of the "right to the confidentiality and integrity of information technological systems". The Constitutional Court derived this right from the general personality protection secured by Articles 2 and 1 of the Basic Law. The case involved challenges to a state law that empowered intelligence officials to conduct surveillance and collect data by covertly infiltrating computer systems through the Internet. The decision extended the Basic Law's privacy protection to personal computers. The Constitutional Court explained that "today's personal computers can be used for a wide variety of purposes, some for the comprehensive collection and storage of highly personal information… corresponding to the enormous rise in the importance of personal computers for the development of the human personality". The right to informational self-determination, said the Constitutional Court, protects individuals against the disclosure of personal data unless surveillance and data collection is necessary to avoid a "concrete danger" to human life or the security of the state. The Constitutional Court noted, "the fundamental right to the integrity and confidentiality of information technology systems is to be applied… if the empowerment to encroach covers systems that, alone or in their technical networking, contain personal data of the person concerned to such a degree that access to the systems facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of his or her personality". The Constitutional Court concluded that general exploratory online searches based on mere suspicion of some remote danger, however serious, is constitutionally impermissible.

American courts, if they are willing to engage with the issues raised by the NSA-Affair, have largely been concerned with the discrete privacy protection provided by the Fourth Amendment to the U.S. Constitution. The broader notion of privacy, anchored in the due process clauses of the Fifth and Fourteenth Amendments, has not played a role.

The Fourth Amendment was implemented in response to the British practice of issuing general search warrants that lacked probable cause (Pittman 1954). And, to the degree that it secures protection of the individual against the overwhelming power of the state, the Fourth Amendment also is a reflection of the founding precepts of American democracy (Newman 2007). In its seminal decision in *Katz v. U.S.*, the Supreme Court rejected the traditional jurisprudence that had aligned the Fourth Amendment's privacy protection with notions of property and trespass (389 U.S. 347, 1967). The Court in *Katz* emphatically declared that "the Fourth Amendment protects people, not places". The substance of this protection consists in the requirement that government searches may be performed only when authorized by a detailed and specific warrant that has been issued by a neutral and detached magistrate on the

basis of sworn evidence demonstrating probable cause (McInnis 2009). The Court has, however, identified a number of exceptions to the Fourth Amendment's warrant requirement, permitting searches that are otherwise "reasonable". Some contend that these exceptions have swallowed the rule, leaving the Fourth Amendment a hollow form that no longer provides meaningful privacy protection (Starkey 2012).

A threshold question is what constitutes a "search" for Fourth Amendment purposes. Far more than the substantive scope of Fourth Amendment protection, this preliminary issue has complicated the application of the Fourth Amendment to intelligence-gathering cases. After *Katz*, the occurrence of a "search" no longer depended on evidence that the state had made a physical intrusion into a private space. Instead, the Court found an intrusion into Katz's *personal sphere of privacy*. In *Katz*, a wiretap had been placed on the outside of a glass pay phone box permitting law enforcement officers to listen to Katz's phone conversation. Although no physical intrusion into the pay phone box had taken place, the Court reasoned that Katz had a subjective expectation that "the words he utters into the mouthpiece will not be broadcast to the world" and that society would accept Katz's expectation as reasonable. This is now the standard for determining whether a "search" has taken place, without which the substantive protections of the Fourth Amendment will not apply: (1) a person "has exhibited an actual (subjective) expectation of privacy"; and (2) society is prepared to recognize that this expectation is (objectively) reasonable.

The Supreme Court applied this standard in *Smith v. Maryland* and found that a Fourth Amendment search had not occurred (442 U.S. 735, 1979). This is relevant because the circumstances of the *Smith* case might be seen as closely analogous to those involved in the NSA-Affair. In *Smith*, law enforcement officers collected evidence of the suspect's telephone contacts by installing a "pen register" on his telephone line at the telephone company's offices. An electronic device, the pen register records only the numbers called from a particular telephone line. The content of phone calls is not documented. The Court concluded that neither of the elements necessary for a Fourth Amendment *search* existed in the case.

First, Smith did not have a subjective expectation in the privacy of the telephone numbers he dialed because "people in general [do not] entertain any actual expectation of privacy in the numbers they dial". The Court reasoned that telephone users know that the phone company registers the numbers they dial and keeps permanent records of that information for billing purposes.

Second, the Court found that a subjective expectation of privacy with respect to the phone numbers one dials—as unlikely as that expectation would be—cannot be regarded as reasonable. Society appreciates, the Court explained, that electronic equipment is used extensively to track and catalogue the telephone numbers called from any particular phone. At the very least, the Court concluded, this is common (and commonly known), because it is necessary for the telephone company to keep billing records. The Court ruled that, in dialing the telephone numbers, Smith held that information out to third parties (at least the telephone company). Exposing information in such an indiscriminate way, which stripped it of any subjective or objective expectation of privacy, meant that the government's collection of the telephone numbers involved only the acquisition of non-private information. On the basis of the

third-party doctrine, the Supreme Court ruled that a search had not occurred and that the Fourth Amendment had no applicability to the case whatsoever.

Judge William Pauley of the Southern District of the New York Federal District Court drew on the obvious parallels between the facts in the *Smith* case and the NSA's bulk telephony metadata collection program when he dismissed a Fourth Amendment challenge to the NSA's surveillance measures in December 2013. Citing *Smith*, Judge Pauley ruled that phone users had no reasonable expectation of privacy that would give them Fourth Amendment rights, especially with respect to information they voluntarily provide to third parties, such as telephone companies (*American Civil Liberties Union v. James Clapper*). In 2015, on appeal from Judge Pauley's order, the United States Court of Appeals for the Second Circuit found that the NSA's bulk telephony metadata collection program exceeded the surveillance authority established by the relevant statutory provisions. But the Appeals Court refused to rule on the constitutional issues in the case, even as it expressed grave misgivings about the continuing adequacy of the *Smith* case and the third party doctrine for ensuring privacy under present technological conditions.

In at least two other lawsuits filed in response to the NSA-Affair (*Smith v. Obama* and *U.S. v. Muhtorov*), the first-instance courts found that the *Smith* precedent and the third-party doctrine precluded a Fourth Amendment challenge to the NSA's data-collection programs.

The high courts in both countires are increasingly aware of the challenge modern telecommunications technology poses to their respective privacy traditions. The German jurisprudence seems better adapted to the new circumstances. The German jurisprudence, dating back to the *Census Act Case*, has been conscious of the distinct privacy harm that could result from the accumulation of personal information data. In its recent cases, the Constitutional Court has sought to strengthen constitutional privacy protection in response to the sweeping personal portrait our ever-more extensive use of technology makes it possible for the state to develop from mere telecommunications metadata. This approach is in line with what is referred to as the "mosaic" theory of privacy, which seeks to account for intrusive conduct as a "collective whole", rather than as isolated or sequential incidents (Kerr 2012).

The American jurisprudence is just beginning to struggle with the dramatic challenge contemporary telecommunications technology poses for privacy. If the courts will hear the cases at all, then so far they have hewn to the traditional sequential approach to enforcing the Fourth Amendment. The clearest move in the direction of the mosaic approach occurred in the *Carpenter v. United States* case decided by the Supreme Court in 2018. Carpenter challenged the government's use of cell-site location information (CSLI) as evidence of his proximity to a number of robberies. CSLI is created as users' cell phones constantly scan their vicinity for the most effective available cell tower. This record produces an increasingly precise record of a cell phone's geographic location. Cell phone network providers routinely document this information. The Supreme Court ruled that the use of the CSLI records should be distinguished from the dialed phone numbers involved in *Smith*, and that their use in Carpenter's trial constituted an illegal "search" under the Fourth Amendment. Chief Justice Roberts wrote the opinion for the Court. First, the Court nodded towards the

mosaic theory of privacy by noting that CSLI records represent a different quantity and quality of information, which is comprehensive, encyclopedic and effortlessly compiled. This information, Justice Roberts explained, touches on the concern the Supreme Court has shown for the privacy owed to "the whole of a person's physical movements". Justice Roberts warned that CSLI represents near perfect surveillance of a person's location—going back almost five years. The risk of excluding CSLI from the protection of the Fourth Amendment, the Court insisted, results in part from the pervasive and insistent role of cell phones in modern life. Second, the Court distinguished the CSLI from the dialed phone numbers in *Smith* by noting that the information involved is not voluntarily shared in any common understanding of that term. Justice Roberts explained that cell phones automatically and constantly produce CSLI, even when the phone's user is not actively employing one of the phone's applications.

For all their differences with respect to the constitutional protection of privacy, the Supreme Court's decision in the *Carpenter* case suggests that American and German jurisprudence might be converging in this discrete but profound way. It would be wrong, however, to rush from this conclusion to any claim of harmonization or a hoped-for universalization of privacy rights. The Supreme Court insisted in *Carpenter* that its decision was narrow and does not disturb the broad and general application of the third-party doctrine articulated in the *Smith* case.

History, politics and law confirm and explain the different notions of privacy prevalent in America and Germany.

Conclusion

The different responses to the NSA-Affair in America and Germany are the product of the two countries' different notions of privacy. Those distinctions are embodied in—and foster—very different legal regimes for the protection of privacy.

The American approach shows greater confidence in the political process for striking the balance between privacy and security. When the courts become involved, they enforce a specialized constitutional privacy right that has been calibrated to respond to the state's surveillance and intelligence-gathering activities. This jurisprudence, so far, has only cautiously embraced the mosaic approach to privacy, which seems to better account for the comprehensive and intimate uses to which we put technology today. The German approach emphasizes the judicial enforcement of a broad and general concept of privacy. In its sensitivity to technology's ubiquity and the deeply revealing portraits that can be developed through the accumulation of a vast amount of discrete data, the German jurisprudence has been a pioneer of the mosaic approach to privacy.

Most profoundly, operating in their unique socio-legal contexts, the two constitutional privacy regimes offer very different visions of personhood. On the one hand, the German Constitutional Court has imagined and enforced a substantive and objective vision of personhood that includes a protected private and intimate sphere. The

state is obliged to help realize this vision. On the other hand, the American courts have reinforced individuals' freedom of action, including the autonomy to dispose of one's privacy. This is an autonomous and subjective vision of personhood.

The challenge posed by the NSA-Affair—a challenge that underlies all our discussions about privacy in our increasingly digitalized and data-centric future—is not to envision and enforce a harmonized approach to privacy, but to come to accept with William Shakespeare that "a rose by any other name would smell as sweet". Our best chance for acting productively to ensure privacy is to appreciate and respect our different notions of privacy.

References

Articles

Altman, I. (1977). *Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33*(66).

Barnett, S. R. (1999). *The right to one's own image: Publicity and privacy rights in the United States and Spain*. *American Journal of Comparative Law, 47*, 555.

Bignami, F. (2007). *European versus American Liberty: A comparative privacy analysis of antiterrorism data mining*. *Boston College Law Review, 48*, 609.

Chandler, A. (2015, April 6). What it takes to make people care about NSA surveillance. *The Atlantic*. http://www.theatlantic.com/national/archive/2015/04/naked-selfies-and-the-nsa/389778/.

Dickovick, J. T., & Eastwood, J. (2013). *Comparative Politics, 452*.

Fetzer, T., & Yoo, C. S. (2013). New technologies and constitutional law. In M. Tushnet, et al. (Eds.), *Routledge handbook of constitutional law* (Vol. 485, pp. 490–492).

Hoffmann-Riem, W. (1998). Informationelle Selbstbestimmung in der Informationsgesellschaft—Auf dem Wege zu einem neuen Konzept des Datenschutzes. *Archiv des öffentlichen Rechts, 123*, 513, 517–518.

Hohmann-Dennhardt, C. (2006). Freiräume—Zum Schutz der Privatheit. *Neue Juristische Wochenschrift, 59*, 545, 546.

Kerr, O. S. (2012). The Mosaic theory of the fourth amendment. *Michigan Law Review, 111*, 311, 316–317, 320.

Krotoszynski, R. J., Jr. (2014–2015). Reconciling privacy and speech in the era of big data: A comparative legal analysis. *William & Mary Law Review, 56*, 1279.

Lachmayer, K. (2014). The challenge to privacy from ever increasing state surveillance: A comparative perspective. *UNSW Law Journal, 37*, 748.

Lijphart, A. (1969). Consociational democracy. *World Politics, 21*, 207.

Lijphart, A. (1971). Comparative politics and the comparative method. *American Political Science Review, 65*, 682, p. 213.

Pittman, R. C. (1954, May). The supremacy of the judiciary: A study of preconstitutional history. *ABAJ, 40*, 389, 391 (quoting Justice Horace Gray Jr.).

Starkey, B. S. (2012). A failure of the fourth amendment & equal protection's promise: How the equal protection clause can change discriminatory stop and frisk policies. *Michigan Journal of Race & Law,* 18, 131.

Stephens, O. H., et al. (2015). II *American Constitutional Law* (6th ed., 406).

Walsh, B. (1976–1977). The judicial power and the protection of the right of privacy. *Dublin University Law Journal, 1*, 3.

Whitman, J. Q. (2004). The two western cultures of privacy: Dignity Versus liberty. *Yale Law Journal, 113,* 1151, 1155.
Yang, T. L. (1966). Privacy: A comparative study of english and american law. *International and Comparative Law Quarterly,* 15, 175.

Books

Dahl, R. A. (2003). *How democratic is the American Constitution?* (73).
Dahrendorf, R. (1967). *Society and democracy in Germany* (276).
de Vries, K. (2013). Privacy, due process, and the computational turn. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology* (9, 17–19).
Gujer, E. (2010). Germany: The long and winding road. In G. J. Schmitt (Ed.), *Safety, liberty, and islamist terrorism: American and European approaches to domestic counterterrorism* (62, 63).
Hofstede, G. (1980). *Cultural consequences: International differences in work related values*.
Hofstede, G. (1991). *Cultures and organizations: Software of the mind*.
Kommers, D. P., & Miller, R. A. (2012). *The constitutional jurisprudence of the Federal Republic of Germany* (3rd ed., 269, at 405).
Lijphart, A. (1999). *Patterns of democracy*.
McInnis, T. (2009). *The evolution of the fourth amendment* (51–56, 75).
Newman, B. A. (2007). *Against that "Powerful Engine of Despotism": The fourth amendment and general warrants at the founding and today*.
Miller, R. A. (Ed.). (2008). *U.S. National Security, Intelligence and Democracy: From the Church Committee to the War on Terror*.
Nissenbaum, H. (2009). *Privacy in context*.
Schaar, P. (2009). *Das Ende der Privatsphäre* (pp. 38, 40, 42, 49, 54, 75–78).
Schmale, W., & Tinnefeld, M.-T. (2014). *Privatheit im digitalen Zeitalter* (11, pp. 18, 86, 244).
Schwarz, H. P. (2010). Woran scheitern deutsche Bundeskanzler? In C. Hillgruber & C. Waldhoff (Eds.), 60 *Jahre Bonner Grundgesetz – Eine geglückte Verfassung?* 29.
Simitis, S. (Ed.). (2014). *Bundesdatenschutzgesetz—Kommentar* (8th ed.).
Simitis, S. (2005). Datenschutz—eine notwendige Utopie. In R. M. Kiesow, et al. (Eds.), *Summa—Dieter Simon zum 70. Geburtstag* (pp. 511, 527).
Solove, D. J. (2008). *Understanding privacy* (4, 5, 9, 16, 18, 20, 25, 29, 45, 47, 50, 61–62, 107–108, 118, 122–123).

Judgements and Laws

American Civil Liberties Union (ACLU) v. James Clapper, No. 13-3994 (S.D. New York December 28, 2013), 959 F.Supp.2d 724.
American Civil Liberties Union v. James Clapper, 785 F.3d 787 (2d. Cir. 2015).
Carpenter v. United States, No. 16-402, 585 U.S. ___ (2018).
Katz v. United States, 389 U.S. 347 (1967).
Smith v. Maryland, 442 U.S. 735 (1979).
Smith v. Obama, 24 F.Supp.3d 1005 (2014).
United States v. Muhtorov, No. 1:12-cr-00033-JLK (D. Colo.).
Census Act Case, 65 BVerfGE 1 (1982).
Online Computer Surveillance Case, 120 BVerfGE 274 (2008).

Constitution of the United States, https://www.senate.gov/civics/constitution_item/constitution.htm.

German Basic Law (C. Tomuschat, D. P. Currie, & D. P. Kommers, Trans.). https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.pdf.

Media and Art

AStA FU. (2014, June 23). *AStA FU Informs Edward Snowden about his Honorary Membership and Demands Asylum for Edward Snowden*, AStA FU. https://www.astafu.de/content/asta-fu-informs-edward-snowden-about-his-honorary-membership-and-demands-asylum-edward-snowd.

Beutler, B. (2014, May 21). The American right, not the 'Tea Party,' is the GOP's big liability. *New Republic*. https://newrepublic.com/article/117845/gop-primary-victories-aside-republicans-still-have-gop-base-problem.

Clement, S. (2013, July 26). Tea party privacy concerns skyrocket, poll finds. *Washington Post*. https://www.washingtonpost.com/news/the-fix/wp/2013/07/26/tea-party-privacy-concerns-skyrocket-poll-finds/.

Cohen, J. (June 10, 2013). Most Americans back NSA tracking phone records, prioritize probes over privacy. *Washington Post*. https://www.washingtonpost.com/politics/most-americans-support-nsa-tracking-phone-records-prioritize-investigations-over-privacy/2013/06/10/51e721d6-d204-11e2-9f1a-1a7cdee20287_story.html.

Deutsche Welle. (2015, February 28). *Police in German city warn of islamist terrorism threat*. http://www.dw.com/en/police-in-german-city-warn-of-islamist-terrorism-threat/a-18286410.

Lemieux, S. (June 8, 2015). How congress learned to stop bowing to president Obama on national security. *The Week*. http://theweek.com/articles/558953/how-congress-learned-stop-bowing-president-obama-national-security.

Noack, R. (2015, June 23). The global cult of Edward Snowden keeps growing. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2015/06/23/the-global-cult-of-edward-snowden-keeps-growing/.

Richter, S., & Albrecht, J. P. (2013, October 30, 7:19 AM). NSA spying on Europe reflects the transatlantic culture gap. *The Guardian.* http://www.theguardian.com/commentisfree/2013/oct/30/nsa-spying-europe-transatlantic-culture-gap.

Rosenbush, S. (June 12, 2014, 5:16 PM). EMC's new index shows public is deeply conflicted over privacy. *Wall Street Journal.* http://blogs.wsj.com/cio/2014/06/12/emcs-new-index-shows-public-is-deeply-conflicted-over-privacy/.

Spiegel Online. (2013, November 8). Spying fallout: German trust in United States plummets. http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html.

The New York Times, (2007, January 17). Letter from Alberto R. Gonzalez, Attorney General of the United States, to Senator Patrick Leahy and Senator Arlen Specter. http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf.

The White House, Press Release, Office of the Press Sec'y, Presidential Policy Directive/PPD-28, at 5. (2014, January 17). Uniting and Strengthening America by fulfilling rights and ending eavesdropping, dragnet-collection and online monitoring act [USA FREEDOM Act], Pub. L. No. 114-23, 129 Stat. 268 (2015).

VICE. (Jan. 1, 2016, 10:49 AM). Germany still on alert after tip about possible Islamic State terror attack. https://news.vice.com/article/germany-still-on-alert-after-tip-about-possible-islamic-state-terror-attack.

Studies and Reports

Bellman, S., et al. (2004). international differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*, 313, 315, 321.

Center for Creative Leadership. (2014). Leader effectiveness and culture: The GLOBE study. http://www.ccl.org/leadership/pdf/assessments/GlobeStudy.pdf.

Cockcroft, S. (2007). Culture, law and information privacy. In *Proceedings of European and Mediterranean Conference on Information Systems* 2007 (EMCIS2007), June 24–26, 2007, Polytechnic University of Valencia, Spain. http://www.academia.edu/7688223/CULTURE_LAW_AND_INFORMATION_PRIVACY.

EMC, The EMC Privacy Index Global & In-Depth Country Results. (2014). http://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf.

IBM. (1999, October). *IBM multi-national privacy survey consumer report 14*. IBMftp://www6.software.ibm.com/software/security/privacy_survey_oct991.pdf.

Motel, S. (2014, April 15). NSA coverage wins Pulitzer, but Americans remain divided on Snowden leaks. Pew Research Center. http://www.pewresearch.org/fact-tank/2014/04/15/nsa-coverage-wins-pulitzer-but-americans-remain-divided-on-snowden-leaks/.

Pew Research Center. (2013, June 17). Public split over impact of NSA leak, but most want Snowden prosecuted. http://www.people-press.org/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted.

Rose, J., et al. (2014, February 19). Data Privacy by the Numbers, *bcg.perspectives*. https://www.bcgperspectives.com/content/Slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/#ad-image-0.

Senate Select Committee on Intelligence—Committee's Study of the Central Intelligence Agency's Detention and Interrogation Program. (December 13, 2012). Available at https://web.archive.org/web/20141209165504/http://www.intelligence.senate.gov/study2014/sscistudy1.pdf.

Professor Russell Miller is the J.B. Stombock Professor of Law at Washington and Lee University. His teaching and research focus on public law subjects and comparative law theory and methods. Professor Miller, an expert in German law and legal culture, is the author/editor of a number of books. He has been recognized for his work on German law and transatlantic affairs. In 2013 Professor Miller was named a KoRSE Fellow (http://www.sicherheitundgesellschaft.uni-freiburg.de/) at the University of Freiburg. Professor Miller was a 2009/2010 Fulbright Senior Research Fellow in residence at the Max Planck Institute for Comparative Public Law and Public International Law (http://www.mpil.de/ww/en/pub/news.cfm) in Heidelberg, Germany. In appreciation for his work on behalf of the Robert Bosch Fellowship and German-American relations, Professor Miller was recognized as the Bosch Alumni of the Year in 2012. Professor Miller has contributed to or been quoted or cited in a number of global media sources, including The *Los Angeles Times*, *the Frankfurter Allgemeine Zeitung*, *Reuters*, and *Der Spiegel*.