Systematic government access to private-sector data in Germany

Paul M. Schwartz*

Abstract

- German law has long been strongly committed to informational privacy, with protection to be found at the constitutional and statutory levels.
- Legislation over the last two decades has expanded the ability of the government, including the police and intelligence agencies, to process, store, and share personal information.
- The leading examples from this study of systematic data access in Germany concern; the leading examples from this study concern 'strategic searches' by intelligence agencies, data mining by the police, the structured statutory system for access to the contents of the 'Anti-Terror File', and the police's 'radio-cell inquiries' pursuant to the Code of Criminal Procedure, section 100g.
- German unease with systematic data access is shown by current controversies with data retention, a new federal bill for 'residence reporting', the abandonment of the ELENA process, and the proposal for a '*Bundes-Cloud*' that is intended to keep German personal data out of the datacentres of US corporations.

National legal context and fundamental principles

Germany has a strong commitment to the rule of law and to information privacy. Its concept of the 'rule of law' is best summed up in the idea of the *Rechtsstaat*, or 'legal state'. The *Rechtsstaat* is a state that is based on civil liberties as well as the expression and protection of constitutional rights. For example, Article 1(1) of the German constitution, the Basic Law, states that human dignity is inviolable, and that the duty of all state authority is to respect and protect it.[1] The Basic Law's Article 2(1) in conjunction with Article 1(1) guarantees the right of the free development of the personality. Article 20(3) of the Basic Law explicitly binds all three branches of government to the constitutional order and to law and justice.

As for information privacy, it has constitutional status in Germany. The constitutional protections derive both from specific and more general constitutional provisions of the Basic Law. These are found in Article 10 (privacy of communications); Article 13 (inviolability of the home); and Article 2(1) in conjunction with Article 1(1) (the basis for a judicially created 'right of informational self-determination' and 'right of confidentiality and integrity in information systems'). This paper discusses these provisions in more detail in the next section.

Federal and state data protection commissioners also play an important role in privacy policy-making in Germany. These officials are established under the Federal Data Protection Law (*Bundesdatenschutzgesetz*, or BDSG).[2] They monitor the data use of the government and of the private sector, and they direct public attention to violations of privacy.

A high level of public attention in Germany is directed to privacy issues. The constitutional complaint against a data retention law was brought by 35,000 citizens, which set a record in Germany for public participation in constitutional litigation. As another indication of this public interest, over 240,000 persons in Germany have opted out of Google Street View. Finally, the media cover privacy issues heavily, and general audience books on the topic, such as *Die Datenfresser* (2011)(The Data Eaters) and *Die Facebook Falle* (2011) (The Facebook Trap), receive significant attention.

* Paul M. Schwartz, University of California, Berkeley, School of Law. Email: pschwartz@law.berkeley.edu.

1 Grundgesetz für die Bundesrepublik Deutschland [GG] [Basic Law for the Federal Republic of Germany, Basic Law], Bundesgesetzblatt III. [BGBl. III.] 100–1 (1949) (most recently amended by Law of July 21, 2010, BGBl. I., 944).

2 A discussion of statutory privacy law in Germany can be found in the subsection entitled 'Statutory Law'.

Finally, the terrorist attacks in the USA on 9/11 and subsequent terrorist actions in Madrid and London have caused the *Bundestag*, or Federal Parliament, to enact a wide-reaching series of laws that modified the structure under which German law enforcement agencies and intelligence organizations gather and share information. The trend of increased legislation about national security and crime had already started before 9/11; an initial round of legislation was driven by post-Cold War concerns about new threats to Germany in a Europe without traditional borders and the traditional post-war power blocs.

Thus, while many in Germany support informational self-determination and data protection, other views exist on these matters. For example, there has also been support expressed for a 'right to security'. In 2008, Manfred Baldus, a German law professor, warned, 'A minimum of State leads not in the least to a maximum of freedom'.[3] He argued that 'real freedom depended as well on the exclusion of private violence' and 'that the security function of the state, that is, the security of freedom from private violence that the state provides, counts as one of the essential and indispensable components of a state centered on freedom and based on the rule of law.' A series of Interior Ministers have stressed the importance of the state's protection of security and provided strong policy leadership for greater data sharing among government agencies and, under certain circumstances, between the private sector and government.

Constitutional, statutory, and regulatory overview

Law

Constitutional provisions

There is a significant body of constitutional law in Germany concerning information privacy. The specific constitutional protections for privacy include the Basic Law's Article 10, which creates constitutional norms regarding the government's ability to carry out the surveillance of communications, including letters and telecommunications. In addition, Article 13 of the Basic Law protects the inviolability of the home and creates constitutional norms for the government's ability to carry out wiretaps within a residence. As Francesca Bignami observes regarding telecommunications privacy law, 'At the constitutional level [in Europe] . . . only in Germany is the privacy of communications and data related to communications afforded protection under a separate article of the Constitution and a separate line of cases.'[4]

The Basic Law's general provisions that safeguard privacy are Article 2(1) in conjunction with Article 1(1). The German Constitutional Court has read these provisions as protecting a general right of personality. As the Federal Constitutional Court observed in its *Data Screening* opinion of 2006, the general right of personality 'is a gap-filling guarantee' that 'is especially required against the background of novel dangers for the development of personality that appear in accompaniment to the progress of science and technology.'[5]

From this general right, the Constitutional Court has identified other important individual privacy rights. These are the right to a private sphere in which one is to be free to shape one's life, a right to one's spoken word, a right of informational self-determination, and, more recently, a right of confidentiality and integrity in information systems.[6]

As a general matter, the German constitutional law of information privacy, as established in the *Census* decision of 1983, permits a public sector entity to collect, process, and transfer personal information subject to a limited set of conditions. One of the most important of these is the requirement that there be a statutory basis for this informational activity. Such a statutory basis requires that all personal data processing have a valid legislative basis, clearness of norms, and observance of the 'principle of proportionality'. The principle of proportionality (*Verhältnismäßigkeitsgrundsatz*) consists of a three-prong test for evaluating the constitutionality of legislation. First, the Court asks whether the means chosen are suitable (*geeignet*). Second, it inquires whether the means chosen are necessary (*erforderlich*). Finally, the Court examines whether the means chosen are reasonable (*zumutbar*).

Due to these important provisions of the Basic Law, and the extensive case law of the Constitutional Court, this Court plays a central role in deciding questions relating to the boundaries of governmental access to private-sector data. The Constitutional Court's significant involvement in these matters is one of the most visible manifestations of the German commitment to

3 Manfred Baldus, 'Freiheitssicherung durch den Rechtsstaat des Grundgesetzes', in Stefan Huster and Karsten Rudolph (eds), *Vom Rechtsstaat zum Präventionsstaat* Frankfurt am Main, Suhrkamp Verlag (2008) 107, 109.

4 Francesca Bignami, 'European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining', (2007) 48 B.C. L. Rev. 609, 639.

5 115 BVerfGE 320, 341–66 (2006) (*Data Screening*).

6 120 BVerfGE 274, 302 (2008) (*Online Search*).

the rule of law in the context of data protection law. Regarding the topic of systematic government access to data, there are important constitutional decisions concerning strategic searches (1999), data mining (2006), and data retention (2010 and 2012).[7] In addition, two important decisions concern the protection of a 'core area of life formation'. These concern acoustic wiretaps within residences (2004) and preventive telecommunications surveillance (2005).[8]

The *G-10* Opinion (1999). The *Bundesnachrichtendienst*, or BND, and other German intelligence agencies are permitted to engage in the surveillance of letters, conversations, or telecommunications through two kinds of legal processes. First, the surveillance can take place as an 'individual investigation', which involves the collection of personal data to investigate criminal behaviour that threatens the survival of the German state or its democratic order.[9] Second, the surveillance can take place as 'strategic surveillance'.[10] Later in this paper, I will discuss the current statutory requirements regarding the terms for strategic surveillance for the BND and the other institutions that are part of the German intelligence community. In this section, I will examine the constitutional requirements before such activity can occur. These standards must then be reflected in the applicable statutory framework.

In the Constitutional Court's *G-10* opinion from 1999, the strategic surveillance in question involved observation of telegram, fax, and, to a lesser extent, telephone traffic transmitted via satellite.[11] The Constitutional Court also noted in this opinion that the government admitted during oral argument that the BND had plans for the surveillance of emails, but the Court did not provide further details about this activity. Today, such searches extend to emails as well as web fora.[12]

In its *G-10* opinion, the Constitutional Court found that the protections of the Basic Law's Article 10 were not limited exclusively to communications that took place entirely within the national borders of Germany. As long as enough of a nexus existed between the surveillance and German territory, the protections of Basic Law, Article 10 were applicable.[13] The Court identified such a nexus in the *G-10* case, where the government surveillance activity occurred within Germany and at least part of the communications ended or originated from within Germany.[14]

The Constitutional Court also found that the dangers of such surveillance were considerable.[15] Most importantly, it pointed to the risk that such surveillance would lead to 'a nervousness in communication, to disturbances in communication, and to behavioral accommodation, in particular to avoidance of certain content of conversations or terms.'[16] For the German Court, the threat was to social communication. In American terms, this idea is similar to that of a chilling impact on speech.

After noting the dangers posed by the data collected in the *G-10* case, the Constitutional Court nevertheless found the surveillance to have a strong justification. The activity to be placed under observation 'affected the foreign and security politics of the Federal Republic . . . to a significant extent'.[17] Moreover, the law permitted the collection of information necessary to detect dangers to Germany. As a result, the Constitutional Court declared that the statute was generally 'not improper'.[18]

The Constitutional Court did go on, however, to find several aspects of the statute to be unconstitutional.[19] Among the elements of the law that it struck down were certain provisions concerning the BND's transfer of personal data to other agencies. These transfers were only permissible when the controlling legislation met the principle of proportionality. As we will see later in this paper, judicial review pursuant to a proportionality analysis has developed as one of the Constitutional Court's most important tools when confronted with statutes that infringe upon privacy. In the *G-10* case, in a demonstration of this technique, the Constitutional Court decided the applicable statute did not limit these data transfers in a permissible fashion.

7 100 BVerfGE 313, (1999) (*G-10*); 115 BVerfGE 320, (2006) (*Data Screening*); 125 BVerfGE 260 (2010) (*Data Retention*); BVerfG, 1 BvR 1299/05 of Jan. 24, 2012 (*Telecommunications Databank*).

8 109 BVerfGE 279 (2004) (Great Eavesdropping); 113 BVerfGE 348 (2005) (Preventive Telecommunications Surveillance).

9 100 BVerfGE 313, 316 (1999) (*G-10*).

10 Id.

11 Id. at 380.

12 Unterrichtung durch das Parlamentarische Kontrollgremium, Deutsche Bundestag, 17. Wahlperiode, Drucksache 17/4278, p. 7 (2010).

13 100 BVerfGE 313, 363–64 (1999) (*G-10*).

14 Id.

15 Id. at 381.

16 Id.

17 Id. at 382.

18 Id. at 384–5.

19 For example, the statute's sect. 3(1) no. 5 permitted international surveillance for investigations of the counterfeiting of currency. The Constitutional Court found that the statutes allowing surveillance to prevent this crime did not follow the principle of 'proportionality.'"Id. at 385. It noted, however, that such surveillance would be constitutionally permissible if the strategic surveillance was limited to cases that threatened 'the stability of the value of the currency of Germany and thereby the economic power of the country'. Id.

To be sure, the Court found, as a general matter, that it was constitutional for the BND to share information gained from its surveillance of telecommunications traffic with other agencies to the extent that the data in question revealed criminal behaviour. The failing of the statute was, however, that it did not restrict data sharing to instances in which serious crimes had been committed, as opposed to more minor delicts. Such a lowered threshold did not meet the proportionality test. The Court also found that the statute allowed a sharing of information that the BND gathered in a manner that was too widespread. It demanded the enactment of new statutory standards for the BND and other intelligence agencies that restricted the transfer of information in a manner similar to limits placed on domestic law enforcement agencies when engaged in an 'individual investigation path'.[20]

These requirements do not present major obstacles to strategic searches, which are regulated in the G-10 Statute, sections 5–8. I will discuss this statute later in this paper; here, however, one might briefly consider the latest statistics concerning the use of this technique by the German intelligence services. According to the 2010 statistics from the Parliamentary Control Panel (*Parlamentarische Kontrollgremium*) regarding the use of applicable statutory authorities, the statutory justification regarding 'international terrorism' was relied upon by German intelligence agencies in searching 1.8 million examples of 'telecommunications traffic'. The official report explained that this number reflected a large percentage of spam, and resulted in the capturing of three faxes, one email, seven voice communications, and fifty-eight 'web fora observations' that were considered to be 'relevant to intelligence services'.[21]

The most frequent uses of these authorities were made, however, not in regard to terrorism, but to 'proliferation and conventional armaments'.[22] Such searches were made of 5.03 million examples of telecommunications traffic. Here, too, the Parliamentary Control Panel noted the existence of a high percentage of spam. The result was 209 instances of telecommunications traffic that were considered relevant to intelligence services. The official report provided no further breakdown of the nature of this traffic.

The *Data Screening* Opinion (2006). Data mining is an established technique of law enforcement authorities. Its use by law enforcement in Germany dates back to the 1970s and the country's struggle against the Red Army Faction (RAF). The German term for this practice is '*Rasterfahndung*', or a 'screening search'.[23]

In its *Data Screening* opinion of 2006, the German Constitutional Court found that data screening posed a significant infringement of the right of informational self-determination. In this opinion, the Court used its existing proportionality test as a constitutional yardstick for evaluating the permissibility of data screening. The *Data Screening* opinion involved a search carried out after the terrorist attacks in the USA on 9/11. The German data mining search was made in the hopes of discovering 'sleeper terrorists' in Germany.

The criminal police collected personal data from universities, the Registration Office for Inhabitants, and the Central Register for Foreigners. According to the Constitutional Court, the different police headquarters received 'data batches' with information on 5.2 million persons. The information collected at the state level was then transferred to the Federal Criminal Police Office (*Bundeskriminalamt*, or BKA), where it was incorporated into a federal database termed 'Sleepers'. The data screening was notably unsuccessful, and all the information in the 'results file' was erased by 2004.

In Germany, laws at the federal and state levels distinguish between the use of 'data screening' to (1) investigate past crimes, or (2) permit a preventive response to potential crimes. Data screening to investigate past crimes is regulated by various state laws and at the federal level by section 98a of the Criminal Procedural Code (*Strafprozeβordnung*).[24] The federal statute applies when the BKA takes a lead role in investigating crimes considered to be a federal matter. The Criminal Procedure Code's basic approach to investigations of past crimes also reflects the orientation taken by the different state laws, and our discussion here can, therefore, concentrate on the federal statute. In Section 98a, the Criminal Procedure Code regulates the 'automatic comparison and transfer of personal data'.[25] It requires 'sufficient factual indications to show that a criminal offense of significant importance has been

20 100 BVerfGE 313, 385–86 (1999) (*G-10*).

21 Unterrichtung durch das Parlamentarische Kontrollgremium, Drucksache 17/4278, p. 7 (2010).

22 Id.

23 In this discussion of the Data Screening opinion, I draw on my article, 'Regulating Governmental Data Mining in the United States and Germany', (2011) 53 William & Mary Law Review 351.

24 Strafprozeβordnung [StPO] [Criminal Procedure Code], Bundesgesetzblatt I. [BGBl. I.] 1074, 1319 (1987) (most recently amended by Law of 22 December 2011, BGBl. I., 3044), sect. 98a.

25 Id.

committed'.[26] Thus, this statute squarely requires proof of the existence of a crime.

In contrast to federal law in Germany, there are state statutes that permit a *preventive* use of data screening.[27] In 2006, the German Federal Constitutional Court established significant limits on such law enforcement use of this practice.[28] In its *Data Screening* opinion, the Constitutional Court found that the state's activity implicated the threat from modern means of surveillance to an individual's underlying communicative ability. It also acknowledged that individuals were obligated to accept limitations on their right of informational self-determination that were justified by weightier public interests. In its use of proportionality review in this opinion, the Constitutional Court found that data screening statutes are only constitutionally permissible when there was 'a concrete danger' to a legal interest.[29] Through this aspect of the *Data Screening* opinion, the Constitutional Court did more than invalidate the state law before it; it also raised significant questions about the majority of the other state laws that permitted preventive data searches.[30]

At the same time, however, the Constitutional Court did *not* declare data screening to be per se disproportionate and, hence, unconstitutional. Its decision was that law enforcement officials had to demonstrate the existence of a certain risk of danger before using this technique. Here was the significant limit placed on its preventative use. As the Constitutional Court stated, a concrete danger was 'a prognosis of probability' based on facts indicating that the predicted harm would occur. The Constitutional Court added, 'Vague clues or bare suppositions are not sufficient'.[31] Rather, data screening required proof of actual preparations for a terrorist attack. Such evidence showing a concrete danger would include, for example, 'factual clues for the preparation of terrorist attacks or the presence in Germany of persons who are preparing terrorist attacks that in the near future will be perpetrated in Germany or elsewhere'.[32]

The *Data Retention* Opinion (2010) and *Telecommunications Databank* Opinion (2012). Pursuant to its obligations under the European Union's Data Retention Directive, Germany enacted a data storage obligation in its Act for the New Regulation of Telecommunications Surveillance (*Gesetz zur Neuregelung der Telekommunikationsüberwachung*) on 21 December 2007. This statute amended the Telecommunications Act (Telekommunikationsgesetz or TKG).[33] On 11 March 2008, the Constitutional Court issued a temporary injunction that suspended certain parts of the statute. In 2010, the Court issued an opinion that struck down the statute. Despite much discussion of alternatives, the *Bundestag* has yet to enact a new data retention statute.

The German data retention statute required suppliers of telecommunication services to store specific kinds of traffic and location data for a period of six months. By choosing this term of a half year, the *Bundestag* opted for the minimum required retention period of the European Data Retention Directive. The newly drafted statutory provisions were inserted into the Telecommunications Act at TKG, sections 113a, 113b. The first provision, TKG, section 113a contained the obligation for a six-month retention period and specified the kinds of data that were to be stored. The second, TKG, section 113b set out the conditions under which law enforcement officials could gain access to the stored data.

In its 2010 opinion, the Constitutional Court found TKG, sections 113a, 113b unconstitutional and declared that the storage of telecommunications data, including traffic data, constituted a serious encroachment on individual rights. Even though the storage was not of content, it was still possible to use the data to make 'content-related conclusions that extend into the users' private sphere'.[34] The result might even permit the drawing of 'personality profiles of virtually all citizens'.[35] Nonetheless, the Constitutional Court also found that data retention could be made compatible with Article 10(1) of the Basic Law. Despite the potential dangers of data retention, access to information about telecommunications connections was of particular importance for 'effective criminal prosecutions and prevention of danger'.[36]

In the view of the Constitutional Court, however, the data retention statute had fatal flaws. To be constitutional, a law needed well-defined provisions for data security; limits on the use of data to investigations of

26 Id.

27 See, eg, Polizeigesetz des Landes Nordrhein-Westfalen [PolG NW] [North Rhine-Westphalia Police Statute], Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen [GV NRW] 410 (2003), sect. 31.

28 115 BVerfGE 320 (2006) (*Data Screening*).

29 Id. at 346.

30 Winfried Bausback, Fesseln für die wehrhafte Demokratie?, NJW 2006, p. 1922, 1924.

31 115 BVerfGE 346.

32 Id. at 365.

33 See the subsection entitled 'Statutory Law' for a discussion of statutory privacy law in Germany.

34 125 BVerfGE 260, 319 (2010) (*Data Retention*).

35 Id.

36 Id. at 323.

particularly serious crimes; sufficient transparency about its use for the public; and judicial control of the transmission and use of the stored data.[37] In addition, prohibitions were required on obtaining access to certain kinds of data, such as privileged communications with clergy or lawyers.[38] Interestingly enough, the Constitutional Court explicitly declared that dynamic IP addresses were subject to less stringent constitutional standards. Although the privacy of dynamic IP addresses did relate to whether anonymous communication could take place, such information could be made discoverable based on 'a sufficient initial suspicion or a concrete danger', or even for a significant regulatory offence, that is, a non-criminal matter.[39]

In a 2012 decision, the Constitutional Court built on its *Data Retention* opinion. The Court found TKG, section 111, which requires providers of telecommunication services to collect their customers' names, dates of birth, and other identifying information, to be consistent with the right of informational self-determination. It reasoned that 'these data neither cover highly personal information nor do they allow creation of personal or movement profiles'.[40] The 'limited informative value of the data' also proved a 'central reason' for the Constitutional Court to find TKG, section 112 permissible, which thus establishes an automated procedure for transmitting collected data to certain governmental agencies.[41]

At the same time, however, the Constitutional Court cautioned the legislature to keep up to date with technological developments and to amend the law with regard to IP addresses if necessary. It reasoned that if static IP addresses become a larger part of Internet communications, 'perhaps on the basis of Internet protocol version 6', communications would become 'de-anonymized on a long term basis'.[42] Because the government arguably could also demand these IP addresses, it could obtain much more information than is currently the case. Therefore, the legislature should monitor the developments and amend the underlying statutory authorities accordingly.[43]

Finally, the Constitutional Court upheld most elements in TKG, section 113, which provides for a manual procedure for transmitting certain types of data. It did so by interpreting this statute in a restrictive manner that would lead to adequate constitutional limits. As an example, the Court declared that TKG, section 113 did not permit access to dynamic IP addresses. Such a reading was necessary because 'the de-anonymization of dynamic IP addresses allows, to a large extent, the de-anonymization of communicative activities on the Internet'.[44] As to the problematic aspects of TKG, section 113, the Court found this statute's access authorization to personal identification numbers (PINs) and Personal Unblocking Key-Numbers (PUKs) objectionable. It found that this part of TKG, section 113 undermined specific, stricter requirements of other statutes.[45]

The *Great Eavesdropping* opinion (2004) and the *Preventive Telecommunications Surveillance* opinion (2005). In two important decisions, the Constitution Court has evaluated the nature of Basic Law, Article 13's protection of the home. These opinions followed amendments to the Basic Law in 1998 that explicitly permitted acoustic and visual surveillance of the home. Until then, there had been some open questions about the extent of Basic Law, Article 13's protection of the privacy of private residences. Article 13(1), which dates to the enactment of the Basic Law in 1949, states, 'The home is inviolable.'[46] Yet, the Basic Law's Article 13(2), also found in its original text, permits judges to order searches. The debate had been about whether surveillance was permissible within the home and whether such surveillance could occur in bedrooms and other areas associated with intimate activities.

The 1998 amendment to the Basic Law resolved only certain aspects of this debate. The constitutional amendment added new subsections to Article 13 of the Basic Law. Of these, the critical new section, Article 13(4), states, 'To avert acute dangers to public safety, especially dangers to life or to the public, technical means of surveillance of the home may be employed only pursuant to judicial order.'[47] Thus, the Basic Law after 1998 explicitly permits at least some surveillance within the home while also continuing to protect 'the inviolability of the home'. It would take a decision of the Constitutional Court to decide the extent to which such surveillance could occur consistent with the Basic Law.

37 See id. at 260–61.

38 See eg, [Criminal Procedure Code] [StPO] sect. 160a.

39 125 BVerfGE 260, 343 (2010) (*Data Retention*).

40 BVerfG, 1 BvR 1299/05 of Jan. 24, 2012, para. 139 (*Telecommunications Databank)*.

41 Id. at 159.

42 Id. at 161.

43 Id.

44 Id. at 172–4.

45 Id. at 184–5.

46 Basic Law, Article 13(1).

47 Id. at Article 13(4).

In its *Great Eavesdropping* opinion (2004), the German Constitutional Court upheld the 1998 amendments as constitutional.[48] The Basic Law did not provide absolute protection for the *space* of private residences. Rather, its absolute protection was provided to behaviour in this space that 'depicts individual development in the core domain of private life formation'.[49] Thus, in the view of the Constitutional Court, the constitution's need for the protection of physical spaces turned on how people use these areas. In particular, its ruling was that 'the greater the probability of capture of highly personal content, the stricter the requirements for lawfulness of surveillance of living quarters'.[50]

The Constitutional Court further elaborated the nature of these requirements in its *Preventive Telecommunications Surveillance* opinion (2005). It stated that preventative surveillance would be constitutionally acceptable only when 'there was an especially high ranking endangered legal interest and a designated situation with concrete stopping points and a connection through direct references to the future carrying out of a criminal offense.'[51] Second, it was sometimes not possible to know when a conversation might touch on the core domain of private life formation.[52] As a result of law enforcement not being able to predict the content of conversations in advance, the Constitutional Court required these officials to actively monitor their surveillance and to stop it immediately if the private domain of life formation was implicated. As an additional safeguard, there was a need for specific protection to guarantee that communications from the 'highly personal domain' would not be stored and subject to further use. As an example, should such material be collected, it was to be immediately erased.[53]

Statutory law

German privacy law regulates information privacy through an omnibus law, the BDSG,[54] and sectoral laws.[55] As a general matter, the BDSG controls this area when there is no specific sectoral statute that is applicable. For online telecommunications and other telecommunications, there is the added wrinkle of the legal organizational concept of the '*Schichtenmodel*', or 'Layer Model'.

The layer model functions through different legal requirements for content, services, and the technical level of transmission. As for the *content* of an online communication, it is regulated either by the BDSG, or any applicable legislation. As for *services* that are provided on the Internet, these are regulated by the *Telemediengesetz*, or Telemedia Law.[56] Concerning the *level* at which the transfer takes place, it is regulated by TKG.[57] As a further matter, the law uses a different range of statutory authorities to govern the access to communications by domestic law enforcement and intelligence agencies (see below).

Not surprisingly, it can be quite difficult to determine which statute applies to a given dimension of an online service, or communication. As German law professor Thomas Hoeren notes, 'Due to the acceleration of legislative activity in recent years, more and more special laws have been added to data protection law, without careful coordination of the application areas of the resulting statutes.'[58] Voice over Internet Protocol (VoIP) and other aspects of technical convergence have only added to the difficulty in maintaining the distinction, for legal purposes, among the layers.

Assessing statutory law regarding the government's systematic data access is, therefore, quite complex. As a basic matter, however, German data protection law represents a considerable hurdle to systematic data access. The use of and access to personal data generally requires a legal basis. German law expresses this concept as a '*Verbot mit Erlaubnisvorbehalt*', or a 'prohibition with conditional permission'. German law starts by forbidding the collection, processing, or use of

48 109 BVerfGE 279 (2004) (Great Eavesdropping).

49 Id. at 314.

50 Id. at 328.

51 113 BVerfGE 348, 392 (2005) (Preventive Telecommunications Surveillance).

52 Some information would fall on one side of the constitutional dividing line, some on the constitutionally-protected side. As an example of kind of information that could be collected without concern about the 'core domain of private life formation', the Court pointed to content that made 'direct reference to concrete criminal actions, such as statements about the planning of approaching criminal offenses, or reports about perpetrated criminal offenses.' Id. at 391.

53 Id. at 392.

54 Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Statute], Bundesgesetzblatt I. [BGBl. I.] 66 (2003) (most recently amended by Law of August 14, 2009, BGBl. I, 2814).

55 For example, there are special data protection provisions for prisoners. See Strafvollzugsgesetz [StVollzG] [Criminal Penalty Enforcement Statute], Bundesgesetzblatt I. [BGBl. I.] 581, 2088 (1976) (most recently amended by Law of 29 July 2009, BGBl. I., 2274), sects 179–187.

56 Telemediengesetz [TMG] [Telemedia Law], Bundesgesetzblatt I. [BGBl. I.] 179 (2007) (most recently amended by Law of 31 May 2010, BGBl. I, 692). For a discussion of the 'Layer Model', see Wissenschaftliche Dienste Deutscher Bundestag, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, 2011, 7 October, p. 10, available at: <https://www.datenschutzzentrum.de/facebook/material/WissDienst-BT-Facebook-ULD.pdf> accessed 27 August 2012.

57 Telekommunikationsgesetz [TKG] [Telecommunications Act], Bundesgesetzblatt I [BGBl. I] 1190 (2004) (most recently amended by Law of 22 December 2011, BGBl. I, 2958).

58 Thomas Hoeren, Wenn Sterne kollabieren, entsteht ein schwarzes Loch—Gedanken zum Ende des Datenschutzes. 1 ZD 145–46 (2011).

personal data. This prohibition is lifted, however, once a statute authorizes the data collection, processing, or use in question. This statute must, of course, also fulfil the proportionality requirement of German law.

Under the BDSG, moreover, data can be processed, shared and transferred only under a limited set of circumstances. BDSG, section 14(1) provides one of the most important of these restrictions. It limits the 'storage, alteration, or use of personal data' by private bodies to circumstances when it is '*necessary* to carry out the tasks for which the controller is responsible and for *the purpose for which the data were collected*' (emphasis added). Thus, this passage sets a standard of necessity as well as a requirement of 'original purpose specification'. BDSG, section 15(1) places similar kinds of restrictions on data transfers to public bodies.

Separate laws existing for law enforcement access, regulatory access, and/or national security access (including a distinction if any between domestic intelligence and foreign intelligence)

Basic organizational concepts and the 'Anti-Terror Database'

As in US law, German law distinguishes between law enforcement and intelligence agencies. The two countries also share a distinction between domestic intelligence and foreign intelligence agencies. Law enforcement agencies are generally tasked with enforcing the criminal code and policing violations of it. Intelligence agencies gather and analyse information that is needed to protect national security.

The BND is the German agency for foreign intelligence. Unlike the United States, where the Federal Bureau of Investigation has both a law enforcement and a domestic intelligence role, Germany has an agency that is exclusively dedicated to domestic intelligence: the *Bundesamt für Verfassungsschutz*, or Federal Office for the Protection of the Constitution. This agency combats threats against the democratic order of Germany; it also has counterparts in each German state. The federal and state offices for the protection of the constitution have traditionally lacked police powers, such as the ability to perform arrests. Finally, the federal investigative police authority is the Federal Criminal Police Office, the BKA.[59]

The development of the federal police service, the BKA, and its role in Germany have long been controversial issues. The negative example of the Gestapo, the centrally organized police force of the Nazis, casts a long shadow. In addition, East Germany's *Ministerium für Staatssicherheit*, or Stasi, provided a later negative example from German history of a centrally organized agency for domestic security. Another factor in the debate about the proper role of a federal police force has been the desire of the German states to keep their own independent authorities for policing and gathering intelligence.

As a result of these factors, since the end of World War II and the creation of the Federal Republic of Germany, a fundamental legal concept has been the '*Trennungsgebot*', or 'Separation Rule'. The *Trennungsgebot* expresses a legal norm for organizational and informational divisions between intelligence and law enforcement agencies. For example, this legal concept would prevent the creation of a single German agency with borderless law enforcement and intelligence capacities, or the limitless sharing of information between law enforcement agencies and intelligence agencies. The rough analogy would be with the concept of 'the wall' in US regulation of the intelligence community. This concept views at least some limits on information sharing between intelligence agencies and law enforcement organizations as necessary for the protection of civil liberties.

Nonetheless, a total ban is not intended on law enforcement agencies and intelligence agencies working together and sharing information. A significant development in Germany since 9/11, and, indeed, since the end of the Cold War, has been a steady stream of legislation that expands the powers of the BKA, BND, Federal Office for the Protection of the Constitution, as well as related agencies, and an increase in their ability to work together and to share information.

One of the best examples of this trend is provided by the creation of an '*Antiterrordatei*', or 'Anti-Terror Database'. Through enactment of federal legislation in 2006, Germany established this databank, which is a common data source with an extended index. The information in the Anti-Terror Database is collected from 38 different security authorities and concerns approximately 18,000 individuals considered to require scrutiny.[60] While a number of different agencies can search the databank,

59 An important organizational distinction can be made with the USA, where the Federal Bureau of Investigation (FBI) has traditionally functioned as both the federal police authority, like Germany's BKA, and as a domestic intelligence agency, such as Germany's Federal Office for the Protection of the Constitution.

60 Drucksache 17/6233, Deutscher Bundestag, 17. Wahlperiode 8 (2011), available at: <http://dipbt.bundestag.de/dip21/btd/17/062/1706223.pdf> accessed 27 August 2012.

and do so electronically, the databank is constructed to distinguish information in 'open' and 'concealed storage'.

If information in the databank is in open storage, a match to a suspect's name will reveal information about him. If information is in concealed storage, the inquiring agency will receive a negative result to its search for data about a person. At the same time, however, the agency that has stored the information in concealed storage will receive data about the inquiry. It is then up to the storing agency to decide whether the applicable legal rules permit it to share further information with the inquiring agency. In 2006, a German civil liberties organization awarded a 'Big Brother Award' to the Conference of Interior Ministers for their role in establishing the Anti-Terror Database.[61]

Intelligence agencies

Strategic surveillance: the basic structure. As noted above, German constitutional law permits the BND to engage in so-called strategic surveillance. Subsequent to the Constitutional Court's *G-10* decision, the *Bundestag*, the Federal Parliament, amended the applicable statutory authorities to make the law conform with the Basic Law. In 2009, the *Bundestag* again amended the relevant statute, the '*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*', or, less formally, the 'G-10 Statute', to provide additional surveillance powers to the BND.[62] In addition, as noted above, federal and state intelligence agencies, as well as police authorities, can also gain access to electronic data in the Anti-Terror Database.

The G-10 Statute is, however, the main statute regulating the BND's access to letters and telecommunications. This law's sections 5–8 contain the provisions applicable to strategic surveillance. G-10 Statute, section 5(1) lists the nature of the dangers that justify the use of strategic surveillance. These include the risk of: an armed attack on Germany; the committing of international terrorist attacks with a direct relation to Germany; international trafficking in weapons of war; drug trafficking; or a limited set of other significant dangers. The statute also sets obligations for the BND to check whether the collected personal data are 'necessary' for one of the purposes of statutory purposes set out in the G-10 Statute, section 5(1). If not, such data are to be immediately erased.

Following the enactment of statutory amendments in 2009, the G-10 Statute contains a specific section that protects a 'core area of private life formation' in the context of both individual surveillance and preventive surveillance. The 2009 amendments to the G-10 Statute reflect the constitutional safeguards that the Constitutional Court identified in its *Great Eavesdropping* opinion (2004) and *Preventive Telecommunications Surveillance* opinion (2005), discussed above. In particular, G-10 Statute, section 5a contains an absolute prohibition on the capture of communications from the core area of private life formation.[63] Should such information, nonetheless, be collected, authorities may not use them and these data are to be erased at once.[64] A protocol of the erasure is to be maintained for purposes of 'the oversight of data protection'.[65] Finally, strategic surveillance may not use 'search terms' (*Suchbegriffe*) that contain 'identifying features' that (1) will lead to a 'targeted acquisition of determined telecommunication connections', or (2) that 'concern the core area of private life'.[66]

The G-10 Statute also contains mechanisms for the oversight of intelligence agencies. It establishes a Parliamentary Control Panel, already mentioned above, as well as the G-10 Commission. Most importantly, the G-10 Commission, like the FISA court in the USA, has a central role in deciding on the permissibility of surveillance by intelligence agencies. To begin, however, with the Parliamentary Control Panel, it consists of members of the *Bundestag*, the German Parliament. The government (*Bundesregierung*) is required by law to 'inform the Parliamentary Control Panel extensively' about 'general activities' of the intelligence agencies and about 'events of particular importance'.[67] The Parliamentary Control Panel may also request files and other papers from intelligence agencies. It publishes an annual report about its oversight activities, which includes highly useful statistics about the use by intelligence agencies of surveillance powers. A 2009 law heightened the Parliamentary Control Panel's constitutional status and its powers to gather information from the government and intelligence agencies.[68]

61 Big Brother Awards, Politics II: Interior Ministers, available at: <http://www.bigbrotherawards.de/2006/.pol/pol-02> accessed 27 August 2012.

62 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz [G-10] [G-10 Statute], Bundesgesetzblatt I. [BGBl. I] 1254, 2298 (2001) (most recently amended by Law of 7 December 2011, BGBl. I, 2576), sect. 5a.

63 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz [G-10] [G-10 Statute], Bundesgesetzblatt I. [BGBl. I] 1254, 2298 (2001) (most recently amended by Law of 7 December 2011, BGBl. I, 2576), sect. 5a.

64 Id.

65 Id.

66 Id. at sect. 5(2).

67 Kontrollgremiumgesetz vom 29.Juli 2009 (BGBI. I S. 2346), sect. 4(1).

68 Bertold Huber, Die Reform der parlamentarischen Kontrolle der Nachrichtendienste und des Gesetzes nach Art. 10 GG, 28 NVwZ 1321 (2009).

As for the G-10 Commission, the Parliamentary Control Panel names the members of the G-10 Commission, which is a non-judicial entity. In turn, the G-10 Commission decides on the 'permissibility and necessity' of surveillance carried out by intelligence agencies pursuant to the G-10 Statute.[69] As the Parliamentary Control Panel explains, 'the supervisory power of the Commission extends to the entire collection, processing and use of personal data by federal intelligence agencies pursuant to the G-10 Statute.'[70]

The role of telecommunication providers. TKG, sections 110–113 provides particularly important statutory examples of systematic data access. In a recent decision, discussed above, the Constitutional Court largely upheld TKG, sections 111–113 as constitutional.[71] These sections require that telecommunication providers collect certain data about their customers, such as name, address, and telephone number, before the service is established. This information is termed '*Bestandsdaten*', or 'inventory information', and is sent to an automated databank of the *Bundesnetzagentur*, or Federal Network Agency. Pursuant to TKG, section 112, governmental agencies can make automated requests for this information from the databank. The legal standard for justifying such access to 'inventory information' is quite low. Law enforcement and intelligence officials can request the information when it is required for discharge of their 'legal functions'. Already in 2003, I had observed about the previous statutory provision creating this process for access to inventory information: 'In Germany, it is quite easy to obtain "inventory information". Law enforcement officials can request it when required for discharge of "their legal functions", and judicial review of this request does not occur.'[72]

Domestic law enforcement agencies

In StPO, section 100g(2), the Code of Criminal Procedure provides important legal authorities for systematic data access.[73] It allows law enforcement agencies to gain information about 'a sufficiently specific spatial and temporal description of telecommunications' in cases of a serious criminal offence, and when the investigation of the matter would otherwise be made significantly more difficult. Under this authority, the police in Berlin, Dresden, and many other locations have made massive requests for cell tower data about any person located in a given area during a specific time period. Thus, a Berlin newspaper, the *taz*, reported in 2012 that the Berlin police since 2008 had made 410 '*Funkzellenanfragen*', or 'Radio cell inquiries' and, thereby, collected information pertaining to 4.2 *million* cell phone connections.[74] These requests had been made to combat an epidemic of vandals setting automobiles on fire. In 2011, the same newspaper revealed that the police had gathered similar kinds of information after an anti-Nazi protest in Dresden. It quoted an attorney who called this action 'the equivalent of data mining through the cell phone'.[75]

Laws requiring broad reporting of personal data (passenger records, financial data) by private-sector entities and if applicable how these laws address systematic access

The data reporting requirements for private-sector entities are mainly based on their business activities. For example, they have to report certain business transactions with entities in sensitive countries[76] as well as the hiring of employees.[77] In addition, German law requires private individuals to notify governmental entities of certain events, such as the move to a new residence or the change in ownership of a vehicle. With regard to the former, a new '*Bundesmeldegesetz*', or 'Federal Residence Reporting Act' is to be enacted by November 2014.

While residence reporting has traditionally left to the state legislature to regulate, the new *Bundesmeldegesetz* will be a federal law that centralizes the reporting function. While the Federal Parliament has enacted a bill, it has not yet received the approval of the *Bundesrat*, or Federal Council. Such approval is required because the law touches upon the states' interests.[78] The bill contains a controversial provision that allows the government to disclose the names and street addresses of

69 G-10 Statute, sect. 15(5).

70 Unterrichtung durch das Parlamentarische Kontrollgremium, Drucksache 17/4278, p. 3.

71 BVerfG, 1 BvR 1299/05 of 24 January 2012.

72 Paul M. Schwartz, 'German and U.S. Telecommunications Privacy Law', (2003) 54 Hastings L. J. 751, 781.

73 In its *Data Retention* decision, which is discussed above, the German Constitutional Court found Code of Criminal Procedure, sect. 100g(1) unconstitutional as far as it allows data collection under TKG, sect. 113a.

74 Konrad Litschko, Polizei sammelte Handydaten, taz, (23 January 2012), available at: <http://www.taz.de/Autobrandstiftung-in-Berlin/!86239/> accessed 27 August 2012.

75 Paul Wrusch, Mal eben ausgespäht, taz, (19 June 2011), available at: <http://taz.de/Demo-berwachung-per-Mobilfunk/!72708/> accessed 27 August 2012.

76 Außenwirtschaftsgesetz [Foreign Trade Act], Bundesgesetzblatt I. [BGBl. I] 1150 (2009) (most recently amended by Regulation of 15 December 2011, BAnz. 2011, 4653).

77 Sozialgesetzbuch, Viertes Buch [SGB IV] [Code of Social Law, Book IV], Bundesgesetzblatt I. [BGBl. I] 3845 (1976) (most recently amended by Law of 12 April 2012 (BGBl. I, 579).

78 Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens [MeldFortG] [Bill for an Act of the Development of Residence Reporting], BT-DS 17/7746, 16 November 2011.

individuals to private entities if the individuals have not objected.[79] The reliance on an opt-out solution has been controversial, and observers have objected to the removal of an opt-in solution from an earlier version of the bill.[80] The final statutory form of the *Bundesmeldegesetz* is as yet uncertain.

Another recent controversy concerning systematic data access involved the federal government's stopping of the ELENA project, which was a planned databank of employee data. ELENA stands for *Elektronisches Entgeltnachweis-Verfahren*, or Electronic Payment Verification Process, and had its basis in a statute enacted in March 2009.[81] It was intended to allow German companies significant savings in human resource departments by streamlining the collection of a wide variety of employee data. A government agency was to run the resulting centralized databank of information, which consisted of name, data of birth, insurance number, home address, time missing work, and 'possible misbehavior'. The resulting information was to be shared for the purposes of unemployment insurance, housing benefits, parental benefits, and other kinds of social insurance. According to the *Spiegel* magazine, ELENA, was to be 'the largest official collection of data in Germany'.[82]

In July 2011, the German government abandoned the ELENA project. The project failed because of the lack of an adequate electronic signature for use within the ELENA process and a series of contested data protection issues. In addition, local political authorities and small and medium-sized businesses, an economic sector termed the '*Mittelstand*', had complained about their costs related to the project.

Laws permitting or restricting private-sector entities from providing government officials with voluntary broad access to data, whether pursuant to a former order or as a result of more informal or cooperative agreements

As noted above, the German constitutional law of information privacy permits a private- or public-sector entity to collect, process, and transfer personal information subject to only a limited set of conditions. As a fundamental matter, there must be a statutory basis for this informational activity. As a result, informal or cooperative agreements are permissible under German law only if they comport with statutory requirements.

Role of the courts

As the discussion of constitutional law above has already indicated, German courts have a central role interpreting the relevant legal norms when personal information is processed, collected, and transferred.

Standards for use, access, retention, and/or destruction by government

Following the Constitutional Court's decision in 2010 voiding the data retention statute, the *Bundestag* has been unable to enact a new law. One proposal has been to replace mass data retention with a 'Quick Freeze' process.[83] Under it, law enforcement and intelligence agencies would obtain an order for data preservation relating to a subject under suspicion. If a crime was, in fact, committed, there would then be a 'thawing' of the data, that is, access provided to it, to aid in the prosecution of the party. Due to the lack of a German data retention law, the European Commission brought court proceedings in 2012 against Germany at the European Court of Justice. The action was based on the failure of Germany to implement the European Union's Data Retention Directive.[84]

As another example of the controversy around this topic, the Max Planck Institute for Foreign and International Criminal Law published an expert opinion in January 2012 finding an absence of any negative impact on the solving of crimes due to the lack of stored data since 2010.[85] The Justice Ministry had authorized this report and welcomed it as proof that data storage was unnecessary.[86] In contrast, the Interior Ministry and

79 Id. at sect. 44.

80 See, eg, Bundesregierung hofft auf Hilfe des Bundesrates gegen den Bundestag, FAZ (9 July 2012), available at <http://www.faz.net/aktuell/politik/inland/kritik-an-meldegesetz-bundesregierung-hofft-auf-hilfe-des-bundesrates-gegen-den-bundestag-11814730.html> accessed 27 August 2012.

81 'Das Ende von ELENA: Arbeitnehmer-Datenbank wird "schnellstmöglich" eingestellt', *MMR-Aktuell* 321105 (2011).

82 'Abschied von "Elena": Regierung stoppt umstrittene Arbeitnehmer-Datenbank', *Spiegel* (18 July 2011), available at: <http://www.spiegel.de/netzwelt/netzpolitik/0,1518,775145,00.html> accessed 27 August 2012.

83 Quick Freeze/Datensicherung, Bundesministerium der Justiz, available at: <http://www.bmj.de/DE/Buerger/digitaleWelt/QuickFreeze/quickfreeze_node.html> accessed 27 August 2012.

84 Data retention: Commission takes Germany to Court requesting that fines be imposed (31 May 2012), available at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/530&format=HTML&aged=0&language=EN&guiLanguage=en> accessed 27 August 2012.

85 Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung, p. 219, available at: <http://vds.brauchts.net/MPI_VDS_Studie.pdf> accessed 27 August 2012.

86 Studie bestreitet Sinn von Vorratsdatenspeicherung, focus (27 January 2012), available at: <http://www.focus.de/politik/deutschland/aufklaerungsquote-nicht-beeinflusst-studie-bestreitet-sinn-von-vorratsdatenspeicherung_aid_707398.html> accessed 27 August 2012.

the BKA criticized the methodology of the expert opinion.[87]

Cross-border and multi-jurisdictional issues (eg, under what circumstances does the government assert jurisdiction over data stored outside its borders)

In its *G-10* opinion, the Constitutional Court found that the protections of the Basic Law's Article 10 were not limited exclusively to communications that took place only within the national borders of Germany. As long as enough of a nexus existed between the surveillance and German territory, the protections of Basic Law, Article 10 were applicable.[88]

Recent controversies

Three current controversies have already been discussed, namely the enactment of a Federal Residence Reporting Act, the abandonment of the ELENA databank of employment data, and the ongoing debate about data retention. An additional controversy concerns the proposal for a German 'Federal Cloud', termed the '*Bundes-Cloud*'.

There has been considerable discussion in Germany about privacy and security issues relating to data processing in the cloud. In the judgment of the Federal Data Protection Commissioner, for example, cloud computing represents a form of '*Auftragsdatenverarbeitung*', or 'contract data processing'.[89] Such activity requires that the party carrying out processing in the cloud 'comply with technical and organizational measures to ensure privacy'.[90]

The discussion has also evaluated the potential for US government access to German data stored in this fashion. An initial window into these attitudes about the cloud was provided by the introduction of Microsoft's Office 365 in Germany. In response to a question, a Microsoft executive discussed the obligation of his company to share data from European data centres with US officials if requested pursuant to appropriate legal authorities.[91] According to an analysis in a German law review, however, such a transfer, even if pursuant to statutory authorities in the USA, would violate the Federal Data Protection Law of Germany.[92] The author of the article, Benno Barnitzke, observes that 'a transfer to U.S. authorities is not covered by an authorization in the German federal data protection statute (BDSG)'.[93] As a consequence, 'the release represents an improper and illegal data processing in the sense of the BDSG'. Moreover, BDSG, section 43 would provide sanctions against it.[94]

Another window into German attitudes about cloud services and storage is offered by a White Paper from the Conference of Federal and State Data Protection Commissioners of Germany. This document raises concerns regarding the lack of transparency for individuals regarding data processing in the cloud.[95] In reference to non-EU nations, or so-called 'Third Countries', the White Paper warns that 'when a public cloud is used in Third Countries, access to the data of the company using the cloud is possible and cannot be controlled'.[96] Finally, a law review article in Germany has warned, 'The solution to this problem should certainly not be that European clouds are moved to the United States, where they would be subject to the provisions of the Safe Harbor Program and the standard contractual clauses and, accordingly, lawfully subject to the access of U.S. authorities.'[97]

In response to German concerns about the clouds run by US companies, the Minister of the Interior, Hans-Peter Friedrich, has called for the development of a *Bundes-Cloud*, or Federal Cloud. The *Bundes-Cloud* is intended to keep 'sensitive governmental and enterprise data from landing with U.S. officials'.[98] The Minister of the Interior has already begun talks about the creation of such a German cloud with Deutsche Telekom and the *Bundesamt für Sicherheit in der Informationstechnik*, or Federal Office for Information Security. Information in the *Bundes-Cloud* in Germany would, however, be accessible to German police and intelligence agencies pursuant to the applicable constitution and statutory provisions. The current discussion in Germany about the *Bundes-Cloud* does not appear concerned, however,

87 Vorratsdatenspeicherung: Friedrich stellt Studie infrage, focus (27 January 2012), available at: <http://www.focus.de/politik/deutschland/vorratsdatenspeicherung-friedrich-stellt-studie-infrage_aid_707678.html> accessed 27 August 2012.

88 100 BVerfGE 313, 363–64 (1999) (*G-10*).

89 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Tätigkeitsbereicht 2009 und 2010, Drucksache 17/5200, pp. 63–4.

90 Id.

91 Benno Barnitzke, 'Microsoft: Zugriff auf personenbezogene Daten in EU-Cloud auf Grund US Patriot Act möglich', *MMR-Aktuell* 3211103 (2011).

92 Id.

93 Id.

94 Id.

95 Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientungshilfe—Cloud Computing p. 16 (26 September 2011).

96 Id.

97 Christian Schröder and Nils Christian Haag, 'Neue Anforderungen an Cloud Computing für die Praxis', (2011) 1 ZD 147, 150 .

98 Jürgen Berke, 'Innenminister Friedrich will Bundes-Cloud aufbauen', *Wirtschaftswoche* (20 January 2012).

about such access; perhaps this absence of a debate about German statutory authorities in this context indicates a general level of satisfaction with these underlying regulations.

Concluding observations

This paper will conclude by pointing out a seeming irony: the current Interior Minister, Hans-Peter Friedrich, has offered both strong advocacy of a new data retention law for Germany and proposed the creation of a *Bundes-Cloud* to protect German personal data from the US government. The irony is that Minister Friedrich desires data retention by German companies to expand the German government's access to certain kinds of information for security and law enforcement purposes, but opposes clouds run by American companies. The existence of such clouds might permit the US government to access data for similar purposes. If one were to speculate, behind the seeming contradiction may be a distrust of the privacy standards of US privacy law. Friedrich's positive views on data retention are not shared, however, even by all members of the current government coalition; the Justice Minister, Sabine Leutheusser-Schnarrenberger, has been highly critical of the desirability and, indeed, the extent of any underlying need for a law mandating data retention. At the same time, many German officials and experts can be considered sceptical of the standards of US information privacy law and, as a result, concerned about systematic data access on the other side of the Atlantic.

doi:10.1093/idpl/ips026
Advance Access Publication 11 September 2012