

Policy Brief | Thorsten Wetzling | June 2017

---

# Germany's intelligence reform:

## More surveillance, modest restraints and inefficient controls



Think Tank at the intersection of technology and society

## Table of Contents

<b>Executive Summary</b>	<b>3</b>
<b>I. Overview</b>	<b>4</b>
a. Codified and uncodified surveillance powers	4
b. Important distinctions in German intelligence law	5
c. Oversight institutions and the surveillance authorization process	6
<b>II. Context on the BND-reform</b>	<b>8</b>
a. A compelling case for change	8
b. Driving factors	10
c. Summary	12
1. New rules for strategic foreign-foreign communications data surveillance	12
2. A separate authorization and control regime	15
3. Rules for international intelligence cooperation	15
4. New rules and institutions for parliamentary intelligence oversight	17
<b>III. Analysis</b>	<b>17</b>
a. The improvements in intelligence reform	17
b. The reform's contested privacy discrimination	18
c. Some of the reform's many deficiencies	19
d. The reform's important omissions	22
e. Open questions	23
<b>IV. Conclusion</b>	<b>24</b>
<b>Bibliography</b>	<b>26</b>



## Executive Summary\*

By December 2016, the most significant intelligence reform in recent German history was finally on the books.<sup>1</sup> It took more than a year of secret negotiations and a brief legislative process to codify important new rules about the practice, authorization and oversight of foreign data collection by the Bundesnachrichtendienst (BND), Germany's foreign intelligence agency.

The reform sets new international standards in regard to the authorization procedures now required for the surveillance of non-national data and the legal requirements for Germany's participation in international intelligence cooperation. For the first time, there now exists a distinction between German nationals, EU nationals, and the rest of the world when it comes to restrictions on signals intelligence (SIGINT). At least de jure, Germany now requires the authorization of almost all strategic surveillance measures by a panel of jurists. By contrast, recent reforms in the United Kingdom or the U.S. offer no such standard for non-national data.

Despite this, the reform still marks a clear victory for the Chancellery and the German security and intelligence establishment. They drove the reform and pushed the de jure expansion of the BND's digital powers through the legislature despite numerous and widely reported scandals such as the careless disclosure of German and European strategic interests to the Five Eyes intelligence alliance and the warrantless spying on citizens, EU partners and international organizations. The reform placed much of the BND's foreign communications data surveillance on a legal footing but did not fix the country's woefully inadequate judicial oversight system. If anything, the reform paved the way for further retreat of judicial oversight in Germany. Its investment in more parliamentary oversight is helpful but not a sufficient response to the astonishing breadth of intelligence governance deficits left unaddressed. While the reform's provisions on the targeting of fellow Europeans and international intelligence cooperation are important steps in the right direction, they are also too weak to actually rein in the German spymasters.

---

\*The author would like to thank Ben Scott and Stefan Heumann for their constructive criticism and valuable comments. The responsibility for the content lies solely with the author.

<sup>1</sup> The Bundestag amended both the foreign intelligence agency act (Gesetz über den Bundesnachrichtendienst, hereafter: BND Law) and the law on parliamentary intelligence oversight (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes). Unfortunately, since the reform there have been no official translations of both laws into English.

## I. Overview

This paper seeks to inform international readers about recent changes to German intelligence law. It depicts the political context of the reform followed by a brief summary of its main changes. Next, the paper elaborates on the reform's main achievements, its constitutionality and its substantial shortcomings. Thereafter, the focus turns to unresolved problems and open questions concerning the future practice of German foreign intelligence.

### a) Codified and uncodified surveillance powers

The text introduces a number of key concepts used in German signals intelligence law and briefly accounts for the country's main legislative framework and its basic intelligence oversight architecture.

The BND and the other 19 German intelligence services have a wide range of digital powers at their disposal.<sup>2</sup> Some powers are based in statute, while others are exercised by executive decree, i.e. without "the legal embodiment of the democratic will" (Born 2002: 17). Table 1 lists a few known powers that pertain to the interception of communications data.

**Table 1: Some of the BND's surveillance powers and their legal basis**

Surveillance of communications data of individual German citizens as well as residents and legal entities in Germany	Section 3 Art. 10 Law
Surveillance of communications data of foreign individuals on foreign territory	Not codified; secret executive decree
Strategic (untargeted) surveillance of communications data with either origin or destination in Germany	Section 5 Art. 10 Law
Strategic (untargeted) surveillance of communications data with neither origin nor destination in Germany	Art. 6 BND Law (2016 reform)
Computer Network Exploitation	Not codified; secret executive decree
Bulk Data Acquisition	Not codified; secret executive decree

The 2016 intelligence reform focused primarily on the practice of strategic surveillance (strategische Fernmeldeaufklärung). This term refers to the bundled collection of large quantities of communications data without concrete individual probable cause. It needs to be distinguished from surveillance measures that are directed at an individual suspect and his/her contacts.

Furthermore, German SIGINT law distinguishes between different types of strategic surveillance measures. Whereas the strategic surveillance of international telecommunication data to and from Germany has long been codified and subjected to judicial review, the strategic surveillance of

<sup>2</sup> Next to 16 intelligence services at the state level, Germany has two other federal intelligence services: the Bundesverfassungsschutz (domestic intelligence service) and the Militärischer Abschirmdienst (military intelligence).



international communications data that has both its origin and destination outside of Germany (Ausland-Ausland-Fernmeldeaufklärung) – up until recently – lacked a comparable legal framework.<sup>3</sup> For easier reference and comparison, Table 2 summarizes Germany's legal and oversight framework for strategic surveillance that existed prior to the 2016 reform, while Table 3 depicts the newly established framework. The following sections will discuss this in greater detail. It's sufficient to say here that German intelligence legislation consists of a "complicated, scattered, and imperfect set of rules" (Gärditz 2017: 421).

### **b. Important distinctions in German intelligence law**

An important norm to guide the practice and judicial oversight of surveillance by the intelligence services is Article 10 of the German Constitution (Basic Law). It guarantees the privacy of correspondence, post and telecommunications as a fundamental "right that protects the rights holder against tapping, monitoring and recording of telecommunication contents [...] the analysis of their contents and the use of the data thus gained" (Deutscher Bundestag 2015: 2). Article 10 of the Basic Law primarily obligates the state to refrain from interfering with privacy. When telecommunication is being monitored, "a deep intrusion into the fundamental right to privacy takes place. The infringement is particularly severe given that the imperative secrecy of these measures means that the targeted individuals are excluded from the authorization procedure" (ibid). Due to this, the German Constitution demands a clear legal basis for all such derogations. The Art. 10 Law provides the required legal basis for this. Established in 1968, it defines the cases and scope for the three federal intelligence services to engage in different forms of communication surveillance and sets the legal framework for judicial oversight.

Another statute discussed in this paper is the BND Law.<sup>4</sup> It provides the mandate for the BND and was substantially reformed in 2016 to include provisions on the practice, authorization and oversight of strategic foreign-foreign communications data surveillance as well as international SIGINT cooperation.

As shown by Tables 2 and 3, the authorization and oversight process for strategic surveillance in German intelligence law differs significantly depending on whether the surveillance measure are deemed to affect German citizens or not. Prominent constitutional scholars argued in 2014 that the BND's strategic foreign-foreign communications data surveillance practice infringes upon the right to private communication guaranteed by Art. 10 of the Basic Law. This right, they argued, protects not just German

---

<sup>3</sup> Notice also that the so-called foreign-foreign traffic may still be transitioning through German internet hubs and, consequently, accessed by Germany's foreign intelligence service on domestic territory.

<sup>4</sup> Other existing statutes such as the act on parliamentary intelligence oversight (PKGr Law) as well as the acts on the domestic and the military intelligence service and additional laws regulating to the vetting and classification procedures are of minor relevance for this paper.



citizens but every person. According to their view, neither nationality of the communicating participants nor country of residence are decisive criteria for the protection of civil rights (Bäcker 2014: 19). Rather, they argue, the key aspect is that German public authorities are bound by the provisions of the Basic Law at all times.

The German government and the 2016 reform did not adopt this position. Instead, the government argued that the right guaranteed by Article 10 of the Basic Law can be territorially restricted so as to protect only German citizens at home and abroad as well as residents and legal entities in Germany. This aspect as well as questions regarding the government's ability to distinguish clearly between national and non-national data and the effectiveness of its data minimization procedures will also be discussed later in the text.

### **c. Oversight institutions and the authorization process**

Important German institutions of intelligence oversight are the Bundestag's permanent intelligence oversight committee (Parlamentarisches Kontrollgremium - PKGr) and the Trust Committee (Vertrauensgremium). The former performs mainly ex post review of intelligence policy whereas the latter's sole task is budget control. The G10 Commission - a quasi-judicial body of the Bundestag - performs judicial oversight on communications interception by the federal intelligence agencies. In addition, the German Federal Data Protection Authority (BfDI) performs reviews on the handling of data by the federal intelligence services. With the 2016 reform, the oversight landscape grew with the addition of the Independent Committee (Unabhängiges Gremium). It is tasked with performing reviews of the BND's strategic foreign-foreign communications data surveillance as to its legality and necessity. In addition, the reform created the institution of a permanent intelligence oversight commissioner (Ständiger Bevollmächtigter) and further intelligence oversight staff within the Bundestag's administration.

The typical authorization process for strategic surveillance begins with the BND requesting permission to intercept communications data from either the German Interior Ministry (BMI)<sup>5</sup> or the Chancellery (Bundeskanzleramt, BKAmt).<sup>6</sup> The government then prepares surveillance orders and presents them to either the G10 Commission or the Independent Committee for judicial review, depending on the surveillance measure being sought. Following their legality and necessity assessment, the G10 Commission or the Independent Committee can then either accept these orders or call for their immediate termination.<sup>7</sup> Whether both commissions have sufficient mandates and resources to be effective in their review function will also be discussed in the sections below.

---

<sup>5</sup> For individual and strategic measures under Art. 10 Law.

<sup>6</sup> For strategic surveillance measures under the BND Law.

<sup>7</sup> See Section 15.6 Art. 10 Law for foreign-domestic strategic surveillance or Sections 9.4 or Sections 9.5 BND LAW for foreign-foreign strategic surveillance, respectively.



What can be said from the outset is that neither the G10 Commission nor the Independent Committee are judicial bodies sui generis. Thus, unlike in the U.S. or in Sweden, "German intelligence law does not entail a preventive judicial control, this blunt desideratum remains a gaping wound in the institutional body of the German intelligence architecture." (Gärditz 2017: 431).

**Table 2: Pre-reform framework for the BND's strategic surveillance**

Practice	Foreign-Domestic Strategic Surveillance (Strategische Fernmeldeaufklärung)	Foreign-Foreign Strategic Surveillance (Ausland-Ausland-Fernmeldeaufklärung)
Law	Section 5 Art. 10 Law	Section 2.1 BND Law and secret interpretations
Surveillance Orders	BND requests them through the Interior Ministry	unregulated
Review Body & Composition	G10 Commission (4 honorary members, 4 deputies)	Only executive control (if at all)
Warrants	Default standard: Ex ante authorization with full knowledge of search terms	n/a
Oversight Mandate	Legality & necessity review; can prompt immediate end of measures deemed unlawful or unnecessary	n/a
Investigation Powers	Full access to premises & documents	n/a
Effective Remedy Procedure	Default standard: Ex post notifications	n/a
Data Minimization	DAFIS Filter System	DAFIS Filter System
Quantity Restriction	20 percent rule in Section 10.4 Art.10 Law	None



**Table 3: Post-reform framework for the BND's strategic surveillance**

Practice	Foreign-Domestic Strategic Surveillance (Strategische Fernmeldeaufklärung)	Foreign-Foreign Strategic Surveillance (Ausland-Ausland-Fernmeldeaufklärung)
Law	Art. 10 Law	BND Law
Surveillance Orders	BND requests them through Interior Ministry	BND requests them through Chancellery
Review Body & Composition	G10 Commission (4 honorary members, 4 deputies)	Independent Committee (UG) (3 members, 3 deputies)
Characterization	Judicial oversight by quasi-judicial body	Restricted judicial oversight by administrative body
Review Sessions	Once a month	Once every three months
Warrants	Default standard: Ex ante authorization with full knowledge of search terms	Default standard: Ex ante authorization with limited knowledge of search terms
Oversight Mandate	G10 Commission can prompt immediate end of measures deemed unlawful or unnecessary	UG can prompt immediate end of measures deemed unlawful or unnecessary
Investigation Powers	Full access to premises & documents	Not specified.
Effective Remedy Procedure	Default standard: Ex post notifications	No notifications.
Data Minimization	DAFIS Filter System	DAFIS Filter System
Quantity Restriction	20% rule in Section 10.4 Art.10-Law	None

## II. Context on the BND-reform

### a. A compelling case for reform

The revelations by Edward Snowden resulting in the Bundestag's far-reaching intelligence inquiry provided the impetus for intelligence reform. The so-called NSA-inquiry brought to light major legal gaps, poor executive control and grave democratic deficits concerning the governance of signals intelligence in Germany. This has caused harm to German and European strategic interests and has led to unjustifiable spying on German and EU citizens, EU Member States and EU institutions as well as international organizations.





More specifically, it emerged in 2014 that Germany's foreign intelligence agency performed its single most important surveillance activity for decades without a clear legal framework, let alone independent authorization and oversight. The activity in question is the collection of communications data with its origin and destination outside of Germany (Ausland-Ausland-Fernmeldeaufklärung) – referred to in this paper as strategic foreign-foreign communications data surveillance.

It is estimated that this practice makes up to 90 percent of the BND's overall strategic surveillance activities (Löffelmann 2015: 1). Yet, despite being so important and despite regularly infringing upon the privacy rights of millions, German intelligence legislation lacked provisions concerning the authorization of collecting and handling of personal data. Instead, as shown in Table 2, prior to the 2016 reform, the BND intercepted, analyzed, stored and transferred most of its strategic surveillance data solely on the basis of a very broad provision in the BND Law and additional secret legal interpretations.<sup>8</sup> When questions regarding the legality of the BND's strategic foreign-foreign communications data surveillance became pressing in the NSA-inquiry, the government revealed a number of wide-ranging and underwhelming legal interpretations that it had used vis-à-vis the intelligence services and private companies.<sup>9</sup>

Prior to 2016, a significant part of Germany's SIGINT practices were also exempt from any form of independent oversight: No parliamentary oversight body, no judicial review commission and no data protection authority had any say on the BND's strategic foreign-foreign communications data surveillance. Instead, a very small circle within the executive single-handedly ordered the collection of data sets, with rights infringements numbering in the millions. The expenditure of public money notwithstanding, the BND's strategic surveillance practice had also never been independently evaluated for its effectiveness. Finally, the government has yet to show that it provides a sufficiently robust protection for data that is not meant to be subjected to strategic foreign-foreign communications surveillance.<sup>10</sup>

All these deficits emerged during the Bundestag's NSA-inquiry. As a result, the already tarnished public trust in the German security and intelligence

---

8 Prior to the 2016 reform, the German government justified the legality of the BND's foreign-foreign strategic surveillance practice with a broad provision in the BND Law according to which "the Federal Intelligence Service shall collect and analyze information required for obtaining foreign intelligence, which is of importance for the foreign and security policy of the Federal Republic of Germany" (Section 1.2).

9 For more information on these legal theories, including the so-called Weltraumtheorie (space theory), Funktionsträgertheorie (functionary theory), see (Biermann 2014; von Notz 2017).

10 Note that Section 6.4 of the BND Law explicitly excludes national data from strategic foreign-foreign surveillance. Due to widespread doubts on the technical feasibility to ensure this protection in practice, the NSA-inquiry committee summoned expert opinions from an IT-security Professor at the University of the Armed Forces and from the Chaos Computer Club. They elaborated on the accuracy of modern geolocation filtering and both reports indicate that a 100 per cent success may only be approximated. See the reports [https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten\\_ip\\_lokalisierung\\_rodosek.pdf](https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisierung_rodosek.pdf) and [www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf](http://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf)



establishment, the Bundestag's oversight mechanisms and the Chancellery's grip on executive control eroded even further.<sup>11</sup> To make things worse, Germany had also introduced a resolution at the United Nations for better privacy protection and intelligence oversight which, seen in conjecture with its own deficits in this realm, cast doubt on the credibility of Germany's foreign (cyber) policy at that time.

### **b. Driving factors**

Facing sustained negative media coverage and increasing pressure for legal certainty from within the services and the telecommunication sector, the government needed a suitable response to growing calls for a radical overhaul of the country's intelligence legislation and governance structures. Yet, powerful voices not just within the intelligence community constantly warned that, if anything, the security threats Germany faces have grown in severity and complexity. To them, it was essential that the BND's powers remained untouched or better yet that the BND received significantly more technical and human resources to professionalize its electronic surveillance practice.<sup>12</sup>

In the end, the key players within the Chancellery realized that it was wishful thinking to believe that they could get away with no reform. The intelligence sector's actions – on a weekly basis – illustrated that this storm would simply not pass. The German public had also become much more aware of the Chancellery's central role in the governance of signals intelligence. Given that there was hardly any regulatory framework, let alone public scrutiny regarding its role in the formulation of the National Intelligence Priority Framework (Aufgabenprofil BND), the authorization of foreign intelligence collection and international intelligence cooperation, the Chancellery may have also found it increasingly difficult to refer to them in public without any reform.

In May 2014, three of the country's most renowned constitutional experts publicly rebuked the government's argument that the BND Law provided a sufficient legal basis for the BND's foreign intelligence collection practice. This aggravated existing concerns among members of the intelligence and security sector and national telecommunication providers. Upset by the legal limbo and out of genuine fear for litigation they pushed hard for a modern legal basis for the BND's surveillance powers. Different cases brought to the constitutional and administrative courts by ISP providers, the G10 Commission, the opposition parties within the inquiry committee as well as several NGOs may have also propelled the Chancellery to seek a reform

---

<sup>11</sup> In every single legislative period over the last decade, the Bundestag established an ad hoc inquiry into allegations of intelligence governance malfeasance. While those proceedings were doubtlessly politicized, they did provide enough material to show that the permanent intelligence oversight mechanisms were neither sufficient nor fit for purpose (Wetzling 2016a).

<sup>12</sup> Their lobbying was strong and briefly put the entire reform effort on halt in the spring of 2016. <https://www.welt.de/politik/deutschland/article153455819/Kanzleramt-legt-BND-Reform-vorerst-auf-Eis.html>



prior to the next federal election and the conclusion of the parliamentary investigation in 2017.<sup>13</sup>

When the Chancellery publicly acknowledged “operational deficits” in the BND’s foreign intelligence collection programs,<sup>14</sup> it became clear that an intelligence reform had to be prepared. The following minimal consensus quickly emerged among the ruling government coalition in the Bundestag: The BND’s mandate needed an update; future data collection on European partners ought to be limited; and intelligence oversight was currently not fit for purpose.

However, actual recommendations on how to reverse engineer an established signals intelligence machinery so as to better accommodate human rights, oversight and accountability standards were in very short supply. The press and the Bundestag were primarily concerned with the ongoing investigation of past malfeasances and the reporting on the BND’s methods. This created a vacuum that the Chancellery took advantage of. It became the real driver behind intelligence reform, albeit operating from quite a different vantage point. From the fall of 2015 onward, a small circle of key players within the Chancellery, the BND, the German foreign, interior and justice ministries as well as a handful of members of parliament and their key advisors worked behind closed doors on the new rules for the BND and its overseers.

Unlike in the UK or in the Netherlands, the German government kept the matter very close to its chest and did not allow any form of pre-legislative scrutiny. The draft bill was presented to parliament on the day before its summer recess in July 2016. A public hearing followed where seven experts made a whole range of recommendations on how to improve the envisaged changes to the BND Law (Deutscher Bundestag 2016). Those recommendations had virtually no effect on the majority of the lawmakers. In October 2016, the Bundestag and the Bundesrat (the Federal Council) adopted the bills without any significant changes.

While the reform entered into force in December 2016, it will take time for the new institutions to become fully operational.<sup>15</sup>

---

13 A detailed review of each of those cases goes beyond the scope of this paper. The biggest internet hub in Germany (DE-Cix) sued the government in a pending case over the legality of surveillance orders. The G10 Commission lost a case against the government for access to the so-called NSA-selectors. The qualified minority lost a case against the government on an access to information request. NGOs such as Reporters without Borders, Amnesty International and Gesellschaft für Freiheitsrechte have also sued the government over the constitutionality of its surveillance practices.

14 The government referred to “technical and organizational deficits at the BND that the Chancellery identified as part of its executive control” (Frankfurter Allgemeine Zeitung, 23.04.2015). Given that the Chancellery failed to provide clear briefing for SIGINT staffers on German strategic interests and the risks of too credulous intelligence cooperation, a more critical self-assessment of executive control would have been in order, too.

15 At the time of writing this has not been achieved and important positions have yet to be filled. For example, the new secretariat of the parliamentary intelligence oversight body (PK1-Bundestagsverwaltung) has yet to appear on the organization chart of the Bundestag administration and new positions (e.g. Leitender Beamter, Section 12.1 PKrG Law) have yet to be filled.



### **c. Summary**

The 2016 reform introduced a number of significant changes to existing German intelligence law. The summary below focuses on aspects deemed particularly relevant for international readers.<sup>16</sup>

#### **1. New rules for strategic foreign-foreign communications data surveillance**

The BND Law now includes several new provisions on the authorization, collection, handling, transfer and oversight of strategic foreign-foreign communications data surveillance (Ausland-Ausland-Fernmeldeaufklärung). In so doing, Germany sets an important new international standard.

Next to specifying the BND's mandate to intercept such data from within Germany (for transitioning traffic) it now also includes a provision on the use of such data that the BND obtained abroad (Section 7). The main takeaways from the new rules in Section 6-18 are:

**Unrestricted metadata collection.** The BND's collection of metadata by means of strategic foreign-foreign communications data surveillance remains unrestricted. The retention of metadata is limited to six months. By contrast, content data may be retained for up to 10 years.<sup>17</sup>

**Unrestricted acquisition and restricted collection of content data.** As before, the BND will continue to acquire raw data without any de jure restrictions when intercepting foreign-foreign communications data in bulk. However, Section 6.2 now obligates the foreign service to use search terms when operationalizing ("collecting") content data from its data pool.<sup>18</sup> Yet, the law defines neither "search term" nor "telecommunication nets" any further. Obviously, this leaves significant operational latitude for the intelligence community. In addition, Section 12 (Eignungsprüfung) provides for an important exception to the general search term provision. "Telecommunication nets," according to this rule, may be temporarily tested in order to assess the quality of their output and to generate new search terms.

---

<sup>16</sup> See (Deutscher Bundestag 2016) for a comprehensive list of individual expert reports on the draft BND-reform.

<sup>17</sup> Section 20.1 BNDG in conjunction with Section 12 BVerfSchG.

<sup>18</sup> Unless otherwise indicated, all references to sections in this text refer to the BND Law.



**New content data protection hierarchy.** In regard to the collection of content, the BND law distinguishes between four different groups for which different authorization procedures, data protection standards and oversight provisions apply. In terms of prioritization, these groups are:

- **Beneficiaries of G10 protection** (i.e. German nationals, domestic legal entities and persons on German territory):<sup>19</sup> The amended BND law stipulates that the collection of content- and metadata from this group by means of strategic foreign-foreign communications data surveillance is not permissible (Section 6.4). Any electronic surveillance on this group is subject to the provisions of the Art. 10 Law which entails stricter rules for the authorization, handling, judicial oversight as well as notification procedures.
- **Public institutions of the European Union and its Member States:** The use of selectors that target public bodies of EU member states or EU institutions is restricted to 12 warranted cases and requires orders that mention the individual search terms (Section 9.2).
- **EU citizens:** The use of selectors that target EU citizens is restricted to 21 warranted cases. Interception orders are not required to mention the individual search terms (Section 9.2).
- **Non-EU data:** The least restrictive regime governs the steering of search terms that aim at non-EU data. This is justifiable (a) to identify and respond to threats to Germany's domestic and external security; (b) maintain Germany's capacity to act and (c) other information relating to the government's secret national intelligence priority framework (Aufgabenprofil). The strategic foreign-foreign communication data surveillance must be administered on "telecommunication nets" the Chancellery identified in its interception orders. There is no requirement for search terms to be listed in such orders.

---

<sup>19</sup> See (Graulich 2017:49).



**Table 4: Authorization criteria for targets of the BND's strategic surveillance<sup>20</sup>**

<b>Group A</b> German citizens at home & abroad, all persons on German territory and domestic legal entities	<b>Group B</b> Public institutions of EU-Bodies & Member States	<b>Group C</b> EU citizens	<b>Group D</b> Rest of the world
<p>This group may not be subjected to strategic surveillance of foreign-foreign communications data.</p> <p>Any surveillance must be done in accordance with Art. 10 Law. (Except for incidental collection)</p>	<p>Group B may be targeted. This requires collection order that must identify search terms.</p> <p>Search terms may only be used if necessary for information related to 11 + 1 warranted cases:</p> <p>eight circumstances under Section 5.1 Art.10-Law</p> <p>+</p> <p>three broad justifications (Section 6.1 BND Law) if needed for third country information of particular relevance to Germany's security.</p> <p>+</p> <p>data collection under Section 12 BND Law</p>	<p>Group C may be targeted. Requires collection order but no need to mention search terms therein.</p> <p>Search terms may only be used if necessary for information related to 20 + 1 warranted cases:</p> <p>eight circumstances under Section 5.1 Art.10-Law</p> <p>+</p> <p>three broad justifications (Section 6.1 BND Law) if needed for third country information of particular relevance to Germany's security.</p> <p>+</p> <p>nine justifications under Section 3.1 Art. 10-Law</p> <p>+</p> <p>data collection under Section 12 BND Law</p>	<p>Group D may be targeted. Requires collection order but no need to mention search terms therein.</p> <p>Search terms can be used if necessary for information related to 3 + 1 very broad broad warranted cases</p> <p>three broad justifications (Section 6.1 BND Law) without the third country relevance caveat</p> <p>+</p> <p>data collection under Section 12</p>
<p>G10 judicial oversight &amp; general notification requirement to allow effective remedy.</p>	<p>Ex ante authorization with knowledge of search terms &amp; Chancellery notification requirement</p> <p>No notifications to surveillance targets.</p>	<p>Ex ante authorization without knowledge of search terms.</p> <p>No notifications to surveillance targets.</p>	<p>Ex ante authorization without knowledge of search terms</p> <p>No notifications to surveillance targets.</p>

<sup>20</sup> Note: The purely "foreign" strategic surveillance practice by the BND, i.e. the collection of foreigners' data on foreign soil remains unregulated. This will be further explained in the analysis part.



**Table 5: Different justifications for strategic surveillance measures in German intelligence law**

<p><b>Three warranted cases of Section 6.1 BND Law</b></p> <ul style="list-style-type: none"> <li>• Risks to the internal or external security of the Federal Republic of Germany;</li> <li>• Germany's ability to act;</li> <li>• Information on developments of foreign and security policy significance that relate to the National Intelligence Priority Framework</li> </ul>
<p><b>Eight warranted cases of Section 5.1 Art. 10 Law</b></p> <ul style="list-style-type: none"> <li>• An armed attack against the nation</li> <li>• Intent to carry out acts of international terror</li> <li>• International proliferation of military weapons</li> <li>• Illegal import or sale of narcotics</li> <li>• Counterfeiting</li> <li>• International money laundering</li> <li>• Smuggling or trafficking of individuals</li> <li>• The international criminal, terrorist or state attack by means of malicious programs on the confidentiality, integrity or availability of IT systems</li> </ul>
<p><b>Nine warranted cases of Section 3.1 Art. 10 Law</b></p> <ul style="list-style-type: none"> <li>• Crimes of treason</li> <li>• Crimes that are a threat to the democratic state</li> <li>• Crimes that threaten external security</li> <li>• Crimes against national defense</li> <li>• Crimes against the security of NATO troops stationed in the Federal Republic of Germany</li> <li>• Crimes against the free democratic order as well as the existence or the security of the country.</li> <li>• Crimes under the Residence Act</li> <li>• Crimes under Sections 202a, 202b and 303a, 303b of the Criminal Code, in so far as they are directed against the internal or external security of the Federal Republic of Germany, in particular against security sensitive bodies of vital institutions</li> <li>• Crimes under Section 13 of the Criminal Code</li> </ul>

**Ban on economic espionage.** The BND Law introduced an explicit ban on the use of foreign-foreign communication surveillance for the purpose of economic espionage. It does not, however, define economic espionage or provide a list of practices that could be categorized as such.

**2. A separate authorization and oversight regime.** The reform created the Independent Committee (Unabhängiges Gremium - UG), a second German authorization body for strategic surveillance. Situated at the Federal Court of Justice in Karlsruhe, the UG provides ex ante authorization of strategic foreign-foreign communications data surveillance by the BND. It consists of three members plus three deputies. Its president and one member must be judges at the Federal Court of Justice. The third member must be a federal public prosecutor at that court. The executive appoints the members of the Independent Committee (Section 16.2). It meets at least every three months and has the power to induce the immediate end to measures it finds unlawful or unnecessary.

**3. Rules for international intelligence cooperation.** In regard to SIGINT cooperation between the BND and its foreign intelligence partners, the



BND Law now contains a number of provisions that are also outstanding by international comparison. Sections 13-15 mark the first specific provisions on international intelligence cooperation in German intelligence law.

- **Section 13.3** states that any new cooperation between the BND and foreign intelligence partners requires a prior written administrative agreement on the aims, the nature and the duration of the cooperation. This also includes an appropriations clause that the data may only be used for the purpose it was collected and that the use of the data must respect fundamental rule of law principles. Agreements also require a consultation among the foreign cooperation partners to comply with a data deletion request by the BND.
- **Section 13.4** defines seven broad permissible aims for new international SIGINT cooperation involving the BND. These include 'information on political, economic or military developments abroad that are relevant for foreign and security' to 'comparable cases'. SIGINT cooperation agreements with EU, EFTA and NATO partners require the approval of the Chancellery. Agreements with other countries require approval by the head of the Chancellery. The executive is required to inform the parliamentary intelligence oversight body about all such agreements.
- **Sections 26-30** introduce new provisions on SIGINT databases. The BND can run joint databases (Section 27) or contribute to foreign-run databases (Section 30). The BND's cooperation with foreign partners on databases is only permissible when (a) deemed particularly relevant for Germany's foreign and security interests; (b) basic rule of law principles are being upheld within partnering states (c) if all partners agree to honor the reciprocity principle (Section 26.2). The Chancellery's authorization and parliamentary oversight notification obligations are the same as those for the SIGINT cooperation agreements. There is a similar requirement that the aims and forms of cooperation on joint databases are documented in writing form to the operation.
- **Section 28** further requires that the BND must keep a detailed separate file arrangement documentation for each database it uses with foreign intelligence partners and for which it is in charge. The German Federal Data Protection Authority (BfDI) must be consulted prior to the installation of a new database file arrangement. It may review the creation of new databases by the BND as well as the data that the BND contributes to joint databases.

**4. New rules and institutions for parliamentary intelligence oversight.** The





reform also introduces significant changes to the law on and future practice of parliamentary intelligence oversight (PKGr Law). Most notably:

- It created the new institution of a permanent intelligence oversight coordinator. As the nine members of the parliamentary intelligence oversight committee often lack the time, resources and knowledge to perform their important mandate, the coordinator can now perform investigations on their behalf. He or she can also be tasked for additional budget control by the Bundestag's Trust Committee. The coordinator prepares the public reports by the intelligence oversight body and takes part in the monthly G10-sessions, the meetings of the parliamentary oversight body and the Trust Committee.
- It further clarified the reporting obligations of the executive. It has to report on the general activities of the three federal intelligence services but also on developments of particular relevance. The amended law now provides three examples for the latter: (a) notable changes to Germany's foreign and domestic security situation; (b) internal administrative developments with substantial ramifications for the pursuit of the services' mandate and (c) singular events that are subject to political discussions or public reporting (Section 4.1 PKGr Law).
- The reform will also create more than a dozen full-time positions for intelligence oversight within the Bundestag's administration. As of yet, these positions have not been filled and there is little information on what is planned for them in the future.

### III. Analysis

The following section provides a critical analysis of Germany's recent intelligence reform. The discussion begins with what the author sees as true improvements in the reform. Especially, when compared to recent surveillance reforms in other countries, Germany's expansion of the authorization procedure to non-national data and its new requirements for SIGINT cooperation stand out as progressive.

#### a. The improvements in intelligence reform

**Democratic legitimacy for a key SIGINT practice.** The reform now provides a specific legal footing for a significant part of the BND's SIGINT activities. Given the magnitude of past deficits and the ubiquitous calls for a better legal framework, this may not seem like a major achievement. Yet despite the reform's many shortcomings, it is a fact that many European countries, let alone nations throughout the world, operate according to intelligence laws that do not contain detailed provisions on the practice of strategic communications data surveillance, let alone restrictions and democratic



oversight on the collection of foreigners' data by national intelligence services.<sup>21</sup> At the very least, by means of this reform, the German parliament has now democratically legitimized almost the entire practice of the BND's strategic communications data surveillance.

**Measures' legality and necessity can be challenged.** Furthermore, the reform provides ex ante authorization and some ex post control provisions. Thus, de jure, the reform offers the possibility to challenge these measures on grounds of legality or necessity by jurists that are not bound by instructions from the executive.

**Rules on international intelligence cooperation.** By international comparison, the reform includes detailed provisions governing the BND's future SIGINT cooperation with foreign intelligence partners. The BND leadership must seek written agreements from foreign partners covering a number of aspects that, by and large, aim to restrict the BND's participation in measures that would be deemed unlawful if performed solely under German jurisdiction. Moreover, next to attaching a number of broad conditions to future SIGINT cooperation agreements, the reform also introduces specific rules on joint databases, particularly those run by the BND. For the latter, the German Federal Data Protection Authority's review mandate covers all the data that the BND contributes to joint databases with foreign partners.

**New ministerial responsibilities.** The reformed BND Law now requires more documentation for individual decisions and includes a number of accountability provisions for the Chancellery's or – as the case may require – the Head of the Chancellery's steering of SIGINT measures. For example, future interception orders must refer to telecommunication nets determined by the Chancellery. The use of selectors targeting EU institutions or EU Member States requires prior notification of the Chancellery and new SIGINT agreements as well as the maintenance of joint databases must be approved by the Chancellery. These and other provisions further reduce the risk of plausible deniability by the executive vis-à-vis its foreign service.

#### **b. The reform's contested privacy discrimination**

The reform of the BND Law is based on the premise that the right to private communication as guaranteed in the German constitution (Art. 10 of the Basic Law) can be territorially restricted so as to protect only German citizens at home and abroad, residents and domestic legal entities in Germany. In other words, the reform presumes that the privacy infringements for non-Germans caused by these surveillance measures can be administered with significantly less safeguards compared to those afforded to Germans (See Table 4 above).

The constitutionality of this restricted interpretation of Art. 10 Basic Law

---

<sup>21</sup> For a good overview, see the comparative study on European SIGINT laws by the European Fundamental Rights Agency: Surveillance by Intelligence Services: fundamental rights safeguards and remedies in the EU, November 2015. <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services>



is highly contested and has yet to be answered by the Constitutional Court. Clearly, the drafters of the intelligence reform took a significant risk: In case their interpretation of the limited territorial reach of Art. 10 of the Basic Law fails to convince the Constitutional Court, they will have to revise almost the entire 2016 reform. This is because the reform and its explanatory memorandum carefully avoid any specific reference to Art. 10 of the Basic Law as well as to the existing regime for the authorization and judicial oversight of strategic surveillance (Art. 10 Law).

Instead of adding new rules for strategic foreign-foreign communications data surveillance into the existing Art. 10 Law and instead of strengthening the G10 Commission's mandate, the government created a whole new parallel legal and oversight framework with the amendments to the BND Law. The ensuing discrimination against privacy protections and the fragmentation of the German oversight landscape could have been avoided. It would have been possible to extend the basic right to private communication under Art. 10 of the German Constitution to foreigners abroad without necessarily extending the ex post notification practice to them. But this would have come at the cost of extending the territorial reach of Art. 10 and this was an option the government tried to avoid at all costs.

Whereas the German Constitutional Court has not equivocally positioned itself on the territorial reach of Art. 10 Basic Law question in the past, it will soon have to take a stance. Litigation is currently being prepared by the Society for Civil Rights (Gesellschaft für Freiheitsrechte, GFF) that will require a definite position by the court.

### **c. Some of the reform's many deficiencies**

**Insufficient Judicial Oversight.** The reform created a second authorization body for strategic communications data surveillance by the BND. Despite being staffed by professional jurists and its proximity to the Federal Court of Justice in Karlsruhe, the Independent Committee (UG) is neither independent nor a court. Not only are its three members and deputies appointed by the executive, one of the three members will also be a public prosecutor from the Federal Public Prosecutor's Office. This is problematic for potential conflicts of interest. Instead, it may be referred to as an administrative body tasked with the ex ante authorization of the newly codified surveillance measures.

While the BND-reform created the UG, the new provisions say very little on its actual oversight powers. By comparison, the G10 commission is not only tasked to authorize surveillance measures but it also has the authority to review the collection, subsequent data handling and use of all personal data related to the surveillance measures. In order to do so, the G10 Commission has guaranteed access to all documents, saved data and data management programs used in conjunction with surveillance measures as well as access to any premises used for SIGINT purposes by all three federal intelligence



agencies (Section 15.5 Art. 10 Law). By contrast, the BND Law makes no mention of such judicial oversight powers for the UG. Clearly, the UG is not meant to engage in any in-depth judicial oversight. Interestingly, however, the law does grant the UG the authority to conduct random checks whether the search terms used by the BND for the targeting of EU-data corresponds to the restrictions articulated in Section 6.3.

Apart from the missing provisions on the UG's actual oversight powers, one can also express serious concerns regarding the authorization procedure. More specifically, when the UG assesses the legality and necessity of a surveillance measure it may do so on the basis of interception orders that do not list the search terms. Any legality and necessity assessment it makes without knowledge of the search terms is likely to lack credibility and substance.

**Further fragmentation of German intelligence oversight system.** Instead of streamlining the existing oversight landscape, the reform has fragmented it further. Next to the Trust Committee (budget oversight), the permanent parliamentary oversight body, the G10 Commission and the Federal Data Protection Authority, democratic intelligence oversight will now also be administered by two new institutions: the Independent Committee and the Parliamentary Oversight Commissioner. As indicated, the fact that Germany now hosts two separate authorization bodies for strategic surveillance – one in Berlin (G10 Commission) and one in Karlsruhe (UG) – can only be explained when seen as a corollary to the government's position on the restricted territorial reach of Art. 10 of the Basic Law. It would have made much more sense to just extend the mandate of the existing G10 Commission. However, not only did the G10 Commission show its own deficits (see next section), it had also displayed a newly-acquired audacity to publicly challenge the government.<sup>22</sup>

While the reform has introduced limited measures to facilitate the exchange of information among oversight bodies – for example, the oversight commissioner's right to attend the different meetings of the Trust Committee, the parliamentary oversight body and the G10 Commission – many members still refer to their respective institutions as silos. Individual members of the G10 Commission are not regularly in touch with the members of the parliamentary oversight body and the reform has not foreseen any specific exchange between the Independent Committee and the G10 Commission. Given the similarity of interception orders and the similar role of telecommunication providers compelled to assist the government, it would certainly be useful for both bodies to be more systematically aligned, possibly even conducting joint assessments and visits on the premises of the foreign service.

**Soft restrictions.** As previously shown, the new provisions in the BND Law

---

<sup>22</sup> In October 2015, the G10 Commission sued the government over access to NSA-selectors. Irrespective of the merits of this unsuccessful case for the G10 Commission, it is safe to assume that the very fact that the Commission turned to the Constitutional Court has tarnished the Chancellery's trust in the Commission's four honorary fellows.



use unduly broad definitions when regulating aspects that are meant to restrict surveillance. For example, consider the minimal requirements for search terms used to collect information on non-EU data (Section 6.1) or the list of permissible goals for new international SIGINT cooperation agreements (Section 13.4). What, one may ask, falls under information required to secure the Federal Republic's capacity to act (Section 6.1) or what defines 'comparable cases' that may give rise to new international SIGINT cooperation (Section 13.4)? Also, the rules on future international SIGINT cooperation agreement need only be unilaterally declared once at the beginning. Follow-up procedures to monitor the adherence to those rules have not been foreseen.

Equally concerning is the fact that the law provides no restrictions on the extensiveness regarding the acquisition of data from "telecommunication nets" (Section 6.1). Hence, Germany's foreign service may acquire as much raw data as it likes or its resources allow. Compare this, for example, with Section 10.4 Art. 10-Law which stipulates that interception orders for strategic communication that may also target national data must identify the geographical area for which information is being sought and also the communication channels (transmission paths). Furthermore, for any strategic surveillance on foreign-domestic communication there is the requirement that the data subjected to surveillance must not exceed 20 percent of the overall capacity of the communication channels identified in the order (Section 5 Art-10-Law).<sup>23</sup>

The BND Law also does not clarify what may be defined as "search term" and how these terms may be used in practice. It may be understandable that an intelligence law does not provide detailed information on operational procedures which can also rapidly change over time, the mere reference to "search term" does provide ample latitude for the intelligence sector to use the most powerful regular expressions, especially if oversight and review bodies lack the knowledge and resources to review the use of regular expressions in surveillance programs.

**Abstract notification requirements instead of more transparency.** Consider briefly the U.S. government's Implementation Plan for the Principles for Intelligence Transparency and its various accompanying measures that seek to make "information publicly available in a manner that enhances public understanding of intelligence activities".<sup>24</sup> For example, a Tumblr site (IC on the Record) features among other declassified documents dozens of orders and opinions by the U.S. Foreign Intelligence Surveillance Court (FISC) – the rough equivalent of Germany's quasi-judicial G10-Commission. In Germany, the G10 Commission itself has no reporting obligations. Instead,

---

<sup>23</sup> This particular provision stems from the pre-digital era and is highly problematic and amenable to frequent abuse. See (Wetzling 2016) for a further elaboration. Given that the reform stayed clear from any changes to the existing Art. 10 Law, this problem remains.

<sup>24</sup> Implementation Plan for the Principles for Intelligence Transparency. Available at <https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf>



the parliamentary intelligence oversight body reports annually to the German Parliament on the measures performed in conjunction with the Art. 10 Law. Those reports are public but they only provide rudimentary factual information about G10 authorizations rather than the Commission's underlying decisions and interpretations of the law. For example, the 2015 G10 report states that in regard to the steering of search terms per threat category per six months, the G10 Commission authorized 949 search terms that fall into the category of "international terrorism."<sup>25</sup>

In regard to the foreign surveillance measures codified in the amended BND Law, Section 16.6 only requires that the Independent Committee informs the parliamentary oversight body about its work at least every six months. There are no further requirements in the law about the content and format, let alone public documentation of such reporting.

#### **d. The reform's important omissions**

**No overhaul for the opaque German intelligence legislation.** German intelligence law remains a mess. It consists of numerous individual pieces of legislation that are rarely straightforward and a challenge even to experienced lawyers. The recent intelligence reform offered a chance to design a comprehensive, modern intelligence law from scratch but that was never seriously considered. The second-best option would have been to insert the new provisions on strategic foreign-foreign communications data surveillance into the existing law on the authorization and judicial oversight of strategic surveillance. For the reasons outline above, this was politically inopportune and therefore carefully avoided. The fact that the actual reform further fragmented the oversight landscape and has rendered the body of German intelligence legislation even less comprehensible has caused little concern.

**No reform of the G10 Commission.** Worse still, this also meant that the numerous legal and institutional deficits that exist with the system for the authorization and judicial oversight of strategic surveillance as regulated for in the Art. 10 Law were left unaddressed by the reform. For example, the G10 Commission (a) still lacks sufficient resources and does not review the handling of data by the intelligence services, (b) remains staffed by four honorary fellows who come together only once a month to authorize a stack of inception orders; (c) still operates without adversarial proceedings (i.e. there is no-one within the commission to present the views of those subjected to surveillance and argue for less infringing measures) and; (d) the abuse-prone and anachronistic rule that restricts the collection of foreign-domestic surveillance data to a maximum of 20 percent of the capacity of the pertinent communication channels also remained in place.<sup>26</sup>

**Other bulk powers not legislated for.** Despite all the valid criticism that the

---

<sup>25</sup> See the 2015 Annual G10 Report by the Parliamentary Intelligence Oversight Body.

<sup>26</sup> See Wetzling 2016 for further elaboration on those deficits.



British intelligence reform received, Westminster did legislate for other bulk powers. By contrast, the BND Law says nothing about the foreign service's hacking powers (Computer Network Exploitation). The BND's acquisition of existing databases from the commercial sector also remain unlegislated. Furthermore, German intelligence law continues to leave the so-called 'reine Auslandsaufklärung', i.e. the BND's strategic surveillance against foreigners on foreign soil without any search term requirements, unregulated (Graulich 2017: 47).

**Effectiveness of strategic surveillance still not assessed.** Do these privacy infringements numbering in the millions actually pay off and offer a concrete security gain? Unfortunately, despite such calls by the Chancellor's coalition partner,<sup>27</sup> the reform did not establish an independent evaluation procedure so as to assess the effectiveness of strategic surveillance and the accuracy of the data minimization programs. Thus, the following two important claims cannot be verified: (1) This huge surveillance infrastructure that was built and operationalized in the shadows of democratic oversight produces actionable intelligence and; (2) our agents only get to see lawfully collected data. The current oversight institutions lack the mandate and the IT-resources to perform any such evaluation. Parliamentarians lack the imagination and the political will to use their legislative and budgetary powers to close this pressing gap. Next to the American example where the Presidential Civil Liberties Oversight Board (PCLOB) performed effectiveness investigations, consider also the Dutch independent oversight board CTIVD. It has recently announced a new project to review "the possibilities of systemic oversight on the acquisition, analysis and deletion of large amounts of data."<sup>28</sup>

**No limit to metadata collection.** A draft version of the BND bill was at one point circulated which included restrictions on the collection, use and transfer of metadata within the framework of strategic foreign-foreign communications data collection. Yet, these restrictions were removed from the bill presented to parliament. Given the importance of metadata for modern surveillance and warfare, and given that metadata by itself is enough to construct highly accurate personal profiles, it is regrettable that the reform did not introduce any limits on the BND here.

#### e. Open questions

**Sufficient technical prowess to curb incidental collection?** The reform assumes the BND's technical prowess great enough to neatly distinguish between different data groups for which different authorization and oversight regimes apply. Yet the tools used for modern communication and its transmission defy coarse categorization. This brings up the question of data minimization. The BND uses the same automated filter program (DAFIS) to sift through the acquired raw data. Even if – and without the effectiveness

<sup>27</sup> Eckpunktepapier SPD Party (June 2015), available online: [http://www.spdfraktion.de/system/files/documents/2015-06-16-eckpunkte\\_reform\\_strafma-r-endfassung.pdf](http://www.spdfraktion.de/system/files/documents/2015-06-16-eckpunkte_reform_strafma-r-endfassung.pdf)

<sup>28</sup> For an English translation of this announcement, see: <https://blog.cyberwar.nl/2017/04/dutch-review-committee-on-the-intelligence-security-services-ctivd-to-self-assess-effectiveness-of-lawfulness-oversight-re-large-scale-data-intensive-a/>

review mentioned above this is pure guesswork – the filter does reach an accuracy level of 98.5 percent this would still mean that the BND incidentally collects, uses and transfers thousands of datasets daily without respecting the law that requires G10 protections and notifications.<sup>29</sup>

Interestingly, Section 10.4 already alludes to incidental collection of content and metadata and requires the immediate deletion of wrongfully obtained data or the notification of the G10 Commission in case the data will be retained. Here the drafters used a somewhat twisted logic: In the pursuit of strategic foreign-foreign communications data collection, the BND must not collect data from German citizens at home or abroad, residents or legal German entities (Section 6.4). If it does (Section 10.4) it must delete that data or inform the G10 Commission if it retains that data. With filters working to 100 percent, there would be no need for this. Given that it will continue to happen, it adds – at least de jure – significantly to the workload of the understaffed G10 Commission. The following table summarizes the wide range of shortcomings with the recent German intelligence reform discussed in the previous section.

**Table 6: Selection of post foreign intelligence reform deficits in Germany**

Insufficient judicial oversight powers and resources	Further fragmentation of the intelligence oversight architecture	Weak restrictions on surveillance	Lack of transparency and abstract reporting requirements	No adversarial proceedings at either G10 Commission or the UG
Severe deficits with the implementation of Art. 10 Law remain unaddressed	Many other surveillance powers remain unlegislated	No independent evaluation of the effectiveness of foreign surveillance tools	Unlimited metadata collection for measures under the BND Law	Significant amount of incidental Collection due to filter inaccuracies

#### IV. Conclusion

Democracies need strong and agile security services to guard against a number of increasingly networked threats. International cooperation among national intelligence services is fundamentally important for our security. Yet, given the invasiveness of modern surveillance, intelligence services ought to be subjected to effective democratic oversight. This promotes rights-based and legitimate intelligence governance that is vital to the social fabric of any democracy.

By and large, Germany's recent intelligence reform did not pave the way toward meeting this important objective. It was designed, first and foremost,

<sup>29</sup> By way of comparison, take a hypothetical scenario discussed in (Martin, 2017): In 2015, the data volume carried only be broadband connection in Germany amounted to roughly 11.500 million gigabyte. If only five percent of this data would not be properly filtered that would mean that 575 million gigabyte of data would not be subject to proper data minimization. A standard article like this one may amount to 0.00005 gigabyte. Put differently, and referring still to the hypothetical example, 11 trillion and 500 billion data set would not be subjected to proper data protection standards required by law.





to provide legal certainty for intelligence service members and private companies involved in pursuit of strategic surveillance.

Legal clarity and the rule of law were not the key objectives of this reform. In fact, the reform created a number of new problems and left major deficits unresolved. Judicial oversight of intelligence, which in theory is the most useful tool to rein in rogue elements given its concrete and immediate sanctioning power, has been hollowed out with this reform. Just take the new Independent Committee as an example. With its creation and the missed opportunity to address the grave deficits of the G10 Commission, the reform unduly fragmented the German oversight landscape and contributed to the retreat of judicial intelligence control. A more fragmented, albeit more resourceful, system of parliamentary intelligence oversight is hardly the appropriate response to Germany's problems with intelligence governance. The reform also did not address the urgent need to provide for an independent evaluation of the effectiveness of the many surveillance programs either. Besides, many key questions surrounding the use of data gained from strategic surveillance remain within the sole and unchecked responsibility of the executive. Despite being in effect since December 2016, the reform is also far from being fully implemented at the time of writing.<sup>30</sup>

However, especially with a view to recent intelligence reform in other countries, Germany's reform has also set a few benchmarks that deserve further recognition. Its intelligence laws now cover a far greater spectrum of SIGINT activities than ever before. The required authorization of foreign-foreign surveillance programs by a panel of jurists also sets a new international standard. By comparison, the U.S. FISA Court only reviews surveillance programs that impact US-nationals.<sup>31</sup> While the terms used to restrict surveillance on non-nationals are vague and the actual investigation powers of the Independent Committee unclear, the BND Law – unlike other European intelligence laws – does give special protection to EU citizens. Also in regard to the new requirements for international intelligence cooperation, Germany has gone further with its reform than many other democracies. The reform brought new documentation and authorization requirements for the executive which may lead to more political accountability, a core problem identified by all intelligence inquiries in Germany over the past decade.

## Bibliography

---

30 For example, the new secretariat of the parliamentary intelligence oversight body (PK1-Bundestagsverwaltung) has yet to appear on the organization chart of the Bundestag administration and new positions (e.g. Leitender Beamter, Section 12.1 PKrG Law) have yet to be filled.

31 To be fair, the U.S. Privacy and Civil Liberties Board (PCLOB) – currently operating its important business with only one member – may also make recommendations designed to protect the rights for non-U.S. persons.



- Bäcker, Matthias. 2014. Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses. 22. Mai 2014. Available at [www.bundestag.de](http://www.bundestag.de).
- Biermann, Kai. 2014. Die Anarchos vom BND. Commentary for Zeit Online. Available at <http://www.zeit.de/politik/deutschland/2014-11/bnd-bundesnachrichtendienst-gesetz-grundrecht>
- Born, Hans and Leigh, Ian. 2002. Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies. (Oslo: Norwegian Parliament Press). Available at [www.dcaf.ch](http://www.dcaf.ch)
- Deutscher Bundestag. 2016. Statements by Gärditz, Graulich, Wetzling, Schindler, Töpfer, Wolff and Bäcker on the draft intelligence reform. Ausschussdrucksachen 18(4)653 A-G. Available at: [ww.bundestag.de/inneres](http://www.bundestag.de/inneres)
- Deutscher Bundestag. 2015. Annual report on surveillance measures by the federal intelligence agencies under Art. 10 Law. Drucksache 18/3709. Available at [www.bundestag.de](http://www.bundestag.de)
- Gärditz, Klaus. 2017. Legal Restraints on the Extraterritorial Activities of Germany's Intelligence Services. in: Miller, Russell (ed.). 2017. Privacy and Power: A transatlantic dialogue in the shadows of the NSA-affair. (Cambridge: Cambridge University Press).
- Graulich, Kurt. 2017. Reform des Gesetzes über den Bundesnachrichtendienst. Kriminalpolitische Zeitschrift 2:1, 43-52.
- Heumann, Stefan. 2017. German exceptionalism? The Debate about the German Foreign Intelligence Service (BND) in: Miller, Russell (ed.). 2017. Privacy and Power: A transatlantic dialogue in the shadows of the NSA-affair. (Cambridge: Cambridge University Press).
- Hofmann-Riem, Wolfgang. 2015. Legal protection against surveillance by intelligence agencies: On the need for its reform. Bucerius Law Journal 2/2015 44-50. Available here: <http://www.law-school.de/>
- Martin, Stephan. 2017. Snowden und die Folgen. Infobrief 113/2017. RAV Berlin. Available at <http://www.rav.de/publikationen/infobriefe/infobrief-113-2017/snowden-und-die-folgen/>
- Meister, Andre. 2016. Secret Report: German Federal Intelligence Service BND violates laws and constitution by the dozen. Available at: <https://cryptome.org/2016/09/de-nixes-xkeyscore-netzpolitik-16-0902.pdf>
- Löffelmann, Markus. 2015. Regelung der Routineaufklärung. Recht + Politik, Volume 6:2015. Available at: <http://www.recht-politik.de/regelung-der-%E2%80%99eroutineaufklarung/>
- Papier, Hans-Jürgen. 2017. Strategische Fernmeldeüberwachung durch den Bundesnachrichtendienst. Deutsche Richterzeitung 01/17, 17-23.
- Töpfer, Eric. Kooperation im kontrollfreien Raum: Zur aktuellen Entgrenzung der Geheimdienste. Infobrief 113/2017. RAV Berlin. Available at: [www.rav.de/publikationen/infobriefe/infobrief-113-2017/kooperation-im-kontrollfreien-raum/](http://www.rav.de/publikationen/infobriefe/infobrief-113-2017/kooperation-im-kontrollfreien-raum/)
- von Notz, Konstantin. 2017. The Challenges of Limiting Intelligence Agencies' Mass Surveillance Regimes: Why Western Democracies Cannot Give up on Communication Privacy. in: Miller, Russell (ed.). 2017. Privacy and Power: A transatlantic dialogue in the shadows of the NSA-affair. (Cambridge: Cambridge University Press).
- Wetzling, Thorsten. 2016. The key to intelligence reform in Germany: Strengthening the G10-Commission's role to authorize strategic surveillance. Policy Brief 02/16. Stiftung Neue Verantwortung, Berlin. Available at: [www.stiftung-nv.de](http://www.stiftung-nv.de)
- Wetzling, Thorsten. 2016a. Aufklärung ohne Aufsicht? Über die Leistungsfähigkeit der Nachrichtendienstkontrolle in Deutschland. Band 43/Demokratie. Heinrich-Böll-Stiftung, Berlin. Available at: [www.boell.de](http://www.boell.de)



## About the author

**Thorsten Wetzling** directs the Privacy Project at the Stiftung Neue Verantwortung. His research and advocacy focuses on the democratization and professionalization of intelligence governance in Germany and Europe. Thorsten testified before the European Parliament and the Bundestag on intelligence legislation and his work appeared in various media outlets, including the Frankfurter Allgemeine Zeitung, Der Spiegel, Zeit Online, Frankfurter Rundschau and Handelsblatt. Thorsten holds a doctorate degree in political science from the Graduate Institute of International and Development Studies in Geneva.

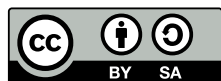
The **Stiftung Neue Verantwortung** (SNV) is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state.

## Imprint

Stiftung Neue Verantwortung e. V.  
Beisheim Center  
Berliner Freiheit 2  
10785 Berlin  
T: +49 (0) 30 81 45 03 78 80

www.stiftung-nv.de  
info@stiftung-nv.de  
Twitter: @SNV\_berlin

Design:  
Make Studio  
www.make-studio.net



This paper is subject to a Creative Commons license (CC BY-SA). The redistribution, publication, transformation or translation of publications of the Stiftung Neue Verantwortung which are marked with the license „CC BY-SA“, including any derivative products, is permitted under the conditions „Attribution“ and „Share Alike“. More details on the licensing terms can be found here: <http://creativecommons.org/licenses/by-sa/4.0/>