**Policy Brief | 02 / 2016**

stiftung | neue verantwortung

# The key to intelligence reform in Germany: Strengthening the G 10-Commission's role to authorise strategic surveillance

by Dr. Thorsten Wetzling

| www.stiftung-nv.de
| Twitter: @snv_berlin

## Executive Summary

Many European countries have recently adopted new intelligence laws or are currently reviewing them. Germany is about to follow suit. Unlike their European colleagues, legislators in Berlin will have to align and defend their particular reform proposals against the substantial shortcomings that the Bundestag's in-depth investigation into signals intelligence cooperation between the Bundesnachrichtendienst (BND) and its intelligence partners (particularly NSA and GCHQ) unearthed.

It is against this backdrop that this paper first reviews the main deficits of the current oversight system for signals intelligence (SIGINT) and then provides recommendations on how to improve and modernize its authorisation, oversight and transparency.

Within the current system of intelligence oversight in Germany, the G 10-Commission is responsible for examining and authorising governmental requests to allow the federal intelligence services to intercept private communications. Unlike other parliamentary control bodies, it holds the important power to order an immediate end to surveillance measures it deems unlawful or unnecessary.

However, due to grave institutional deficits and significant gaps in the current intelligence law, the G 10-Commission cannot properly perform its important democratic control function. For example, the core business of the BND's SIGINT activities – i.e. the acquisition and collection of foreign-foreign communication data (data that has both its origin and destination outside of Germany) – does not fall within the mandate of the G 10-Commission. Currently, this important practice is not subject to democratic control, let alone sufficiently regulated by the intelligence law. The G 10-Commission also lacks the resources and the technical know-how to conduct meaningful judicial review over the data processing by the federal intelligence services.

A significant reform of the current SIGINT authorisation and control process is required to overcome the current democratic deficits and to ensure that surveillance legislation and practice conform to international human rights standards and the German Basic Law.
The following reform measures are particularly important and ought to be addressed by Germany's pending intelligence reform

- The G 10-Commission must be able to review the legality and necessity of foreign-foreign telecommunications surveillance. A new intelligence law ought to address the entire spectrum of possible infringements of the right to private communication.

- A civil liberties advocate should be embedded in the process of authorizing communication surveillance in Germany. He/she would represent the interest of those directly affected by SIGINT measures who currently play no part in Germany's unique quasi-judicial "substitute procedure" (German Constitutional Court). The civil liberties advocate would delineate how an envisaged surveillance measure would conflict with the right to private communication and could make the case for a less intrusive but perhaps equally insightful SIGINT operation.

- The G 10-Commission needs substantial empowerment. More important than the amount of individual commissioners is an efficient secretariat. This requires financial and human resources to enable them to pre-examine interception warrants in light of the extended mandate of the G 10-Commission.

Dr. Thorsten Wetzling
Project Leader, twetzling@stiftung-nv.de

**Table of conduct**

*„The privacy of correspondence, posts and telecommunications shall be inviolable. Restrictions may be ordered only pursuant to a law."*
*Basic Law of the Federal Republic of Germany, Art. 10*

*„No one shall be subjected to arbitrary or unlawful interference with his privacy […] or correspondence. Everyone has the right to the protection of the law against such interference […]"*
*International Covenant on Civil and Political Rights, Art. 17.*

*"The Federal Intelligence Service shall collect and analyse information required for obtaining foreign intelligence, which is of importance for the foreign and security policy of the Federal Republic of Germany.*
*(Federal Intelligence Service Act (BNDG)*

## Introduction*

The work of the "NSA Inquiry Committee" set up by the German Parliament (Bundestag) provided a first opportunity for the public to learn about the country's Foreign Intelligence Service (Bundesnachrichtendienst, BND) bulk collection of foreign-foreign communication data. This pertains to the collection, processing and use of millions of communication data originating and ending outside of Germany.[1] The BND refers to this practice as „routine surveillance", a practice which is estimated to amount to ninety percent of all BND SIGINT activities. (Löffelmann 2015: 2).

This practice runs counter to the European Convention on Human Rights, the International Covenant on Civil and Political Rights and the German Basic Law. These guarantee the privacy of correspondence, post and telecommunications as a "Right to protection (Abwehrrecht) against tapping, monitoring and recording of telecommunication contents […] the analysis of their contents and the use of the data thus gained" (Drucksache 18/3709: 2). Article 10 of the Basic Law lists "subjective rights that primarily obligate the state to refrain from interfering with privacy. When tele-

* The author would like to thank Dr. Bertold Huber, Frank Hofmann, Professor Niko Härting, Markus Löning, Dr. Stefan Heumann and Sebastian Rieger for their constructive criticism and valuable comments. The responsibility for the contents lies solely with the author.

communications are 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 authorisation procedure" (Drucksache 17/8639: 2, personal translation).

Prominent experts in constitutional law agree on the fact that the BND practice of collecting foreign communication data infringes upon the right to private communication guaranteed by Art. 10 of the Basic Law. This right, so the widespread consensus, protects not just German citizens but every person. The prevailing opinion is that neither the nationality of the communicating participants nor their country of residence are decisive criteria for the protection of civil rights (Bäcker 2014: 19). More decisive is the fact that German public authorities are bound by the provisions of the Basic Law at all times.

The intrusions of intelligence services into the constitutionally protected privacy of telecommunication are considered particularly severe (Epping 2012: 319). They may only be mandated on the basis of a law. Derogations from the course of law may take place only within strict conditions.[2]

The Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnis, commonly referred to as „Article 10 Law" in reference to Article 10 of the Basic Law which ascertains the right to privacy of communication, defines the cases, scope and conditions for the three federal intelligence services to engage in communication surveillance. Yet, the authority of the BND in the field of strategic surveillance of foreign telecommunication data fails to be governed by that law. Neither the Article 10 Law nor the vague mandate of the foreign intelligence services in the BND law provide the necessary legal basis (Huber 2013; SPD-Bundestagsfraktion 2015).

In the absence of a sufficient legal basis, the executive faces allegations of massive violations of the fundamental right to privacy. What is more, in this highly sensitive field of security policy and fundamental rights, the entire spectrum of executive conduct has been bypassing not only the general public but also the supervisory bodies of the Bundestag. There has been no independent assessment of the legal interpretations for the strategic surveillance of foreign telecommunication, not to mention the handling of collected data and their transfer to third parties. No Parliamentary Intelligence Oversight Panel (Parlamentarisches Kontrollgremium, PKGr), no G 10-Com-

mission and no Data Protection Commissioner (Bundesbeauftragte für Datenschutz und die Informationsfreiheit, BfDI) ever had any say in this process.

Considering that these massive infringements of fundamental rights continue to lack legitimacy and considering the complete lack of separation of powers as regards the authorisation and execution of strategic surveillance of foreign telecommunications, it is urgent and necessary to discuss on a fundamental level how to ensure that the intrusion of intelligence services into telecommunication privacy complies with the rule of law and is subject to democratic control. This debate should not focus solely on expressing criticism but also formulate "concrete and viable reform proposals" (SPD-Bundestagsfraktion 2015: 3).

This policy brief aims at providing such a contribution and particularly examines the practice and the institutional framework of the G 10-Commission. This hitherto rather unknown panel of the Bundestag is quasi-judicial in nature. Its function is to authorise the intrusion of intelligence services into the privacy of correspondence, post and telecommunication and it takes on a crucial role for the protection of fundamental rights in cases of state surveillance. The G 10-Commission is the sole body in the German oversight system that is qualified to assess whether intrusions of the intelligence services into telecommunication privacy are necessary and lawful. Unlike the Parliamentary Intelligence Oversight Body (PKGr), the G 10-Commission may demand that measures considered unlawful be stopped immediately. It can thus ensure an effective protection of fundamental rights.

At present however, the G 10-Commission is not capable of fulfilling this role. This brief first points out the severe deficits of the actual G 10 procedure before generating clear recommendations for action to remedy the considerable constitutional unbalance without putting national security at risk.

## 1. A Critique of the Present System

This section first summarises the wide scope of deficits as regards the democratic control of SIGINT in Germany. These include the quality of the relevant intelligence service legislation as well as the mandate of the G 10-Commission. In a further step, it will outline decisive shortcomings of the present system as regards the institutional and practical implementation.

**Foreign-Foreign telecommunication surveillance: a source of illegitimate infringements of fundamental rights and unconstitutionality**

At the international level, the Article 10 law has been enjoying a good reputation for years. Countries willing to democratize their security sector often refer to the German legislation for guidance.[3] Just recently, in its report on the democratic control of SIGINT, the renowned Venice Commission of the Council of Europe highlighted Germany and Sweden as two states with laws that "present definite advantages" in international comparison (Venice Commission 2015: para 27).

Germany cannot however rest on its international laurels any longer. The Article 10 Law may contain progressive elements but it solely regulates the interception and surveillance of domestic communication or communications that originate or end in Germany. Once one knows that the "core business" (Huber 2013) of German SIGINT is beyond the reach of the German oversight system, the exemplarity of Germany's law and practice wanes. Without the option to pronounce on the lawfulness and necessity of the quantitatively much more significant foreign telecommunication surveillance, the G 10-Commission would remain, even in the opinion of one of its members, a "fair-weather commission" (Expert interview -1).

**Static body of intelligence law and secret interpretations**

Compared to German police law, the federal legislation on intelligence services presents a much lower density (Löffelmann 2015: 2). Clear and determined provisions however are of especially great significance for the legislation on intelligence services. After all, "[t]he secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight" (OHCHR 2014: para. 29).
Further, the intelligence law is too static. The structures required for the continuous assessment and adjustment of this body of laws are missing.[4] While the police law is characterised by dense case law, the German intelligence legislation, by virtue of the frequent exclusions of legal proceedings, rarely benefits from the important contributions that judges, lawyers and prosecutors can make to the definition and clarification of norms. This explains why the surprising and much criticised legal interpretation and practices of the executive as regards the territorial restriction of Ar-

ticle 10 of the Basic Law could remain unchallenged for years.[5] Secret interpretations of the intelligence law has expanded the latitude of the executive far beyond the core area of executive responsibility attributed to it by the German Constitutional Court.

The fact that the government was able to do entirely without the democratic legitimation of the Bundestag shows how severely disrupted the separation of powers is in this important field of security politics. By contrast, consider the normal practice: Parliament passes a law and the executive branch applies it.

Its interpretation can then be subjected to judicial review and the entire process is conducted under the watch of academia and the public.

„Secret provisions and secret interpretations – even secret judicial interpretations – do not comply with the criteria of a 'law'," the former UN High Commissioner for Human Rights states with concern in her report on the right to privacy (OHCHR 2014: para. 29). The duty of each State is rather to ensure „that every intrusion into the right to privacy, family, home or correspondence is authorized by laws that a) are publicly accessible, b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; c) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected; and d) provide for effective safeguards against abuse." (OHCHR 2014: para 28).

**The Role of the Executive Is not sufficiently accounted for in the law**

The Federal Ministry of the Interior (Bundesinnenministerium, BMI) plays a decisive role in the authorization of communications surveillance by the federal intelligence services. Bertold Huber, Vice Chairman of the G 10-Commission, recently described the procedure for authorizing the telecommunication surveillance measures stipulated in the Article 10 Law in those terms: "The service in question [Federal Intelligence Service, Federal Office for the Protection of the Constitution or the Military Counter Intelligence Agency (MAD), note by the author] submits a request to the BMI. The ministry carefully examines the request and when it considers it to be justified, it authorises the request and issues the corresponding warrant which generally howe-

ver may not be executed before the G 10-Commission has given its approval" (Huber 2014: 43).

Irrespective of the fact that foreign-foreign communications control is excluded from these procedures, the executive control also seems woefully ineffective: concrete verifiable information on the authorisation procedure of strategic surveillance of foreign-foreign communication, a procedure settled and agreed on solely by the executive, is missing. In the case of foreign communication surveillance, the BMI does not issue any warrants (Expert interview-2) – the BND presumably conducts its key business based entirely on its own competence and without any control. Unlike the procedures provided for in the Article 10 Law regarding interferences of intelligence services with the privacy of communication, the BND is apparently not required to submit requests to the BMI in order to conduct what it calls "routine surveillance". It thus remains unclear whether and how the Federal Government actually exercises any executive control over foreign communications surveillance: Does the BND have to formally justify the geographic and temporal dimension of interception measures? In how far are the necessity criteria for the justification of intrusions in the affected communication and data transmission observed? It also remains open to question whether the handling of the intercepted data originating from sole foreign surveillance is examined to verify that the otherwise mandatory procedural provisions are respected (examination, labelling and deletion requirements, release of information and principle of purpose). Equally doubtful is whether the BMI is presently assessing whether "those occurrences in foreign countries that the BND would like to collect data on present any direct connection to the concrete assignment profile (Auftragsprofil, APB) defined by the federal government for the BND or are related to the protection of the lives of German and allied forces deployed in crisis areas ("Force Protection")" (SPD-Bundestagsfraktion 2015: 10).

One may thus suspect that the BND monitors communications starting and ending in foreign countries without being subjected to any external control by the Federal Government, the Bundestag or the Data Protection Authority.

**Practically No Independent Control of the BND Data Processing**

The Article 10 Law specifies that the remit of the G 10-Commission covers the entire collection, processing and use of the personal data that the Federal Intelligence Service gathers under this law. Setting aside the fact that the BND also collects personal

data in a manner that is not regulated by the Article 10 Law, the wording here is emblematic. The law does not talk of control obligations or of control responsibilities. Rather, the honorary members of the commission are free, if they wish to and have the time, to also control the manner in which the BND handles the collected data. Hence, it amounts to an open invitation to conduct more work in addition to the required examinations of admissibility and necessity of surveillance under the Art. 10 Law.

As described earlier, the G 10-Commission is the only body in the German intelligence oversight system that is able to effectively protect fundamental rights and safeguard privacy of telecommunications from interference by the three federal intelligence services.

This „responsible task" (Drucksache 18/3709: 4) has so far been performed by four persons holding part-time, honorary positions and a rather vague formal competence to look into data handling. This is hardly sufficient. The G 10-Commission members „are to be given access to any documentation, especially stored data and the data processing software connected to the surveillance measure" (§15 Para. 5. No. 3 Article 10 Law). What may sound progressive at first - and is to be commended as regards the unrestricted access – does, on closer inspection, not result in de facto independent control of intelligence data processing. The G 10-Commission is not subject to any information requirement as regards its work. The relevant ministries, not the G 10-Commission, inform the Parliamentary Intelligence Oversight Body (PKGr) which in turn informs the Bundestag on a yearly basis on the "execution as well as type and scope" of the surveillance measures.

The latest publicly accessible information given by the PKGr solely states the following on the matter: "Further, the members of the [G 10] Commission and the staff of the [PD-5] secretary [of the Bundestag administration] conducted information and control visits to the services and gathered information on the concrete implementation of the concerned measures and on compliance with statutory provisions" (Drucksache 18/3709: 4). It is worth remarking that the members of the G 10-Commission will generally travel from the whole of Germany to Berlin once a month in order to decide on the admissibility and necessity of intelligence communication surveillance activities, not only of the BND but also of BfV and MAD. Realistically, this leaves little time to conduct examinations in the field of data protection. Open to question is also

whether all members possess the required juridical and technical expertise or acquire this knowledge in the course of their mandate.

While the G 10-Commission members may provide the „Data Protection Commissioner with opportunities to comment on data protection issues" (§15 Para. 5 Article 10 Law) and while the BfDI is theoretically also entitled to perform controls "in so far as the intelligence services are gathering or processing personal data", this does not however apply to personal data collected on the basis of the Art. 10 law. These fall under the exclusive control competence of the G 10-Commission" (Drucksache 18/59: 5). Thus if, as this has been implied by the former Data Protection Commissioner in the case of strategic surveillance of foreign telecommunications, no G 10 regulation is available and the government does not provide any information to the BfDI (Bundestagstextarchiv 2015; Krempl 2015), then a severe control vacuum exists.

Considering the lack of capacity and of reporting obligations of the G 10-Commission and in light of the fact that neither G 10-Commission nor BfDI exert independent control over the strategic surveillance of foreign telecommunications, it has so far remained in the hands of the authority that is gathering the data to also heed legal standards for data processing.[6] Clearly, Germany does therefore not meet the standards for independent control of data processing that the Venice Commission has recently emphasized anew (Venice Commission 2015: para 121).[7]

**The Authorization Procedure is Insufficient and not Immune to Abuse by the Executive**

Considering the gravity of the fundamental right infringements and the complexity of SIGINT, it is important to thoroughly clarify the questions of the extent of the restriction measures submitted for approval as well as their legality and necessity. The secretariat of the G 10-Commission is currently responsible for the preparation of the monthly sessions. Notably, the commission members receive information on the BMI warrants only on the day of their monthly meeting. It is thus questionable whether the commission members are amply prepared to challenge the position that the executive has taken.

Understandably, the honorary members of the commission who travelled from outside of Berlin wish to take a train home in the evening. What happens however when

their deliberations require more time and a series of warrants have yet to be discussed towards the end of their meeting? Will they be resubmitted to the commission the following month or does the work of the commission inevitably become less thorough towards the end? In that case, it is far more likely that fundamental rights rather than security concerns fall victim to a rushed assessment of the warrants.[8] It is precisely in situations like this that there is a risk to see important questions related to the legality and necessity of specific surveillance measures being neglected in practice. Thus, a catalogue of minimal requirements should be available that would automatically be applied in those cases where a thorough assessment is not feasible.

In a statement to the NSA Inquiry Committee, Hans De With, chairman of the G 10-Commission until January 2014, pointed out a further severe deficit of the present authorisation procedure: It is prone to abuse by the executive. Frank Hofman (current member of the G 10-Commission) took this up again in an interview: "The government consciously deceived the G 10-Commission on the true purpose of the surveillance measures in Frankfurt. […] One expected that the BND wanted to get permission from the Commission for the wiretapping of German citizens outside of Germany. In fact, the intelligence service used the approval in order to massively tap into transit traffic. […] The G 10-Commission is abused as a Trojan Horse." (Strozyk 2015).

**Anachronistic 20 Percent Rule for the Collection of „International Telecommunications"**

At present, the Article 10 Law allows the Intelligence Service to "automatically collect, record and exploit telecommunications that take place from Germany to a foreign country (in specific States/ areas) or from there to Germany." (Drucksache 18/59: 4). To do so, "the BND may screen up to 20 percent of all telecommunications handled over a specific hub according to predefined criteria" (Ibid). The 20 percent limit however does not refer to the data quantity sent through an internet cable but to the capacity of the wire through which the transport takes place (Bundestagstextarchiv 2015b). Klaus Landefeld, Chairman for Infrastructure and Networks at the Association of the Internet Industry (eco) e.V. as well as council member of the DE-CIX Management GmbH, put this into more concrete terms for the NSA Inquiry Committee: "The capacity is always only partially used so that the BND may collect far more than 20 percent of the data that flows through a cable. This is not what one has in mind

when one pictures restrictions of the surveillance of telecommunication" (Bundestagstextarchiv 2015b).

**Insufficient selection criteria and lack of transparency**

According to the Article 10 law, the chairman of the G 10-Commission is the only member who has to be qualified to hold the position of a judge. The other commission members are not submitted to any selection criteria. The commission members receive no training or any other preparation for the honorary position when they first take on their office. Thus for many, the start is a bit of a "plunge" (Expert interview 2). This becomes particularly apparent in situations where the Federal Ministry mandates communication surveillances according to § 3 or § 5 of the Article 10 Law and the commission members cannot adequately estimate whether to trust the argumentation of the BMI or the statements of single sources. "Precisely because we do not sit together with the BMI officers, it is from time to time difficult to evaluate whether to follow the reasoning for a mandated restriction measure" (Expert interview 1). The commission members thus often fumble in the dark and detailed assessments are the result of the interest or avocation of single commission members rather than an expression of systemic procedures.

The lack of any reporting requirements for the G 10-Commission has already been emphasised. Its secretariat (PD-5) keeps the minutes of its decisions. These however do not include the assessments of the commission members (Expert interview 3). It also remains unclear whether the members of the G 10-Commission are allowed to pass information onto the members of the Parliamentary Intelligence Oversight Body, and if so, which.

The following table summarises the deficits as regards the existing system of SIGINT control in Germany:

- Core business of the BND's SIGINT activities (i.e. the surveillance of communication originating and ending outside of Germany) is presently exempt from democratic control and not based on a legal footing
- Lack of technical, expert and staff capacity in the secretariat of the G 10-Commission
- Role of the executive insufficiently accounted for in the intelligence law
- Executive control over BND's core SIGINT activities is dysfunctional
- Existing G 10 authorisation procedure prone to executive abuse
- Inadequate control of data processing by the G 10-Commission and exclusion of the BfDI in cases of G 10 procedures and core business
- Selection criteria for G 10-Commission members and honorary positions inadequate for this important control function
- No contradictory procedure embedded in the authorisation procedure
- De facto circumventions of the existing 20 percent rule that restricts the collection of domestic-foreign communication
- No reporting requirements for the G 10-Commission

Overview of the deficits as regards democratic control over intelligence surveillance of communication

## 2. Reform Proposals

Considering the previously delineated problems affecting the protection of fundamental rights and the imbalanced separation of powers, it is high time to lead a broad discussion on how to provide legal and democratic control over the whole of SIGINT activities by the BND in future.

Recently, the German Social Democratic Party (SPD) deplored the lack of "concrete and viable proposals for a reform of the pertinent SIGINT law and practice that has become a constitutional necessity" (SPD-Bundestagsfraktion 2015: 3). The deficits previously described may not be dispelled simply by extending the legal scope of the Article 10 Law to the bulk collection of foreign telecommunication data. Rather, a clear catalogue of criteria should be compiled giving due consideration to security interests, other available options for the collection of information and the intrusion intensity of the measure. Such a catalogue should be developed with the participation of civil liberty experts and define the process and decision criteria for a new

authorisation procedure. This would not only apply to the necessary assessments of legality and necessity of the single measures but also to the further handling of the data collected as part of the measures and to the question of how to take reasonable account of the guarantees provided by law in this area.

The necessary reform of democratic control over SIGINT should pay consideration to the following aspects:

- authorisation procedure
- the subsequent handling of the collected data
- the right to effective remedy (Art. 19 Para. 4 Basic Law).

The following section considers policy recommendations. They were developed on the basis of a series of background talks and expert interviews and emphasise the aspects that a reform should most urgently address.

**The Entire Range of SIGINT Activities Should be Regulated**

The Bundestag should adopt a new Article 10 law that unequivocally and bindingly regulates all intrusions into the privacy of correspondence, post and telecommunications by the federal intelligence services. As Art. [10] of the Basic Law does not solely apply to German citizens, it is also valid for natural persons in foreign countries. Hence, at the very least, non-German communication data must also benefit from some form of basic protection. Surveillance measures conducted purely on data from outside Germany must in future also fall under the remit of the G 10-Commission. This however by no means implies that the quality of data protection offered by the Basic Law should be identical for German citizens, EU citizens and the rest of the world.

In order to shake off its reputation as an "irrelevant fair-weather commission" (Expert-interview-1), and to prevent future abuse as Trojan Horse, the new Article 10 Law, by analogy with § 3 and § 5 of the present law, should provide a sufficiently detailed list of the conditions required for a lawful authorization of foreign telecommunications data surveillance.

This law must respect the minimal requirements as concerns the clarity and precision of provisions in national security legislation. As regards the requirements for the surveillance of foreign telecommunications, the general guidelines laid out by the SPD paper contain good individual suggestions: The paper e.g. demands that "processes taking place outside of Germany for which the BND wishes to collect information must be directly related to the concrete assignment profile (APB) of the Federal Government for the BND or be connected with the protection of the lives of German and allied forces deployed in crisis areas ("Force Protection")". (SPD-Bundestagsfraktion 2015: 10). In this case however, not only the „Federal Chancellery should be legally required to pass on the BND assignment profile in an appropriate form to the G 10-Commission" (Ibid). The assignment profile must also be underpinned by democratic legitimacy, which would require at the very least a fundamental discussion on the essential issues of the APB to take place in the plenary of the Bundestag. The core issues of the APB must subsequently be recapitulated in the BND law.

**Time for the „Super G 10-Commission" and closer co-ordination with the Federal Commissioner for Data Protection**

In addition to the extension of the authorisation procedure onto foreign telecommunications surveillance, it is necessary to decisively improve the controlling

capacity and options of the G 10-Commission as regards the authorized measures. The required amendment of the Article 10 Law would otherwise prove futile, as the G 10-Commission could not guarantee an effective protection of fundamental rights. After all, the "control of foreign telecommunication surveillance by intelligence services is not an activity that can take place "on the side" but rather requires a high level of legal and technical expertise and a great deal of personal dedication" (Löffelmann 2015: 3).

Should the G 10-Commission be responsible for the authorisation of all BND telecommunication surveillance in future, this significant supervisory body then requires massive reinforcement. In this respect, a secretariat able to work effectively seems much more decisive than the number of members.

It should conduct preliminary examinations of the warrants in line with and on behalf of the G 10-Commission. After specialists conducted a comprehensive prelimi-

nary examination, they could present the G 10-Commission with a decision proposal comprising the main issues. This requires significantly more "material resources and qualified support staff of the Bundestag administration" with "juristic, technical and intelligence expertise" (SPD-Bundestagsfraktion 2015: 8) to be invested into the Secretariat PD 5 of the Bundestag as is presently the case.

What is more, it is time to replace the honorary character of the G 10-Commission membership with employed status. Instead of presently four honorary members (and their deputies), the G 10-Commission should consist in future of at least just as many employed members who meet on several days every month if need be.

The authority to be informed and assess in detail the feeding-in of selectors into the collection system of the BND also bears great significance for the effectiveness of the G 10-Commission. The SPD general guidelines formulates an important demand: "The G 10-Commission must be entitled at all times to review all search terms used for the selection of the information gathered and verify whether these serve the purpose of fulfilling the task and do not contravene German interests. All rights resulting from § 15 Para. 5 of the Article 10 Law must extend to the control of the entire strategic surveillance of telecommunications by the BND" (SPD-Bundestagsfraktion 2015: 13).

In this matter, experts such as Klaus Landefeld draw attention to the fact that selectors cannot be controlled statically. They change on an hourly basis. Thus not only is an increase in the staff of the G 10-Commission necessary but also an ongoing, permanent control of the surveillance measures. This would be the only way to counter massive data collection with a proper, independent control.

The future G 10-Commission should also be commissioned to critically assess the cable selection for the strategic surveillance of foreign telecommunications. The following questions play a central role: What justifies the cable selection? Could another, less intrusive measure be sufficient to gain the same knowledge?

As with the requirements of the warrants under the Article 10 Law, in the case of foreign-foreign communication surveillance the option must be available for the Commission to have the executive cancel without delay a warrant "which the commission declares to be illegal or unnecessary" (§ 6 Sentence 3 Article 10 Law).

Further, the G 10-Commission should assess, in close co-ordination with the Federal Data Protection Agency, whether the BND's collection, processing and exchange of data as well as deletion of no longer useful data is conducted in accordance with the legal data protection requirements. In order to do so, and as with the present provisions of the Article 10 Law (in particular §§ 4, 6, 7, 7a, 11), similar provisions pertinent to the strategic surveillance of foreign telecommunications must be included into the law. It would also be conceivable to set up a new unit for security audits at the BfDI which would be sufficiently staffed and equipped with adequate expertise and technology. A close connection with the G 10-Commission could be promoted by setting up the new BfDI unit geographically close to the Bundestag. This would thus partly counter the risk of fragmentation of the controlling bodies.

**Introduce a Contradictory Procedure within the G 10 Authorisation Process**

A fundamental principle of the Rechtsstaat consists in "[…] the freedom from state control and surveillance measures so long as no ground exists for a criminal procedure" (Drucksache 18/5453: 3). A further principle, the so-called Richtervorbehalt, states that intrusions of a severe or potentially abusive nature into essential rights of individuals must be conditional on judicial order or authorisation.

The groundless and massive collection of communication data in the absence of any suspicion by the Federal Intelligence Services conflicts with the first principle. Furthermore, the German control system over infringements of the fundamental right deriving from Art. 10 Basic Law has been referred to as a "substitute procedure" (2BvF 1/69) by the Bundesverfassungsgericht given that no exhaustive judicial control is intended prior to the implementation of such surveillance measures.[9] The situation is different in the case of e.g. police preparatory investigation. Due to the lack of transparency in the use of undercover investigators, the Bundestag saw grounds to "make provisions for prior judicial control. Both the code of criminal procedure and the police law provide for […] a judicial decision on the permissibility of the use of an undercover investigator" (Roggan 2006: 191). In contrast, the Federal Constitutional Court considers the „G 10-Commission to be a controlling body of its own kind beyond judicial power that serves as a substitute precisely for judicial review" (NVwZ 1994: 367).

The party Die Linke recently called for the complete termination of intelligence intrusions into the privacy of correspondence, post and telecommunications and presented a "legislative proposal for the termination of the Article 10 Law" (Drucksache 18/5453). This proposal rightly points to the great discrepancy between the low encroachment threshold (i.e. the required preconditions for the surveillance measures) that applies to the intelligence services on one side and the significantly higher intrusion barrier that applies to the authorities for public risk prevention and criminal prosecution on the other. Considering the trend towards increasing overlaps of the three areas of constitutional relevance "intelligence service activity, preventive police measures and criminal prosecution", members of the Government Commission for the Review of Security Legislation (Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung) also recommend to "assess whether and in how far overlapping areas may be reduced" and in doing so "reduce [...] prima facie the competence of the intelligence services" (Regierungskommission 2013: 164). Some in security circles conceded that a lot of what the intelligence services undertake as part of the technical surveillance inside Germany should be conducted by the Federal Criminal Police Officer and other police agencies (Expert interview 4).

Thus it is inherently right and important to consider how to raise the encroachment threshold of intelligence services in future. This does not imply that intelligence service intrusions into the privacy of telecommunications be entirely abolished. Further, these considerations must include the critique that has been repeatedly expressed as regards the practicalities of the Richtervorbehalt.10 Finally, the most constructive approach at present seems to be to hold on to the construct of the G 10-Commission. Besides an increase in personnel and the extension of controlling authority, a further decisive change is however urgently required: the integration of a civil liberty advocate into its authorisation process. This would significantly raise the practical encroachment threshold for the implementation of surveillance measures by intelligence services.

The new Article 10 Law should for its part stipulate that, besides the BMI representatives who explain the various warrants to the G 10-Commission, one person should be present who represents the interests of the persons targeted by the surveillance measures who "have no opportunity to play a part in this substitute procedure".

The role of the civil liberty advocate is to justify to the commission members in how far the warrant contradicts the right to privacy and which measures with a lower intrusive intensity would serve a similar purpose. Within the G 10 procedure, the civil liberty advocate should be allotted the competence to notify the Parliamentary Intelligence Oversight Body of decisions of a specific significance and of relevance to fundamental rights, such as decisions that justify new methods or goals of operation. One should also take into consideration the option to provide this person with the competence to file a law suit against the surveillance measures that he/she considers to be contradicting fundamental rights. The implementation of this recommendation would put Germany on the footsteps of the very promising reform efforts undertaken by Sweden and the USA.[11]

**Best Practices in Tackling the „Discrimination Problem"**

Over the course of the past decades, democratic states have created a series of protection and control mechanisms to protect the privacy of their own citizens from intrusions by their own intelligence services. Edward Snowden's disclosures on the extent and the practice of worldwide internet and communication surveillance by western intelligence services however provided impressive proof of how defenceless these citizens are in the face of surveillance by foreign intelligence services. Further, it became evident in the NSA inquiry committee of the Bundestag that the Federal Intelligence Services pays just as little attention to the protection of the rights and data of non-German citizens as the NSA to the rights and data of non-US citizens.

The indignation of the Federal Government over the spying among friends presents little credibility considering its own practice. More so: Now that Austria, the Netherlands, Belgium, Switzerland and Luxembourg have started investigating on the collection, processing and transmission of data from the transit traffic of European wires, the Federal Government must consider the European dimension of the "BND/NSA scandal".

This sensitive problem of international relations can be addressed at least in part with an exemplary reform of the democratic control over intelligence services. Implementing international best practices related to the "discrimination problem" would make an important contribution to a better protection of the data of German citizens from the intelligence services of allied or befriended states.

Instead of venturing on a „non-binding ‚No-Spy' agreement", Germany could start by creating good constitutional protection mechanisms that offer significantly better protection for the data of foreigners. This standard would then be actively demanded by others so as to eventually become a common standard. "The more our partners resolve to adopt comparable standards, the less our citizens have to fear an intrusion on their privacy by the services of befriended countries" (SPD-Bundestagsfraktion 2015: 8).

This goal is not easy to implement in practice. Would the collected data of all non-EU citizens receive the same protection as the data of German citizens (including prior authorisation of data collection, requirements for data processing and identification, regulations for the deletion and transmission of data, notification requirements, legal protection guarantees), then these changes would put the constitutional obligation of the intelligence service into question. Hence the following specifications appear moderate: First, no distinction should be made between the data of German residents and EU-citizens. The same data protection provisions and right to effective remedy that are currently only granted to German citizens as regards intrusions by the intelligence service into their telecommunication privacy should be extended and equally apply to EU-citizens. This will result in an additional burden for the controlling bodies. The state must however establish and maintain the necessary infrastructure for the assertion of these comprehensive citizens' fundamental rights. The fact that the administrations would face a great challenge is not a convincing argument against the assertion of rights and legal claims.

Second, it is true that the quasi-judicial prior authorisation will be extended to all surveillance measures executed by intelligence services, i.e. also to those measures that solely aim at collecting data of non-EU citizens. Sufficient expertise and increased personnel in the G 10-Commission, including the involvement of a civil liberty advocate in the authorisation procedure and the use of a clear justification requirement (see below) for the newly created G 10-Commission, already create significantly higher barriers for intelligence service intrusions into the telecommunication privacy of upright non-German citizens.

Third, as regards the specific procedures of data collection and data processing, Germany should at least not rank behind the standard laid out in US Presidential Policy Directive 28. This directive states that domestic and foreign data should as much as

possible be governed by the same standards to the extent that is compatible with national security.[12]

Fourth, and tempering the previous a little, an essential distinction must be made when it comes to the extension of the right to effective remedy to Non-Germans. Here it may be permissible to reserve the right to notification (§ 12 Article 10 Law) and the right to effective remedy (Art. 19IV Basic Law) only to Germans and EU-citizens. Based on the existing jurisprudence of the Federal Constitutional Court, such an interpretation of the obligation to provide for an effective protection of basic rights appears possible.[13]

**More Transparency with a Justification Requirement and the Publication of G10 Commission Decisions**

The separation of powers does not function well when the public is entirely excluded. Respecting internationally proven standards is not the only decisive aspect in order to bring about an improved performance of the executive, judicial and parliamentary control of secret services; a minimum of transparency plays an equally important role, too.

Thus the G 10-Commission should in future be subject to a requirement to justify its decisions. As is the case for court decisions, the individual decisions made by the G 10-Commission should be justified in detail. This justification should include such aspects as a clear identification of the specific constitutional issues that require a decision and notes on how these issues were resolved using which interpretation of the law. The justification should also indicate whether and in how far the G 10 decision differs from previous decisions or guiding principles of the decision making process.[14] The G 10 secretariat should keep minutes of the whole of the G 10 decisions and hand these for review to the parliamentary control committee.

The US-American practice should basically serve as an example: The Director of National Intelligence publishes individual decisions of the FISA courts[15] based on the recommendations of the President's Review Group on Intelligence and Communications Technologies in order to inform the public of the arguments used to approve or reject instructed restriction measures. For reasons of confidentiality, individual G 10 decisions would similarly have to be blackened.

## Conclusion

The federal intelligence services have thus far been able to conduct foreign telecommunication data surveillance without much interference from the executive, the legislative or the judiciary. Apparently they have been apprehensive of a "moratorium of G 10 collection and [...] a parliamentary consideration of the subject with unpredictable consequences" (Strozyk 2015). Our democracy should welcome a proper "parliamentary consideration" of this important security practice. In fact, the Bundestag could in future better protect the intelligence services from unethical or unwise instructions of the executive. In addition, the intelligence services ought to provide convincing arguments to make the case for why the surveillance of telecommunications is and should remain an important instrument of the German security policy. Regardless of the important issues addressed in this study as regards the legal basis and the constitutionality of the authorisation procedure, there is so far no convincing evidence that the massive surveillance of communications offers an efficient mean to gain information that are of significance for the German foreign and security policy.[16]

Many of the deficits described in this study have been known for more than two years now. No serious measures have been taken so far to overcome this constitutionally unacceptable situation. This is particularly surprising considering that in autumn 2013 Germany had already pleaded at the United Nations for the extension of the protection of privacy in the digital age. The resolution adopted by the General Assembly calls on all member states to protect the right to privacy and to "review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection," as well as "To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data, including metadata" (United Nations 2015: para. 4c and 4d).

The NSA Inquiry Committee of the Bundestag, set up in March 2014, is also tasked with clarifying whether "legal and technical changes [are] required to the German system of foreign surveillance carried out by the intelligence services in order to

ensure that German authorities comply fully with fundamental and human rights, and if so, which? In addition, the inquiry committee is expected to recommend ways to ensure that the executive, parliamentary, judicial and independent data-protection oversight of the federal security authorities [can] be ensured fully and effectively." (Drucksache 18/843: 5).

The German system of democratic intelligence oversight presently lacks concrete and verifiable provisions that would allow Parliament or an independent expert body to rein in on the bulk of the BND's SIGINT activities. To date, these activities of the state are solely administered in closely-knit executive circles. This concerns both the authorisation procedure, the data processing and the exchange of data with foreign intelligence partners.

If one wants to avoid political damage in future, as well as support effective intelligence services in their critically important work while pursuing a credible international foreign and security policy, then the many deficits outlined in this study may no longer be ignored. It is high time for a comprehensive reform of the legislation, management and control practice pertaining to SIGINT in Germany. The strengthening and extension of the G 10-Commission represents a particularly important step in this respect.

The credibility of German foreign and security policy, Germany's respectful contribution to the implementation of the very UN Resolution that she has tabled and numerous lawsuits that have already been filed require a prompt reaction on the part of both the Bundestag and the Federal Government.[17]

**References**

Bäcker, M. (2015): Der BND baut sich einen rechtsfreien Raum: Erkenntnisse aus dem NSA-Untersuchungsausschuss. Available at: http://www.verfassungsblog.de/der-bnd-baut-sich-einen-rechtsfreien-raum-erkenntnisse-aus-dem-nsa-untersuchungsausschuss.

Bäcker, M. (2014a): Erhebung, Bevorratung und Übermittlung von Telekommunika- tionsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22.Mai 2014, p. 1-23.

Bäcker, M. (2014b): Der Fall des Geheimen – Ein blick unter den eigenen Teppich. In FlfF-Kommunikation FlfF e.V. (Ed..), p. 35-40.

Çaliskan, S. (2015): Rechtsverletzungen statt Kampf gegen die NSA. Gastbeitrag in der Frankfurter Rundschau vom 21.07.2015. Available at: http://www.fr-on- line.de/gastbeitraege/nsa-skandal-rechtsverletzungen-statt-kampf-gegen-die- nsa,29976308,31266000,view,asFirstTeaser.html

Deutscher Bundestag (2015): Schaar: Sicherheitsdienste effektiver beaufsichtigen. Textarchiv des Bundestages. Available at: http://www.bundestag.de/dokumente/textarchiv/2015/kw03_pa_1ua/352812

Epping, V. (2012): Grundrechte – 5. Auflage. (Berlin: Springer Verlag).
Große Strafrechtskommission des Deutschen Richterbundes (2008): Das Verhältnis von Gericht, Staatsanwaltschaft und Polizei im Ermittlungsverfahren, Strafprozessuale Regeln und faktische (Fehl-?) Entwicklungen, Gutachten im Auftrag des Bundesministerium der Justiz.

Heumann, S. (2015): Bundesnachrichtendienst unter Beobachtung: Erste Erkenntnisse aus eineinhalb Jahren Überwachungsdebatte. Impulspapier der stiftung neue verantwortung. Available at: http://www.stiftung-nv.de/publikation/bundesnachrichtendienst-unter-beobachtung-erste-erkenntnisse-aus-einein-halb-jahren

Heumann, S. & Wetzling, T. (2014): Policy Brief. Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kont-

rolle. Stiftung neue Verantwortung, p.1-27. Available at: http://www.stiftung-nv. de/sites/default/files/052014_snv_policy_brief_strategische_auslandsuberwa- chung.pdf

Huber, B. (2013): Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite. Neue Juristische Wochenschrift, Heft 35/2013, p. 2572-2577.

Huber, B. (2014): Die Fernmeldeaufklärung des Bundesnachrichtendienstes: Rechtsgrundlagen und bestehende Regelungsdefizite. Vorgänge nr. 206/207. Also Available at: https://netzpolitik.org/2015/die-fernmeldeaufklaerung-des-bun- desnachrichtendienstes-rechtsgrundlagen-und-bestehende-regelungsdefizite.

Huber, B. (im Erscheinen): Selektorenlisten und Sonderermittler. Neue Zeitung für Verwaltungsrecht. Ausgabe 19/2015.

Krempl, S. (2015). NSA-Ausschuss: Peter Schaar sieht große Lücken bei BND-Kontrol- le. Available at: www.heise.de

Löffelmann, M. (2015): Regelung der „Routineaufklärung", recht + politik, Ausgabe 6/2015, Available at: http://www.recht-politik.de/wp-content/ uploads/2015/06/Ausgabe-vom-22.-Juni-2015-Regelung-der-Routineaufklä- rung-PDF-Download.pdf

Privacy and Civil Liberties Oversight Board (2014): Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveil- lance Act. Available at: https://www.pclob.gov/library/702-Report.pdf

Regierungskommission (2013): Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland. Available at: http://www.bmi. bund.de/SharedDocs/Downloads/DE/Broschueren/2013/regierungskommissi- on-sicherheitsgesetzgebung.pdf?__blob=publicationFile

Roggan, F. (2006): Verdeckte Ermittler in Polizei- und Strafprozessrecht", in: Roggan, F. and Kutscha, M. (Ed.), Handbuch zum Recht der Inneren Sicherheit – 2. Edition, (Berlin: Berliner Wissenschaftsverlag).

Schantz, P. (2015): Rechtsschutz gegen die strategische Fernmeldeüberwachung: Ein blinder Fleck im Rechtsstaat. Neue Zeitung für Verwaltungsrecht, Ausgabe 13/2015, Seiten 873-877.

Scott, B. (2015): Expert Statement for the Committee of Inquiry of the German Parliament. stiftung neue verantwortung, July 2015.

SPD-Bundestagsfraktion. (2015): Eckpunkte der SPD-Bundestagsfraktion für eine grundlegende Reform der strategischen Fernmeldeaufklärung des BND mit in- ternationaler Vorbildwirklung. Available at: http://www.spd-bundestagsfrakti- on.de/sites/default/files/2015-06-16-spd-eckpunkte_reform_strafma-r-endfas- sung.pdf
Strozyk, J. L. (2015): Überwachung des Internetknotens: DE-CIX verklagt BND. Available at https://www.tagesschau.de/inland/decix-klage-bnd-101.html

Venice Commission of the Council of Europe. (2015): "Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democrat- ic Oversight of Signals Intelligence Agencies." Available at http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e.
Vereinte Nationen (2015): Das Recht auf Privatheit im digitalen Zeitalter. Resolution der Generalversammlung A/Res/69/166.

Vladeck, S. (2015): The case for a FISA Special Advocate, in: Texas A&M University Law Review (forthcoming). Available at: http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2546388

Werkmeister, C. (2011): Probleme bei der Grundrechtsberechtigung von Ausländern. Availabe at: http://www.juraexamen.info/probleme-bei-der-grundrechtsberechtigung-von-auslandern/

Wetzling, T. (2015): Großbaustelle Geheimdienstkontrolle. Gastbeitrag für die Frank- furter Allgemeine Zeitung. Available at: http://www.faz.net/aktuell/politik/inland/bnd-nsa-affaere-reform-der-geheimdienstkontrolle-noetig-13565482. html

Wetzling, T. (2015a): Expert Statement for the European Parliaments' Com- mittee on Civil Liberties, Justice and Home Affairs (LIBE). Available at: http://www.europarl.europa.eu/committees/en/libe/events-nationalparl.html?id=20150528CHE00195

United Nations High Commissioner for Human Rights (OHCHR). (2014): Das Recht auf Privatheit im digitalen Zeitalter. Bericht A/HRC/27/37.

**Bundestag Drucksachen**

Drucksache 17/8247. Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht über die Kontrolltätigkeit gemäß §13 PkGrG (Berichtszeitraum September 2009 – Oktober 2011).

Drucksache 17/8639. Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht über die Kontrolltätigkeit gemäß §13 PkGrG (Berichtszeitraum 1. Januar bis 31. Dezember 2010).

Drucksache 18/5453. Entwurf eines Gesetzes zur Aufhebung des Artikel-10-Gesetzes und weiterer Gesetze mit Befugnis für die Nachrichtendienste des Bundes zu Beschränkungen von Art. 10 des Grundgesetzes. des Bundestages.

Drucksache 18/59. Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß §26 Abs. 2 des Bundesdatenschutzgesetzes.

Drucksache 18/843. Antrag der Fraktionen CDU/CSU, SPD, DIE LINKE, und Bündnis90/Die GRÜNEN: Einsetzung eines Untersuchungsausschusses.

**Expert interviews**

The author conducted interviews in summer 2015 with members of the G 10-Commission and experts connected to the intelligence services and the Bundestag. To respect the wishes of some of the interviewees, the author anonymised their personal information.

**Endotes**

1 A so-called „routine surveillance" includes no collection of „communications of German citizens or individuals who are located on the German territory" (Löffelmann 2015:2). The work of the NSA Inquiry Committee of the Bundestag made it however clear that no clean separation of the data can be entirely guaranteed. In its report, the US-American Privacy and Civil Liberties Oversight Board (PCLOB) also pointed to the enormous costs and the difficulty linked to identifying and taking out the data of the country's own citizens in the very large collection of data (PCLOB 2014:100).

2 If the legislator has made use of this option, the question of the „substitute to the legal recourse" is open. According to the Federal Constitutional Court, this should include a "re-examination" equivalent to court control in material terms and as regards the procedure" (2 BvF 1/69).

3 See for instance the following comment of the Parliamentary Intelligence Oversight Body: "During the reporting period, several visits of foreign delegations took place. One important aspect that explains the interest of the delegations for the work of the Body is the good reputation of control in this country. The structure of control and the competence regulated primarily in the PKGrG and the Article 10 Law are indeed exemplary for the design of parliamentary control in other states, especially those in Eastern Europe." (Drucksache 17/8247: 9)

4 At the federal level, this includes the Act on the Protection of the Constitution (BVerfSchG), the Act on the Federal Intelligence Services (BND-G), the MAD Act (MADG), the Article 10 Law (G10-G), the Act on the Parliamentary Intelligence Oversight Body (PKGrG), the Telecommunications Act (TKG) and the regulation on technical and organisational measures for the surveillance of telecommunications (TKÜG), the BSI-Act (BSIG), the Federal Data Protection Act (BDSG), the AZR Act (AZRG), the Customs Investigation Services Act (ZFdG), the Anti-Terror Database Act (ATDG) as well as the Act for the Establishment of a Standardised Central Database of Police Offices and Intelligence Services at Federal and State (Länder) Level for Combatting Violent Right-Wing Extremism (RED-G).

5 The general guidelines by the social-democrat (SPD) parliamentary group additionally deplores the fact that "the application of German data protection right has been eluded for years in this area (Key word "Space theory")".

6 According to §6 of the Article 10 Law, the BND must assess immediately and then every six months whether the collected personal data is necessary to fulfil its task. If the data is neither necessary nor required for transmission to another office, then it must be immediately deleted under the supervision of an official who is qualified to hold the position of a judge.

7 „Balancing of privacy and other human rights concerns against other interests comes in at several points in the process, but two crucial points are when a decision is made to use particular selectors, and when human analysts decide whether or not to keep the information in question. […] The second type of decision is of a „data protection" character, which can be overseen afterwards by an expert administrative body. Such a body must be independent and have appropriate powers." (Venice Commission 2015: para. 121).

8 After all, the BMI can „in case of danger, instruct the execution of surveillance measures even before the Commission has been informed" (§15 para. 6 Article 10 Law).

9 According to §13 Article 10 Law, the legal recourse "against the instruction of surveillance measures according to §§ 3 and 5 para. 1 sentence 3 No. 1 and their execution" is not permitted before the targeted persons are notified. Since however this does not apply to all risks listed under § 5 Para. 1, it is impossible to say whether the judicial control is excluded from the outset for all G 10 measures.

10 The große Strafrechtskommission (criminal law committee) of the German Association of Judges (Deutscher Richterbund) comes to the unanimous conclusion that "The commission sees deficits in the effective judicial control of state intervention powers (Richtervorbehalte) due to insufficient resources available to the court and prosecuting authorities." (Große Strafrechtskommission 2008: 224).

11 See on this matter e.g. the comments of the Venice Commission: "There is empirical evidence that such privacy advocates in law enforcement and internal security

surveillance can have some significance in helping ensure that the parameters of investigations really are drawn as narrowly as possible. See the Swedish official inquiry into secret surveillance (SOU 2012: 44). Privacy advocates (nominated by the Bar Council and appointed by the government) represent the interests of targeted persons and organizations in the authorization process before the Swedish Defence Intelligence Court." (Venice Commission 2015: para. 104). The idea of a civil liberty advocate has also been the subject of many discussions in the USA over the past year. Senator Blumenthal's legislative proposal (https://www.congress.gov/bill/113th- congress/senate-bill/1467/text) showed a particular depth of detail. The Presidential Review Group on Intelligence and Communications Technologies also took up this idea in its 28th recommendation. Stephen Vladeck's study on this topic is also recommended reading (Vladeck 2015).

12 The corresponding wording of the Presidential Policy Directive – Signals Intelligence Activities (PPD-28) under Section 4 reads: "To the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality".

13 See for instance the following argumentation of the Federal Constitutional Court: "Should the exercise of fundamental rights automatically affect the legal order in other states and should the conflicting interests of the bearers of fundamental rights be settled in a jurisdiction where the German legal order does not have sole claim to validity, then the power of the legislature are greater than when legal relations of mainly domestic nature are settled. In particular, the legislature is not precluded from considering specific circumstances that characterise the matter in need of elaboration but escape its power. The German legislator thus has the choice between protecting German fundamental rights standards in an undiminished form, [...] or maintaining a field of application, thus accepting a reduction of fundamental rights standards. Under these circumstances, and with regards to the constitution, the legislator is not precluded from choosing the second option." (BVerfGE 92, 26: para. 62)

14 These recommendations for a practical design of the G 10 justifications are based on the ideas formulated in Senator Blumenthal's legislative proposal towards the end of the sixth section.

15 An example can be found on the following page: http://www.dni.gov/files/do- cuments/0315/FISC%200pinion%20and%200rder%20May%2018%202012.pdf

16 Thus, when one is working on improving democratic control over telecommunication surveillance, one should consider the question of whether this practice, the legal reform of which requires numerous legal and institutional changes, actually draws in sufficient information gain. As regards the related question of the necessity of data preservation, neither the Max-Plank-Institute nor the research service of the Bundestag were able to "find evidence that the types of massive communication surveillance resulted in the promised increase in security" (Çaliskan 2015)

17 The operator of the internet node DE-CIX is presently considering whether to file an action before the Federal Administrative Court. The actions of the organisation Reporters Without Borders and that of Prof. Härting are already pending before the Federal Administrative Court. Additionally, the G 10-Commission is considering whether to file a lawsuit against the government before the Federal Constitutional Court for inspecting the list of selectors. Considering the large number of open legal questions, further lawsuits are likely to be filed. In Autria, the deputy Peter Pilz filed a lawsuit against the Deutsche Telekom and two members of the German government.

## About the author

Dr. Thorsten Wetzling leads the privacy project at the stiftung neue verantwortung. The project engages policy makers, civil society and experts in the development of reform proposals to improve the democratization and professionalization of intelligence governance in Germany. Thorsten holds a doctorate degree in political science from the Graduate Institute of International and Development Studies in Geneva.

## About snv

The stiftung neue verantwortung is a non-profit think tank in Berlin that brings together expertise from government, research institutions, NGOs and companies to develop, discuss, and disseminate proposals on current political issues. The goal of stiftung neue verantwortung is to assist stakeholders, both in and outside of politics, in making effective decisions that benefit the common good by using a combination of content-based expertise, practical political experience and cross-sectoral cooperation.

## Impressum

stiftung neue verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T. +49 30 81 45 03 78 80
F. +49 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de
Twitter: @snv_Berlin

Layout:
Sebastian Rieger