National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

GERMANY

Version of 23 September 2014

Deutsches Institut für Menschenrechte
Eric Töpfer

Introduction[1]

> (1) The privacy of correspondence, posts and telecommunications shall be inviolable.
>
> (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.
>
> *(Article 10 of the German Basic Law)*[2]

1. The institutional and legal landscape of telecommunications surveillance by German state agencies is vast (see table 1). More than three dozen security authorities are warranted to intercept and collect data related to telecommunications, i.e. 16 police forces of the *Länder*, the Federal Criminal Police Office (*Bundeskriminalamt*), the Federal Police (*Bundespolizei*), the Customs Criminal Investigation Office (*Zollkriminalamt*), and the intelligence services, namely the domestic secret service also known as *Verfassungsschutz*, which is in fact a network of one federal office (*Bundesamt für Verfassungsschutz*) and 16 state offices serving the "protection of the constitution" in the domain of the 17 ministries of the interior, the Military Counter-Intelligence Service (*Militärischer Abschirmdienst*) in the domain of the Federal Ministry of Defence, and – with a staff of more than 6,000 the largest one – the Federal Intelligence Service (*Bundesnachrichtendienst*) in the domain of the Federal Chancellery (*Bundeskanzleramt*).

2. According to the specific tasks of these authorities, legislation differentiates between surveillance for purposes of criminal investigation, for averting dangers and for the collection of intelligence. Moreover, it is differentiated between the collection of content data (e.g. phone calls or email communication), traffic data also known as "metadata" (e.g. internet protocol address or telephone numbers, date and time of communication), inventory data (e.g. name and address of subscriber), the operation of IMSI Catchers, and the bugging of computers to bypass encryption of communications, known as *Quellen-Telekommunikationsüberwachung*. In sum, the legal framework for the surveillance of telecommunication by German security agencies comprises numerous individual provisions in more than 30 laws of the Federation and the *Länder* that regulate the tasks and warrants of the security agencies and the obligations of service providers. In addition, data protection acts and other legislation of the Federation and the *Länder* provide for control and oversight, citizens' rights, and authorities' duties to report on the extent of selected areas of telecommunications surveillance.

3. However, as the focus of the FRA's ad hoc request is on "mass surveillance" by national intelligence authorities, the key piece of legislation is the Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*),[3] also known as Article 10 Act (*G 10*) regulating wiretapping and telecommunications surveillance by the

[1] Acknowledgement: The author wishes to thank Franziska Weißenberger who supported the research for this report. Any mistakes are, however, in his own responsibility.

[2] Germany, Basic Law (*Grundgesetz*), English version available at: http://www.gesetze-im-internet.de/englisch_gg/

[3] Germany, the Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), 26 June 2001, last amended at 6 June 2013, available at: http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html.

German intelligence agencies. The act was passed in 1968 and amended many times since then. The G 10 regulates both surveillance that targets selected individuals or organisations, as most other provisions on German telecommunication surveillance do, and actual indiscriminate mass surveillance, the so-called "strategic" interception of international communication to and from Germany which is the exclusive domain of the Federal Intelligence Service (*Bundesnachrichtendienst* – BND). In addition, the BND is – to an even greater extent – intercepting communications in or between foreign countries in the context of its "open sky" surveillance.

Table 1: Federal regulation of telecommunications surveillance in Germany[4]

	Criminal investigation	**Averting dangers / Prevention**	**Intelligence**	**Service provider obligations**
General provisions				§ 2 G10 § 114 TKG
Content data	§§ 100a StPO	§ 20l BKAG § 23a ZfDG	G 10	§ 110 TKG
Metadata **(§ 96 TKG)**	§ 100g StPO	§ 20m BKAG § 23g ZfDG	§ 8a (2) BVerfSchG § 2a BNDG § 4a MADG	*§§ 113a, 113b TKG implementing the EU Data Retention Directive by committing service providers to store metadata for six months were declared null and void by the Federal Constitutional Court in 2010. Hence, the only obligations that exists, is the obligation of § 96 TKG to delete metadata immediately after the termination of a telecommunication, unless clients have agreed to longer retention periods.*
Inventory data **(§§ 95 TKG, 14 TMG)**	§ 100j StPO §§ 7 BKAG	§ 22a BPolG	§§ 8a (1), 8d BVerfSchG	§§ 111, 112, 113 TKG

[4] On 19 August 2014 the Federal Ministry of the Interior presented a draft bill on IT security which aims among others to amend Section 15 of the Telemedia Act and Section 100 of the Telecommunications Act in order to authorize providers of telemedia and telecommunication services to collect and use metadata for the purposes of detection, limitation and elimination of malfunctions. As service providers shall also inform the Federal Network Agency (*Bundesnetzagentur*) immediately in case of cyber-attacks, critics fear a revival of data retention through the backdoor. However, the draft bill does neither provide for any mandatory retention of metadata nor would the domestic intelligence service be directly involved: According to the bill, the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) – which should be informed by the Federal Network Agency in severe cases of cyber incidents – should collaborate with "competent federal authorities", including the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*), on critical infrastructure protection and joint situation awareness by sharing relevant information. Sources: Germany, Federal Ministry of the Interior (*Bundesministerium des Innern*), Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, 18 August 2014. Spiegel Online (2014), 'IT Sicherheitsgesetz. Datenschützer fürchten Vorratsspeicherung durch die Hintertür', 22 August 2014, available at: http://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-datenschuetzer-kritisieren-plan-von-de-maiziere-a-987582.html.

	§§ 7 (5), 15 ZfDG	§§ 7, 20b, 22 BKAG §§ 7 (5), 15 ZfDG	§§ 2a, 2b BNDG §§ 4a, 4b MADG	§ 14 TMG
IMSI Catcher	§ 100i StPO	§ 20n BKAG	§ 9 (4) BVerfSchG	
Bugging computers to bypass encryption (*Quellen-Telekommunikationsüberwachung*)	Currently not in use, legal basis controversial	§ 20l (2) BKAG	-	-

BKAG = Bundeskriminalamtgesetz (Federal Criminal Police Office Act)[5]
BNDG = Bundesnachrichtendienstgesetz (Federal Intelligence Service Act)[6]
BPolG = Bundespolizeigesetz (Federal Police Act)[7]
BVerfSchG = Bundesverfassungsschutzgesetz (Federal Act on the Protection of the Constitution)[8]
G 10 = Artikel 10-Gesetz (Article 10 Act)[9]
MADG = MAD-Gesetz (Military Shield Service Act)[10]
StPO = Strafprozessordnung (Code of Criminal Procedure)[11]
TKG = Telekommunikationsgesetz (Telecommunications Act)[12]
TMG = Telemediengesetz (Telemedia Act)[13]
ZfDG = Zollfahndungsdienstgesetz (Customs Investigation Service Act)[14]

The Article 10 Act and BND strategic surveillance

4. Until the end of the Cold War strategic surveillance of international radio communications under the G 10 was limited to the purpose of pre-empting military attacks against the Federal Republic of Germany. After the fall of the wall the scope of BND strategic surveillance was expanded. In 1994 the Combating Crime Act (*Verbrechensbekämpfungsgesetz*)[15] amended the G 10 significantly and warranted mass surveillance also for purposes of pre-empting international terrorism, arms proliferation and organised crime such as drug trafficking or money laundering, and authorised the transfer of obtained information to other German security authorities. Several provisions of these amendments were found to be incompatible with the German Basic Law (*Grundgesetz*) by the Federal Constitutional Court (*Bundesverfassungsgericht*) in 1999.[16] Hence, a major revision of the G 10 was passed in 2001 that satisfied the verdict of the court on the one hand but also expanded the surveillance powers of the BND on the other hand. Since then strategic surveillance can also be ordered in cases of oversea

[5] Germany, Federal Criminal Police Office (*Bundeskriminalamtgesetz*), 7 July 1997, last amended 20 June 2013, available at: http://www.gesetze-im-internet.de/bkag_1997/BJNR165010997.html.
[6] Germany, Federal Intelligence Service Act (*Bundesnachrichtendienstgesetz*), 20 December 1990, last amended 20 June 2013, available at: http://www.gesetze-im-internet.de/bndg/BJNR029790990.html.
[7] Germany, Federal Police Act (*Bundespolizeigesetz*), 19 October 1994, last amended at 20 June 2013, available at: http://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html.
[8] Germany, Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*), 20 December 1990, last amended at 20 June 2013, available at: http://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html.
[9] See footnote 2.
[10] Germany, Military Shield Service Act (*Gesetz über den Militärischen Abschirmdienst*), 20 December 1990, last amended at 20 June 2013, available at: http://www.gesetze-im-internet.de/madg/BJNR029770990.html.
[11] Germany, Code of Criminal Procedure (*Strafprozessordnung*), 12 September 1950, last amended at 23 April 2014, available at: http://www.gesetze-im-internet.de/stpo/BJNR006290950.html.
[12] Germany, Telecommunications Act (*Telekommunikationsgesetz*), 22 June 2004, last amended at 25 July 2014, available at: http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html.
[13] Germany, Telemedia Act (*Telemediengesetz*), 26 February 2007, last amended at 31 May 2010, available at: http://www.gesetze-im-internet.de/tmg/BJNR017910007.html.
[14] Germany, Customs Investigation Service Act (*Zollfahndungsdienstgesetz*), 16 August 2002, last amended 20 June 2013, http://www.gesetze-im-internet.de/zfdg/BJNR320210002.html.
[15] Germany, Combating Crime Act (*Verbrechensbekämpfungsgesetz*), 28 October 1994.
[16] Germany, Federal Constitional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999. See Annex 4.

hostage-takings of Germans or other threats for the life and limb of persons abroad that significantly touch German interests. Moreover, the interception of 20 per cent of the information flow of selected routes of "bundled transmissions", namely telecommunications cables, satellite transmissions and microwave radio relay, was authorised for all purposes of surveillance.

5. The flow of information may be automatically filtered by using search terms which can be of substantial (search words) or formal nature (telephone numbers or email addresses). Formal search terms should, however, not include connections in Germany or of Germans abroad. Therefore, today personal data can be easily collected by targeting telecommunication connection of foreigners, whereas the interception of radio communications in the early days of the G 10 did not allow such targeted surveillance. In a second step, the obtained information is then searched for "relevant" information which can be done also by automated means, also using German telephone numbers and other connections that are suspected to be related to the above listed risks. All information that is not selected as relevant has to be deleted immediately. In the recent years, millions of individual communications were thus filtered in the first step of dragnet search, with a peak of 37 million communications in 2010. By focusing on formal search terms, i.e. phone numbers, email addresses etc. these numbers were reportedly reduced most recently: In 2012, around 850,000 communications were caught by the dragnet search, most of it in the area of arms proliferation, and 288 of these communications were singled out as relevant in the second step of the filtering process.[17]

6. Such "relevant" data have to be tagged as being obtained by restrictions of communications privacy. Their relevance has to be assessed by the Federal Intelligence Service once in six months; if not of interest any more they have to be deleted under supervision of a staff member who is a fully qualified lawyer. Deletions have to be logfiled, and the logfiles need to be stored for one year for purposes of oversight and control. Relevant data can be transferred under specified conditions and for limited purposes to the Federal Government, other German security authorities, and foreign intelligence services. Receivers of information have to keep the data tagged as being obtained by G 10 surveillance and must not use the data for other purposes than those for which they were received. German authorities that receive information obtained by strategic surveillance have to examine every six months if these data are still required and have to order deletion immediately if they are not deemed relevant any longer.

7. According to the G 10 and the Telecommunications Act (*Telekommunikationsgesetz*), Telecommunication service providers are obliged to cooperate with the BND to facilitate strategic surveillance. They have to provide both information about the development of their infrastructure and access to backdoors. The service providers and their involved staff who need to be pre-screened by the intelligence services under the Security Screening Act (*Sicherheitsüberprüfungsgesetz*)[18] are bound to secrecy.

Oversight and legal remedies

8. Apart from administrative oversight by the Federal Government, strategic surveillance by the BND is supervised by the Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*) of the German

[17] Scheele, J. (2014), Verdachtslose Rasterfahndung des BND. Zehnjahresbilanz 2002-2012, *Bürgerrechte & Polizei/CILIP*, No. 105 (May 2014), pp. 34-43.
[18] Germany, Security Screening Act (*Sicherheitsüberprüfungsgesetz*), 20 April 1994, last amended 7 December 2012, available at: http://www.gesetze-im-internet.de/s_g/BJNR086700994.html.

Bundestag (*Deutscher Bundestag*) and its G 10 Commission (*G 10-Kommission*). Both bodies meet in camera. Their members and staff are bound to secrecy, and the dates of their meetings are not communicated to a wider public by, for instance, publishing them on the website of the German Bundestag as all its committees do. Except for short activity reports published on a biannual respectively annual basis no documents are made available to the public. Whereas the Control Panel is composed of [currently] nine elected Members of Parliament, the G 10-Commission has four members and four proxies who are elected by the Control Panel and serve on an honorary basis. Both oversight bodies are supported by a small secretariat that is part of the administration of the German Bundestag. The Control Panel approves the selection of "telecommunication relations", i.e. the geographical regions of interest, which reportedly comprised 150 nations and another 46 regions for the monitoring of "international terrorism" in 2010.[19] The G 10 Commission has to approve the issued surveillance orders and the list of search terms for the filtering process. Moreover, the G 10 Commission decides if and when persons whose communications have been caught by the strategic dragnet search are notified about this fact. Usually, notifications should be issued after the termination of surveillance but the period can be extended and notifications can even be waived after five years if the members of the G 10 Commission are unanimously convinced that the purpose of surveillance will be undermined by notification also in the future. Finally, the G 10 Commission is in charge of deciding complaints of persons who believe that they are affected by surveillance of their telecommunication by the federal intelligence agencies.

9. In addition, the Trust Panel (*Vertrauensgremium*), a sub-committee of the Budget Committee of the German Bundestag, is deciding on the secret budgets of the federal intelligence services and thus also on investments of the BND in new surveillance technologies. Like the Control Panel, the Trust Panel is composed of nine elected Members of Parliament who meet in camera and publish short activity reports.

10. In the case of strategic surveillance, legal complaints challenging the issuing and implementation of surveillance orders can be lodged with the Federal Administrative Court (*Bundesverwaltungsgericht*) in Leipzig which is the first and last instance for all issues related to the BND. Except for surveillance orders for purposes to pre-empt military attacks that can only be challenged by persons who have been notified about having been subjects of surveillance, any person can lodge a legal complaint in Leipzig. However, as a recent case illustrates, the burden of proof that one was actually affected by secret surveillance is very high if not demonstrated by a notification.[20] If complainants fail at the court in Leipzig they may lodge a complaint beyond the instances with the Federal Constitutional Court (*Bundesverfassungsgericht*) in Karlsruhe.

11. Unlike with other personal data processed by the BND, the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für Datenschutz und Informationsfreiheit*) is not in charge of supervising the legality of processing data obtained by G 10 operations as this area is explicitly excluded from her domain. However, the G 10 Commission can request the expertise of her office.

---

[19] Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), *BVerwG 6 A 1.13*, 28 May 2014, para. 30, available at: http://www.bverwg.de/entscheidungen/entscheidung.php?ent=280514U6A1.13.0.

[20] Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), BVerwG 6 A 1.13, 28 May 2014. See Annex 4.

12. In theory, data subjects can request access to information on their personal data held by the BND, according to Section 7 of the BND Act (*Bundesnachrichtendienstgesetz*) read in conjunction with Section 15 of the Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*). However, the chances for success to get access to G 10 data from strategic surveillance equals zero. Firstly, requesting data subjects have to refer to "precise circumstances" to justify their request. Secondly, they have to demonstrate a "special interest". Thirdly, the BND will certainly not inform persons about the existence of G 10 data who have not already been notified under the G 10 Act about their surveillance as the service can deny access to data if the revelation could pose risks to national security or the service's sources and tasks. Hence, the only avenue which is actually open to persons who seek information is the G 10 Commission.

The spying of the "open sky"

13. Surveillance of communications in and between foreign countries, so called "open sky" surveillance, is the core business of the BND. In 1999, the BND reported during legal proceedings at the Federal Constitutional Court that of the 15,000 communications that were then caught on a daily basis only 700 fell within the scope of the G 10.[21] In 2013, the BND confirmed in response to revelations of the Snowden files that 417 million metadata collected by "open sky" surveillance in December 2012 among others in Afghanistan were transferred to the U.S. National Security Agency;[22] and in August 2014 it was reported that communications of the U.S. Secretaries of State, Hillary Clinton and John Kerry, were allegedly caught during visits in the Near and Middle East as unintended by-catch in the BND dragnet casted over these regions.[23]

14. Despite its massive extent, BND "open sky" surveillance is not regulated by the G 10. Usually "open sky" surveillance is justified by Section 1 (2) of the BND Act which defines the task of the BND as following: "The Federal Intelligence Service collects and analyses information which is necessary for the purpose of generating intelligence on foreign countries which is of relevance for the foreign and security policy of the Federal Republic of Germany." Moreover, the BND Act explicitly states that the collection of data outside Germany does not fall under German data protection regulation. Nonetheless, the Federal Constitutional Court decided in its 1999 verdict that fundamental rights have to be respected, at least when foreign-to-foreign communication is collected or processed in Germany.[24] Given the court's confirmation that the fundamental right to privacy of communications is not limited to German citizens, the NSA revelations have recently amplified critical voices calling for the regulation of "open sky" surveillance in accordance with the law.[25]

---

[21] Huber, B. (2013), 'Die strategische Rasterfahndung des Bundesnachrichtendienstes', *Neue Juristische Wochenzeitschrift*, 35/2013, p. 2575.
[22] König, M. (2014), 'Die 500-Millionen-Frage', *Süddeutsche Zeitung*, 8 August 2013, available at: http://www.sueddeutsche.de/politik/bnd-nsa-spaehaffaere-die-millionen-frage-1.1742027.
[23] Der Spiegel (2014), 'Beifang im Netz', 18 August 2014 (34/2014).
[24] Federal Constitutional Court (*Federal Constitutional Court*), BVerfG, 1 BvR 2226/94, 14 July 1999.
[25] See among others Huber, B. (2013), 'Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite', *Neue Juristische Wochenzeitschrift*, Vol. 32, No. 35, pp. 2572-2577; Bäcker, M. (2014): *Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stelungnahme zur Anhörung des NSA-Untersuchungsauschusses am 22. Mai 2014*, available at: https://www.bundestag.de/blob/280844/35ec929cf03c4f60bc70fc8ef404c5cc/mat_a_sv-2-3-pdf-data.pdf; Hoffmann-Riem, W. (2014), *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses*

15. In theory, foreigners could request access to information in accordance with Section 7 of the BND Act. However, as, firstly, they would need to refer to “precise circumstances” and demonstrate a “special interest” to justify their claim, and, secondly, the BND would need to see no risks implied by the revelation of information, there is hardly a case to imagine in which persons affected by “open sky” surveillance could be able to reclaim their data.

am 22. Mail 2014, Hamburg, Bucerius Law School, available at: https://www.bundestag.de/blob/280846/04f34c512c86876b06f7c162e673f2db/mat_a_sv-2-1neu--pdf-data.pdf.

Version of 23 September 2014

Annex 1 – Legal Framework relating to mass surveillance

A - Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	**A definition of the categories of individuals liable to be subjected to such surveillance**	**Nature of circumstances which may give rise to surveillance**	**List purposes for which surveillance can be carried out**	**Previous approval / need for a warrant**	**List key steps to be followed in the course of surveillance**	**Time limits, geographical scope and other limits of mass surveillance as provided for by the law**	**Is the law allowing for mass surveillance in another country (EU MS or third countries)?**
Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, also known as *Artikel 10-Gesetz* or *G 10*)[26] – Act of the Parliament	The G 10 provides for both telecommunications **surveillance of individual persons or organisations** (Section 3) and **"strategic" interception of international telecommunications** between foreign countries and Germany (Section 5)	Section 3 G 10 warrants for postal and telecommunications **surveillance in "individual cases"** of "anyone" who is suspected to plan, commit or having committed a) crimes against national security listed in a catalogue referring to acts criminalised by the Penal Code (*Strafgesetzbuch*), the Association Act	The *Verfassungsschutz*, the Military Counter-Intelligence Service (MAD) and the Federal Intelligence Service (BND) are warranted to intercept telecommunications to avert threats to the "free democratic basic order", the existence or security of the Federation or a	G 10 telecommunications surveillance of the federal intelligence authorities are subject to oversight by the Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*) of the German Bundestag and the G 10 Commission (*G 10-Kommission*) whose members are appointed by	Every surveillance order has to be applied for by the head of an intelligence service or his permanent deputy. The application has to be in written form and it needs to justify the surveillance and provide detailed information on its target, form, scope and duration. (Section 9 G 10)	Every issued interception order has to clearly describe the form of surveillance, the extent and period of time. They have to be limited to three months but can be extended with the approval of the G 10 Commission. Strategic surveillance orders have to define the used search terms,	Section 5 G 10 provides for **"strategic" surveillance of communications from other countries (EU and third countries) to and from Germany** by the Federal Intelligence Service (BND). Surveillance in or between foreign countries is not regulated by the G 10. This so-called

[26] Germany, the Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), 26 June 2001, last amended at 6 June 2013, available at: http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html.

		(*Vereinsgesetz*) and the Residence Act (*Aufenthaltsgesetz*), b) violent assaults by "terrorist associations", c) the formation of clandestine groups of foreigners, or against "anyone" who is suspected to be member of an association that aims to commit crimes against national security or the "free democratic basic order". Section 5 G 10 warrants only the Federal Intelligence Service (BND) to **"strategically" intercept international telecommunications to and from Germany**, using "search terms". Though these search terms may also comprise phone numbers or email addresses they **must not target connections**	*Land*, including the security of foreign NATO-troops based in Germany (Section 1 (1) G 10). In addition, the BND is also warranted to strategically intercept communications to pre-empt threats of international terrorism, the proliferation of arms, organised trafficking of illegal drugs, money forgery, money laundering, the smuggling of irregular migrants, and in cases of oversea hostage-takings of Germans or other threats against life and limb against persons in foreign countries that do significantly touch German interests.	the Control Panel (Section 1 (2) G 10). Control of eavesdropping by the *Verfassungsschutz* authorities of the *Länder* is regulated by laws of the *Länder* (Section 16 G 10) which are not detailed here. The G 10 Commission, headed by a fully qualified lawyer and holding in camera meetings, has to **approve all individual cases of telecommunications surveillance ex ante under Section 3 G 10**. For this purpose the Federal Ministry of the Interior informs the Commission once a month about orders to intercept before they are put into effect. (Section 15 G 10)	On the basis of an application, the Federal Ministry of the Interior issues a written order and informs, if necessary, the telecommunication service provider. (Sections 10 G 10) The actual data collection has to be realised under supervision of a fully qualified lawyer serving the warranted authority. Data collection need to be stopped immediately if no longer necessary. Both the Ministry of the Interior and, if previously informed, the telecommunication service provider have to be notified about the termination of surveillance (Section 11 G 10). Collected data have to be examined	the area of interest, the cable or satellite connections, and the amount of data flow to be intercepted on the selected connections. However, the flow of data must not exceed 20 per cent of the total flow on these connections. Whereas no limits in terms of nationality exist for the telecommunications surveillance of individuals under Section 3 G 10, connections of persons living in Germany and German citizens abroad may not be deliberately targeted by strategic surveillance. Surveillance is also limited if it touches "the core of private life" (*Kernbereich privater*	**"open sky" surveillance** – being the core business of the BND and reportedly dwarfing the extent of G 10 strategic surveillance – is only implicitly mentioned in Section 1 (2) of the Federal Intelligence Service Act (*Bundesnachrichtendienstgesetz*), defining as task of the BND the collection and analysis of information necessary for producing intelligence of relevance for German foreign and security policy. Section 1 (2) read in conjunction with Section 2 (1) of the BND Act makes clear that data protection standards shall only apply to information collected in

		in Germany or foreign connections of German citizens (Section 5 (2) G 10). Section 8 G 10 regulates the **rare case of strategic surveillance ordered to pre-empt risks for life and limb of individuals in foreign countries** when German interests are touched significantly, e.g. in cases of hostage-taking of German citizens.		In the case of **strategic surveillance** under Section 5 G 10, the "telecommunication relations", in fact the targeted geographic regions and states, to be intercepted have to be approved by the Parliamentary Control Panel, whereas the G 10 Commission has to previously approve the search terms ex ante. (Section 5 (1) and Section 15 (6) in conjunction with Section 10 (4) G 10). In case of "danger at hand" (*Gefahr im Verzug*) interception can be ordered by the Ministry of the Interior without previous approval but these orders are reviewed by the G 10 Commission latest at their next meeting. (Section 15 (6) G 10)	immediately and then every six months if required to fulfil the authorities' tasks of the purposes of surveillance. Unless no longer required, collected data have to be deleted immediately. (Sections 4 (1) and 6 (1) G 10) In the case of the automated dragnet search of strategic surveillance under Sections 5 and 8 G 10 the relevance of obtained information can be examined in a second step of automated filtering that might also rely on identifiers of German telecommunication connections. (Section 6 (3) G 10) Any obtained G 10 data that are deemed to be required and, hence, are stored have to be tagged	*Lebensgestaltung*). The only exceptions from this general rule are 1) automated surveillance in individual cases of which the further use of recorded information has to be approved ex ante by the G 10 Commission and 2) strategic surveillance aiming to pre-empt military strikes against Germany. (Sections 3a and 5a G 10) Finally, individual surveillance under Section 3 G 10 is limited to a certain extent and with variations according to the persons' functions, when information is collected about communications of clerics, lawyers, Members of Parliament, journalists and counselling staff. (Section 3b G 10)	Germany. Nevertheless the BND is bound – as every other agency – to the fundamentals of the constitutional order, eg. the principle of proportionality and ensuring everyone´s human dignity. The constitutionality of this situation for the privacy of foreigners' communications is, however, questioned and calls for legal regulation of "open sky surveillance are growing since the Snowden revelations began.

					as data resulting from restrictions of the privacy of communications. (Sections 4 (2) and 6 (2) G 10) Obtained G 10 data must be transferred to third parties (other German intelligence authorities, the federal government, the Federal Office for Business and Export Control, the police or public prosecution, foreign intelligence authorites) only for specified purposes; and third parties should keep the data tagged as G 10 data and have to examine if data are still relevant and required in the light of the purpose for which they where transferred every six months (Sections 4, 7 and 7a G 10). Foreign intelligence	According to Section 4 (2) of the BND Act read in conjunction with Section 11 of the Federal Act on the Protection of the Constitution, data obtained about minors younger than 16 years must only be stored and processed if the minor is suspected to plan or commit serious crimes specified in these laws.	

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					services are not bound by periodical examination obligations but the G 10 Commission has to be informed about data transfers to foreign services and transfers need to be approved by the Federal Chancellery.		

B - Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, also known as *Artikel 10-Gesetz* or *G 10*) Federal Intelligence Service Act (*Bundesnachrichtendienstgesetz*)[27] Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*)[28] Federal Data Protection Act (*Bundesdatenschutzgesetz*)[29]	Apart from the above mentioned limitations of surveillance and the obligation to tag data obtained by wiretapping, persons subjected to individual surveillance under Section 3 G 10 have to be informed after the termination of surveillance, if such a notice does not erode the aim of surveillance or if no "comprehensive harms for the well-being of the Federation or a Land" is risked. If such an information is not issued within 12 months after the termination of surveillance, any extension of this period needs to be approved by the G 10 Commission. The Commission then decides for how long the information can be postponed. In case of unanimous decisions of the Commission that even five years after the termination of surveillance non-information is very likely to be justified also	If data protection rules apply at all (see Annex 1A for the extralegality of "open sky" surveillance by the BND) they do not make a distinction between German citizens and foreigners but are valid for all "affected persons".	According to Sections 1 (2) and 2 (1) of the BND Act, data protection safeguards only apply to data collected in Germany. Nonetheless, foreigners can apply for access to data with the BND under Section 7 of the BND Act. For the difficulties to exercise the rights in practice, see second column of this table.

[27] Germany, Federal Intelligence Service Act (*Bundesnachrichtendienstgesetz*), 20 December 1990, last amended 20 June 2013, available at: http://www.gesetze-im-internet.de/bndg/BJNR029790990.html.
[28] Germany, Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*), 20 December 1990, last amended at 20 June 2013, available at: http://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html.
[29] Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), 20 December 1990, last amended 14 August 2009, English version available at: http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
	in the future and obtained data can be deleted, it can be decided to refrain from informing former subjects of surveillance. (Section 12 (1) G 10) Similarly, these provisions also apply for persons whose communication data have been caught by the dragnet search of strategic surveillance under Sections 5 or 8 G 10 as relevant information, if their data have not been deleted immediately after the collection. (Section 12 (2) G 10) Complaints against the admissability and necessity of restrictions of the privacy of communications can be lodged with the G 10 Commission that is supervising the overall collection, processing and usage of G 10 data by federal intelligence services (Section 15 (5) G 10). According to Section 24 (2) sentence 3 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*), G 10 data are explicitly excluded from the remit of the Federal Commissioner for Data Protection who is usually also supervising data processing by the federal intelligence agencies. However, the G 10 Commission may request the Data Protection Commissioner's expertise.		

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
	Issued surveillance orders and other decisions of the BND can be legally challenged. However, any order on individual surveillance or on strategic surveillance aiming to pre-empt military attacks against Germany can be only challenged after affected persons are informed by the surveillance. Only orders on strategic surveillance to pre-empt international terrorism, arms proliferation and organised crime can be legally challenged before such an information notice is issued. (Section 13 G 10) According to Section 50 of the Administrative Courts Order (*Verwaltungsgerichtsordnung*)[30] the Federal Administrative Court (*Bundesverwaltungsgericht*) in Leipzig is responsible for legal challenges against the BND and its (mass) surveillance. According the Sections 7 and 5 of the BND Act read in conjunction with Sections 15 and 12 of the Act on the Protection of the Constitution data subjects have, at least in theory, the right to access their data and request correction or deletion. However,		

[30] Germany, Administrative Courts Order (*Verwaltungsgerichtsordnung*), 21 January 1960, last amended 8 July 2014, available at: http://www.gesetze-im-internet.de/vwgo/BJNR000170960.html.

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
	the threshold is high: Data subjects have to justify their request by referral to a "precise circumstance" and they have to demonstrate a "special interest". Moreover, access to information can be denied if the authorities believe that national security or the completion of their tasks are threatened, sources may be revealed, or the interests of third parties affected. If access is granted, no information has to be revealed on the origins of the data or third parties to which data were transferred. Denial of access rights does not need to be publicly justified. The collection and processing of data from "open sky" surveillance do not fall within the scope of the G 10 and are, thus, not supervised by the G 10 Commission. Hence, "open sky" surveillance is supervised by the Parliamentary Control Panel. In addition, if open sky data are stored and processed by the BND in Germany, the Federal Commissioner for Data Protection should be in charge: According to Section 24 of the Federal Data Protection Act, data protection supervision at all federal authorities falls into the remit of the		

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
	Federal Commissioner for Data Protection, and also the federal intelligence authorities are obliged to support the Commissioner and her or his authorised agents, answer questions, deliver files and allow inspections. However, in "individual cases" support can be denied by the Federal Chancellery for reasons of national security according to Section 24 (4) of the Federal Data Protection Act. The extent to which the Federal Chancellery makes use of this provision is not known.		

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Federal Chancellery (*Bundeskanzleramt*)	Executive	Sections 1 (1) and 12 of the Federal Intelligence Service Act (*BND-Gesetz*)	Administrative and functional supervision of the Federal Intelligence Service (BND) and coordination of the three federal intelligence authorities, i.e. the BND, the Military Shield Service (MAD) and the Federal Office for the Protection of the Constitution.	The overall staff of the Federal Chancellery is 480. No figures are available for Department 6 (one of six departments of the Chancellery) that is in charge of the supervision of the Federal Intelligence Service and the coordination of the three federal intelligence authorities.[31] The head of Department 6, the so-called Intelligence Services Coordinator ("*Geheimdienstkoordinator*"), is appointed by the Federal Chancellor; he or she acts as proxy of the Commissioner for Intelligence Services (*Beauftragter für die Nachrichtendienste*).	Issuing instructions, defining federal intelligence priorities and taking disciplinary action against members of the intelligence services.
Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*)	Parliamentary	Control Panel Act (*Kontrollgremiumgesetz*)[32] and Section 1, 5, 7, 8 and 14 of the Article 10 Act (*Artikel 10-Gesetz*)	Ex ante approval of "telecommunications connections" for strategic surveillance by the BND. Otherwise, the Control Panel is informed by the Federal Ministry of the Interior on an biannual	Currently, the Parliamentary Control Panel is composed of nine Members of Parliament who are elected as panel members by the majority of the German Bundestag for one legislative period (the number of members is not legally regulated but can vary	Apart from reporting obligations of the Federal Government, the Control Panel has the right to request information from the federal intelligence authorities, to inspect their premises, to process hints from members of

[31] Bundesregierung, *Das Bundeskanzleramt*, available at: http://www.bundesregierung.de/Webs/Breg/DE/Bundesregierung/Bundeskanzleramt/_node.html

[32] Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009, available at: http://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html.

			basis over the implementation of the G 10 Act and leaves the control of telecommunications surveillance mainly to the G 10 Commission. However, the Control Panel could use its powers to take own initiatives to examine telecommunications surveillance by the intelligence authorities, unless limited by the "direct executive responsibility" of the Federal Government.	in each legislative period). The Panel has to meet at least once in three months but usually meets once in a month. The chair rotates on an annual basis between MPs from the parties in power and the opposition parties.[33] The work of the panel is supported by a secretariat with a staff of six persons (three legal experts and three assistants and secretaries) who, however, also support the work of the G 10 Commission and two other special bodies of the German Bundestag. In addition, the Control Panel is creating an operational unit to support its work with five persons of the higher service, one assistant and a secretary.[34] In addition, the members of the panel may – in accordance with Section 11 of the Control Panel Act - appoint individual staff of their party faction to support	the intelligence services and to commission reports by external experts. However, the Control Panel holds in camerameetings and has an obligation of confidentiality, unless two third of its members decide to publicly comment on particular issues. The Panel submits twice in a legislative period brief public reports on its activities to the German Bundestag, The most recent one, published in December 2013, was 14 pages long.[36] In addition, the Parliamentary Control Panel publishes annual report on the kind and extent of surveillance orders according to the G 10.

[33] https://www.bundestag.de/bundestag/gremien18/pkgr

[34] Thorsten Denkler (2014): 'Bundestagsverwaltung sucht fünf Trüffelschweine', in: *Süddeutsche Zeitung*, 13.03.2014. http://www.sueddeutsche.de/politik/2.220/kontrolle-der-nachrichtendienste-bundestagsverwaltung-sucht-fuenf-trueffelschweine-1.1911701. Additional details provided via telephone by a member of the secretariat PD 5 of the German Bundestag on 9 September 2014 and via email by the chair of the Control Panel on 17 September 2014.

[36] German Bundestag (2013): *Unterrichtung durch das Parlamentarische Kontrollgremium (Berichtszeitraum November 2011 bis Oktober 2013)*. Drucksache 18/217, 19.12.2013.

				their work as members of the control panel. The Federal Government has to be consulted and the majority of the Control Panel has to approve the appointment. These persons may, however, usually not attend the meetings of the panel. In September 2014 six staff members of the parliamentary party factions were appointed to support the work of the Control Panel.[35]	
Trust Panel (*Vertrauensgremium*)	Parliamentary	Section 10a of the Federal Budget Rules (*Bundeshaushaltsordnung*)[37]	The Trust Panel of the German Bundestag decides on the secret budget of the federal intelligence authorities and, thus, also on investments in surveillance technologies.	The nine members of the Trust Panel are Members of Parliament who are elected by the majority of the German Bundestag. They cooperate with the Control Panel.[38] The membership of MPs in both the Control Panel and the Trust Panel is possible. The members of the Trust Panel are supported by the small secretariat of the Budget Committee.	Issuing recommendations on the overall budget of the federal intelligence authorities to the Budget Commission of the German Bundestag. The Trust Panel is also bound to obligations of confidentiality and has powers very similar to the Control Panel in terms of rights to information and inspection but cannot issue public statements. It only publishes a brief report on its activities

[35] Information provided via email by the chair of the Control Panel on 17 September 2014.
[37] Germany, Federal Budget Order (*Bundeshaushaltsordnung*), 19 August 1969, last amended 15 July 2013, available at: http://www.gesetze-im-internet.de/bho/BJNR012840969.html.
[38] German Bundestag (2014): 'Parlamentarische Kontrollgremien', in: *Datenhandbuch des Deutschen Bundestages*, available at: http://www.bundestag.de/blob/196230/d08910426e22fe7e9910dfe06c39b2f9/kapitel_11_06_parlamentarische_kontrollgremien-data.pdf.

					twice in a legislative period.
G 10 Commission (*G 10-Kommission*)	Parliamentary	Section 1, 4 and 15 of the Article 10 Act	Ex ante approval of surveillance orders and supervision of data protection throughout the overall life cycle of collected data.	The four members of the G 10 Commission and their four proxies are serving on an honarary basis. They are elected by the Parliamentary Control Panel but are not necessarily Members of Parliament. Usually they are independent experts. The work of the G 10 Commission is supported by the same administrative secretariat that is working for the Parliamentary Control Panel.	Issuing of legally binding decisions on the admissibility of surveillance orders and on complaints. Right to request information from the federal intelligence authorities and to inspect their premises to check storage and processing of G 10 data.
Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für Datenschutz und Informationsfreiheit*)	Executive/Parliamentary	Federal Data Protection Act (*Bundesdatenschutzgesetz*)	Oversight of the implementation of data protection regulations. Processing of G 10 data is excluded from the remit of the Federal Data Protection Commissioner according to Section 24 of the Federal Data Protection Act, except in cases when the G 10 Commission asks for his or her expertise and opinion.	The Federal Commissioner for Data Protection is proposed by the Federal Government and elected by the majority of the German Bundestag. In 2014, her office has a staff of 87.[39] Department 5, which is in charge of the oversight over the federal intelligence and police services, is one of nine departments and has currently a staff of six persons, to be increased to 7.5 in September 2014.[40]	Issuing non-binding complaints (*Beanstandungen*)

[39] Germany, Budget Law 2014 (*Haushaltsgesetz 2014*), 15 July 2014.
[40] Information provided via telephone by the head of department on 18 August 2014.

Annex 3 – Remedies

Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (*Gesetz über die Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*)				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
Collection	No	Yes, in theory the right of access exists but to exercise this right in practice is very difficult. (see Annex 1B for the provisions of Section 7 BND Act)	Individuals can either lodge a complaint with the G 10 Commission if they believe that they are under G10 surveillance, or they can lodge a legal complaint with the Federal Administrative Court (*Bundesverwaltungsgericht*) if they challenge data processing in the context of strategic G 10 surveillance but only when challenging orders directed against international terrorism, arms proliferation, drug trafficking, money forgery or laundering, or organised human trafficking. If failing at the Federal Administrative Court, complainants can take their cases to the Federal Constitutional Court (*Bundesverfassungsgericht*). Whereas the Federal Data Protection Commissioner has no mandate to supervise information obtained by G 10 surveillance, he or she could, theoretically, process complaints of persons who seek access to data obtained by the BND through “open sky” surveillance. The Commissioner has, however, no formal power to enforce access rights as he or she can only issue non-binding complaints against the BND.	Section 12 and 13 of the Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (G 10) Section 50 (1) No. 4 of the Rules of the Administrative Courts (*Verwaltungsgerichtsordnung*) Article 93 (1) No. 4a of the Basic Law (*Grundgesetz*) read in conjunction with Section 13 No. 8a and Chapter 15 of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz*) Section 7 of the BND Act read in conjunction with Section 21, 24 and 25 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*) for the theoretical case of foreigners seeking access to their data obtained by “open sky” surveillance.
Analysis	No			
Storing	No			
Destruction	No			
After the whole surveillance process has ended	Yes, but not necessarily (see Annex 1B)			

Annex 4 – Surveillance-related case law at national level

Case title	BVerfG, 1 BvR 2226/94 (Constitutional complaints against the expansion of BND powers for strategic telecommunications surveillance)
Decision date	14.07.1999
Reference details	Bundesverfassungsgericht (*Federal Constitutional Court*)
Key facts of the case	Three constitutional complaints by one academic, two journalists, one of which living in Uruguay, one publisher and one citizen of Uruguay working for a journalist challenged the amendment of the G 10 by the Combating Crime Act (*Verbrechensbekämpfungsgesetz*) passed in 1994; in particular they complained about the significant expansion of BND powers for strategic telecommunications surveillance for purposes of pre-empting international terrorism, arms proliferation and organised crime, the limited obligations to notify intercepted persons if data were deleted after three months, the widened opportunities to transfer data to other authorities and lacking legal remedy.
Main reasoning/argumentation	The court argued that the federal legislator may regulate BND telecommunications surveillance for purposes serving German foreign and security policy beyond pre-empting military conflict. However, strategic surveillance to collect intelligence for general purposes of crime control is not compatible with the Basic Law. Moreover, the court reasoned that the privacy of communications does not only protect the content of communication but also the circumstances of communication (metadata) and the processing and use of obtained information, including the transfer of data to third parties. Hence, information obtained by telecommunications surveillance needs special protection, e.g. by tagging, and further use should be bound by the original purpose of data collection, unless provided for by law. In addition, persons who have been subjected to surveillance need, in principle, to be notified at least afterwards, and control mechanisms need to be independent and effective throughout the whole cycle of data processing. Finally, the court argued that the privacy of telecommunications is not limited to German territory; at least the fundamental right to the privacy of communications has to be respected if data of foreign telecommunications are collected and processed on German soil.
Key issues (concepts, interpretations)clarified by the case	Strategic interception of the BND based on a G 10-warrant cannot be expanded unlimited, purpose limitation needs of data collection needs to be to be respected, and independent control needs to be effective.
Results (sanctions) and key consequences or implications of the case	The court ruled that the G 10 provisions on the competences of the BND regarding surveillance for the purpose to pre-empt money laundering, on the use of obtained data, the transfer of data to other authorities and on the limited obligation to notify affected persons are not compatible with the German Basic Law. In addition, the court demanded stronger oversight by the G 10 Commission. The G 10 was then substantially revised in June 2001 by the Act Revising the G 10 (*Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses*) to fulfil this obligation. However, the opportunity was taken to expand the powers of the BND to intercept not only international radio communications but cable transmissions, to use strategic surveillance also in

	case of hostage-taking abroad, and to use obtained information also for combating extremist organisations and anti-constitutional parties. Two of the complainants took their case further to the European Court of Human Rights. The Court decided in 2006 that the complaint was manifestly ill-founded.[41]

Case title	BVerwG 6 A 1.07 (Complaint by a convicted member of a "terrorist association" against BND strategic surveillance after 9/11 and late information about being surveilled)
Decision date	23.01.2008
Reference details	Federal Administrative Court (*Bundesverwaltungsgericht*)
Key facts of the case	A few days after 9/11 the Federal Ministry of the Interior issued an order for strategic surveillance for the area of "international terrorism" by the BND by which five communications of the complainant with a connection in Afghanistan were caught in October and November 2001. With the approval of the G 10 Commission the complainant was only informed about the surveillance in 2006, after he was arrested and convicted for being member of a "terrorist association". The complainant applied for the declaration that the strategic surveillance was not justified as the search for "sleepers" who prepare assaults in third countries does not fall under the purpose of Section 5 G 10 to pre-empt international terrorism related to Germany. In addition, he appliced for the declaration that he was informed about the interception of his telecommunications too late.
Main reasoning/argumentation	The court argued that the BND surveillance was justified as the term "international terrorism related to Germany" does not imply a focus on the risk of terrorist assaults in Germany. Rather the nature of the terrorist threat makes international cooperation and burden sharing necessary. Moreover, the court determined that its power to assess the decision of the G 10 Commission to inform the complainant only five years after the termination of surveillance is limited due to the prerogative of the G 10 Commission. Given the difficulties to predict the implications of an information about surveillance for the work of the intelligence services, decisions of the G 10 Commission against notifications are according to the letter of Section 12 G 10 if the Commission fears negative effects.
Key issues (concepts, interpretations) clarified by the case	The scope of "international terrorism related to Germany" was clarified and the prerogative of the G 10 Commission regarding decisions about notifications was confirmed.
Results (sanctions) and key consequences or implications of the case	The court dismissed the case.

Case title	Az. BVerwG 6 A 1.13 (Complaint by a lawyer against BND strategic surveillance in 2010 under Section 5 G 10)

[41] European Court of Human Rights (ECtHR), *Weber and Saravia v. Germany*, 54934/00, 29 June 2006.

Decision date	28.05.2014
Reference details	Federal Administrative Court (*Bundesverwaltungsgericht*)
Key facts of the case	In February 2013, a lawyer lodged a complaint against strategic surveillance of communications under Section 5 G 10 by the Federal Intelligence Service (BND) after it was reported that 37 million communications were caught in 2010 by the dragnet search, most of it emails, of which only 12 were considered as "relevant". The complainant argued that it was very likely that he was affected because of his frequent international email communication as professional lawyer with contacts abroad and, hence, he applied for the declaration that the BND acted in a disproportionate manner and violated his privacy of communication.
Main reasoning/argumentation	It was not evident for the court that email communications of the lawyer were caught by the dragnet surveillance of the BND as all communications that were not filtered as "relevant" by automated means were deleted more or less immediately and logfiles from 2010 were already deleted after one year. Hence, the court argued that despite the obvious difficulties to present hard evidence they must not lower the threshold as this would otherwise invite popular action against BND's strategic surveillance unnecessarily duplicating the independent and effective oversight by the G 10 Commission.
Key issues (concepts, interpretations) clarified by the case	Applications for declaration against strategic surveillance of telecommunication under Section 5 G 10 are only admissible if it is evident that complainants were actually affected. The right to an effective remedy does not mean that the burden of proof has to be eased.
Results (sanctions) and key consequences or implications of the case	The court decided that the complaint is not admissible. The complainant has to bear the costs of the legal procedure. When the judgement was proclaimed, the lawyer announced to lodge a constitutional complaint with the Federal Constitutional Court.[42]

[42] Süddeutsche Zeitung (2014), 'Karlsruhe soll BND-Überwachung prüfen', 28 May 2014.

Annex 5 – Key stakeholders at national level

Name of stakeholder **(in English as well as your national language)**	**Type of stakeholder** ***(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)***	**Contact details**	**Website**
Federal Intelligence Service (*Bundesnachrichtendienst*)	Public authority (German foreign intelligence service)	Bundesnachrichtendienst Heilmannstraße 30 82049 Pullach Tel.: +49 89 7 93 15 67 Mail: zentrale@bundesnachrichtendienst.de	http://www.bnd.bund.de
Federal Chancellery (*Bundeskanzleramt*)	Government	Bundeskanzleramt 11012 Berlin Tel.: +49 30 18 400 0 Mail: poststelle@bk.bund.de	http://www.bundeskanzleramt.de
Federal Ministry of the Interior (*Bundesministerium des Innern*)	Government	Bundesministerium des Innern Alt-Moabit 101D 10559 Berlin Tel.: +49 30 18 681 0 Mail: poststelle@bmi.bund.de	http://www.bmi.bund.de
Federal Ministry of Justice and Consumer Protection (*Bundesministerium der Justiz und für Verbraucherschutz*)	Government	Bundesministerium der Justiz und für Verbraucherschutz Mohrenstraße 37 10117 Berlin Tel.: +49 30 18 580 0 Mail: poststelle@bmjv.bund.de	http://www.bmjv.bund.de
Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*)	Parliament (responsible for scrutiny of the work of the intelligence services at Federal level)	Parlamentarisches Kontrollgremium Deutscher Bundestag Platz der Republik 1 11011 Berlin Tel.: +49 30 227 0 Mail: mail@bundestag.de	https://www.bundestag.de/bundestag/gremien18/pkgr
Trust Panel (*Vertrauensgremium*)	Parliament (a subcommitte of the Budget Committee deciding on the secret	Vertrauensgremium Deutscher Bundestag	N/A

	budgets of the federal intelligence services)	Platz der Republik 1 11011 Berlin Tel.: +49 30 227 0 Mail: mail@bundestag.de	
G 10 Commission (*G10-Kommission*)	Parliament (takes decisions on the necessity and admissibility of restrictions on the privacy of correspondence, posts and telecommunications)	G 10-Kommission Deutscher Bundestag Platz der Republik 1 11011 Berlin Tel.: +49 30 227 0 Mail: mail@bundestag.de	https://www.bundestag.de/bundestag/gremien18/g10
Committee on Internal Affairs (*Innenausschuss*)	Parliament	Innenausschuss Deutscher Bundestag Platz der Republik 1 11011 Berlin Tel.: +49 30 227 32858 Mail: innenausschuss@bundestag.de	http://www.bundestag.de/htdocs_e/bundestag/committees/a04
1st Committee of Inquiry ("NSA") (1. Untersuchungsausschuss "NSA")	Parliament	1. Untersuchungsausschuss der 18. Wahlperiode Deutscher Bundestag Platz der Republik 1 11011 Berlin Tel. +49 30 227 39217 Mail: 1.untersuchungsausschuss@bundestag.de	http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss
Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für Datenschutz und Informationsfreiheit)*	Public authority	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 53117 Bonn Tel.: +49 0228 997799 0 Mail: poststelle@bfdi.bund.de	http://www.bfdi.bund.de
Federal Constitutional Court (*Bundesverfassungsgericht*)	Court	Bundesverfassungsgericht Postfach 1771 76006 Karlsruhe Tel.: +49 721 9101 0 Mail: bverfg@bundesverfassungsgericht.de	http://www.bverfg.de

Federal Administrative Court (*Bundesverwaltungsgericht*)	Court	Bundesverwaltungsgericht Postfach 10 08 54 04008 Leipzig Tel.: +49 341 2007 0 Mail: poststelle@bverwg.de	http://www.bverwg.de
German Institute for Human Rights (*Deutsches Institut für Menschenrechte*)	National Human Rights Institution	Deutsches Institut für Menschenrechte Zimmerstraße 26/27 10969 Berlin Tel.: +49 30 25 93 59 0 Mail: info@institut-fuer-menschenrechte.de	http://www.institut-fuer-menschenrechte.de
Chaos Computer Club	Civil society	Chaos Computer Club e. V. Humboldtstraße 53 22083 Hamburg Mail: mail@ccc.de	http://www.ccc.de
Deutsche Vereinigung für Datenschutz	Civil society	Deutsche Vereinigung für Datenschutz Rheingasse 8-10 53113 Bonn Tel: +49 228 22 24 98 Mail: dvd@datenschutzverein.de	https://www.datenschutzverein.de/
Digital Courage	Civil society	Digitalcourage e.V. Marktstraße 18 33602 Bielefeld Tel.: +49 521 1639 1639 Mail: mail@digitalcourage.de	https://digitalcourage.de/
Digitale Gesellschaft	Civil society	Digitale Gesellschaft e. V. Sophienstraße 5 10178 Berlin Tel.: +49 30 68916575 Mail: info@digitalegesellschaft.de	https://digitalegesellschaft.de/
Humanistic Union (*Humanistische Union*)	Civil society	Humanistische Union Bundesgeschäftsstelle Haus der Demokratie und Menschenrechte Greifswalder Straße 4 10405 Berlin	http://www.humanistische-union.de

		Tel.: +49 30 20 45 02 56 Mail: info@humanistische-union.de	
Internationale Liga für Menschenrechte	Civil society	Internationalen Liga für Menschenrechte Haus der Demokratie und Menschenrechte Greifswalder Straße 4 10405 Berlin Tel.: +49 30 396 21 22 Mail: vorstand@ilmr.de	http://ilmr.de/
netzpolitik.org	Civil society	netzpolitik.org Schönhauser Allee 6/7 10119 Berlin Tel.: +49 30 92105 986 Mail: kontakt@netzpolitik.org	https://netzpolitik.org/
Privacy Project	Civil society	Privacy Project c/o Stiftung Neue Verantwortung Beisheim Center Berliner Freiheit 2 10785 Berlin Tel.: +49 30 81 45 03 78 80 Mail: info@privacyproject.de	http://privacy-project.net
Prof. Dr. Matthias Bäcker	Academia	Prof. Dr. Matthias Bäcker Juniorprofessur für öffentliches Recht Fakultät für Rechtswissenschaft und Volkswirtschaftslehre Universität Mannheim 68161 Mannheim Tel.: +49 621 181 1598 Mail: mbaecker@mail.uni-mannheim.de	http://baecker.uni-mannheim.de/zur_person/index.html
Prof. Dr. Niko Härting	Academia (and practising lawyer)		
Prof. Dr. Wolfgang Hoffmann-Riem	Academia	Prof. Dr. Wolfgang Hoffmann-Riem Bucerius Law School Jungiusstraße 6 20355 Hamburg Mail: whoffmann-riem@gmx.de	http://www.jura.uni-hamburg.de/personen/hoffmann-riem
Prof. Dr. Fredrik Roggan	Academia	Prof. Dr. Fredrik Roggan	http://www.fhpolbb.de/prof-dr-fredrik-

		Strafrecht und Besonderes Verwaltungsrecht Fachhochschule der Polizei des Landes Brandenburg Bernauer Strasse 146 16515 Oranienburg Tel.: +49 3301 8502545 Mail: fredrik.roggan@fhpolbb.de	roggan
Prof. Dr. Heinrich-Amadeus Wolff	Academia	Prof. Dr. Heinrich-Amadeus Wolff Lehrstuhl für Öffentliches Recht, insbesondere Staatsrecht und Verfassungsgeschichte Juristische Fakultät Europa-Universität Viadrina Frankfurt (Oder) Große Scharrnstraße 59 15230 Frankfurt (Oder) Mail: wolff@europa-uni.de	http://www.rewi.europa-uni.de/de/lehrstuhl/or/staatsrecht/lehrstuhlinhaber/index.html

Annex 6 – Indicative bibliography

1. Government/ministries/public authorities in charge of surveillance

- Federal Ministry of the Interior and Federal Ministry of Justice (*Bundesministerium des Innern und Bundesministerium der Justiz*) (2013), *Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland*, Berlin, available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2013/regierungskommission-sicherheitsgesetzgebung.html.

- Federal Ministry of Justice and Consumer Protection (*Bundesministerium der Justiz und für Verbraucherschutz*) (2014), *Keine rechtsfreien Räume für Geheimdienst. Bundesminister der Justiz und für Verbraucherschutz Heiko Maas im Gespräch mit dpa*, 4 August 2014, available at: http://www.bmjv.de/SharedDocs/Interviews/DE/2014/Online/20140804_Interview_DPA.html?nn=1468636.

- German Bundestag (*Deutscher Bundestag*) (2003), *Unterrichtung durch die Bundesregierung. Bericht der Bundesregierung über die Erfahrungen mit dem Gesetz zur Neuregelung von Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10)*, Drucksache 15/2042, 12 November 2003.

- German Bundestag (*Deutscher Bundestag*) (2012), *„Strategische Fernmeldeaufklärung" durch Geheimdienste des Bundes. Antwort der Bundesregierung auf eine Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, weiterer Abgeordneter und der Fraktion DIE LINKE*, Drucksache 17/9640, 15 May 2012.

- German Bundestag (*Deutscher Bundestag*) (2013), *Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontroll nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum November 2011 bis Oktober 2013)*, Drucksache 18/217, 19 December 2013.

- German Bundestag (*Deutscher Bundestag*) (2013), *Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes (Berichtszeitraum 1. Januar bis 31. Dezember 2012)*, Drucksache 18/218, 19 December 2013.

- German Bundestag (*Deutscher Bundestag*) (2014), *Die strategische Rasterfahndung des Bundesnachrichtendienstes im Zeitraum 2002 bis 2012. Antwort der Bundesregierung auf eine Kleine Anfrage der Abgeordneten Jan Korte, Halina Wawzyniak, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE*, Drucksache 18/733, 5 March 2014.

- German Bundestag (*Deutscher Bundestag*) (2014), *Überprüfung der Auslandsaufklärung des Bundesnachrichtendienstes. Antwort der Bundesregierung auf eine Kleine Anfrage der Abgeordneten Jan Korte, Dr. André Hahn, Martina Renner, weiterer Abgeordneter und der Fraktion DIE LINKE*, Drucksache 18/2128, 16 July 2014.

2. **National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance**

- Caspar, J. (2014), 'Strategische Auslandsüberwachung . Jenseits der Grenzen des Rechtsstaates?' *PinG – Privacy in Germany*, Vol. 2, No. 1 (1/2014), pp. 1-6.

- Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit*) (2013), *Abhöraktivitäten US-amerikanischer Nachrichtendienste in Deutschland. Bericht an den Deutschen Bundestag gemäß § 26 Absatz 2 Satz 3 BDSG*, Berlin: Deutscher Bundestag, Drucksache 18/59, 15.11.2013.

3. **Academic and research institutes, think tanks, investigative media report.**

- Bäcker, M. (2014), Strategische Kommunikationsüberwachung auf dem Prüfstand, Kommunikation & Recht, Vol. 17, No. 9, pp. 556-561.

- Bäcker, M. (2014), *Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stelungnahme zur Anhörung des NSA-Untersuchungsauschusses am 22. Mai 2014*, available at: https://www.bundestag.de/blob/280844/35ec929cf03c4f60bc70fc8ef404c5cc/mat_a_sv-2-3-pdf-data.pdf.

- Bäcker, M. (2011), 'Das G 10 und die Kompetenzordnung', *Die Öffentliche Verwaltung*, Vol. 64, No. 21, pp. 840-848.

- Deiseroth, D. (2013), 'Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf', *Zeitschrift für Rechtspolitik*, No. 7/2013, pp. 194-197.

- Heumann, S. and Wetzling, T. (2014), *Strategische Auslandsüberwachung. Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle*, Berlin, Stiftung Neue Verantwortung, available at: http://privacy-project.net/cms/assets/uploads/2014/06/SNV-Policy_Brief_Strategische-Auslands%C3%BCberwachung-LANGVERSION.pdf.

- Hoffmann-Riem, W. (2014), *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mail 2014*, Hamburg, Bucerius Law School, available at: https://www.bundestag.de/blob/280846/04f34c512c86876b06f7c162e673f2db/mat_a_sv-2-1neu--pdf-data.pdf.

- Huber, B. (2013), 'Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite', *Neue Juristische Wochenzeitschrift*, Vol. 32, No. 35, pp. 2572-2577.

- Huber, B. (2009), 'Die Reform der parlamentarischen Kontrolle der Nachrichtendienste und des Gesetzes nach Art. 10 GG', *Neue Zeitschrift für Verwaltungsrecht*, Vol. 28, No. 21, pp. 1321-1328.

- Kornblum, T. (2011), *Rechtsschutz gegen geheimdienstliche Aktivitäten*, Berlin, Duncker & Humblot.
- Roggan, F. (2012), *G 10-Gesetz*, Baden-Baden: Nomos Verlag.
- Rosenbach, M. and Stark, H. (2014), *Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung*, München, Deutsche Verlags-Anstalt.
- Scheele, J. (2014), 'Verdachtslose Rasterfahndung des BND. Zehnjahresbilanz 2002-2012', *Bürgerrechte & Polizei/CILIP*, No. 105 (May 2014), pp. 34-43.
- Der Spiegel (2014), *Snowdens Deutschland-Akte*, 16 June 2014 (25/2014), English version available at: http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html.